

ASDM Livre 2 : Guide de configuration d'ASDM Cisco Secure Firewall ASA, 7.19

Dernière modification : 2026-08-27

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)

© 2022–2026 Cisco Systems, Inc. Tous droits réservés.

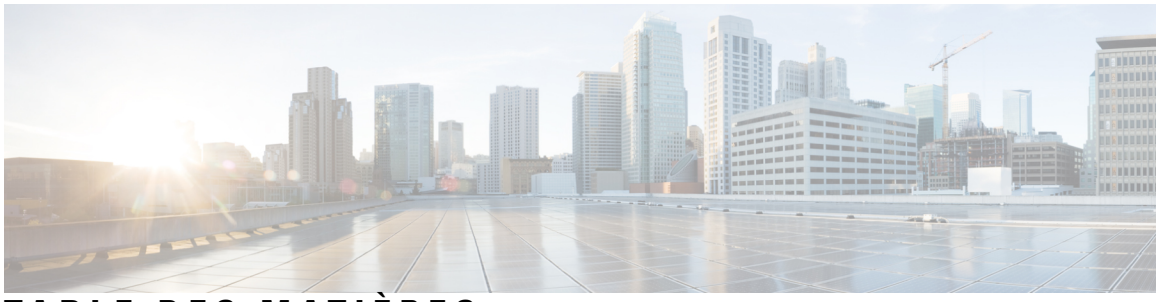


TABLE DES MATIÈRES

PRÉFACE

À propos de ce guide xvii

Objectifs du document xvii

Documentation associée xvii

Conventions de document xvii

Communications, services et renseignements supplémentaires xix

CHAPITRE 1

Introduction aux services de pare-feu Secure Firewall ASA 1

Comment mettre en œuvre les services de pare-feu 1

Contrôle d'accès de base 2

Filtrage URL 2

Protection contre les menaces 2

Services de pare-feu pour les environnements virtuels 3

NAT (Network Address Translation; Translation d'adresses de réseau) 4

Inspection des applications 4

Scénario d'utilisation : exposer un serveur au public 5

PARTIE I

Contrôle d'accès 9

CHAPITRE 2

Règles d'accès 11

Contrôle d'accès au réseau 11

Renseignements généraux sur les règles 12

Règles d'accès d'interface et règles d'accès globales 12

Règles entrantes et sortantes 12

Ordre des règles 13

Autorisations implicites 13

Refus implicite 14

NAT et critères d’accès 14
Interfaces de niveau de sécurité identiques et règles d’accès 14
Règles d'accès étendues 15
Règles d’accès étendues pour le retour du trafic 15
Autoriser le trafic de diffusion et de multidiffusion 15
Règles d’accès de gestion 16
Règles EtherType 16
EtherTypes pris en charge et autres types de trafic 16
Règles EtherType pour le retour du trafic 17
Autoriser MPLS 17
Licences pour les règles d’accès 17
Lignes directrices relatives au contrôle d’accès 17
Configurer le contrôle d’accès 19
Configurer les règles d’accès 19
Propriétés de la règle d’accès 20
Configurer les options avancées pour les règles d'accès 23
Configurer les règles d’accès de gestion 24
Configurer les règles EtherType 25
Configurer les règles d’accès ICMP 27
Surveillance des règles d’accès 28
Évaluation des messages Syslog pour les règles d’accès 28
Historique des règles d'accès 29

CHAPITRE 3 **Objets pour le contrôle d’accès.** 33
Lignes directrices relatives aux objets 33
Configurer les objets. 34
Configurer les objets et groupes de réseau 34
Configurer un objet réseau 34
Configurer un groupe d’objets réseau 35
Configurer des objets de service et des groupes de services 35
Configurer un objet de service 35
Configurer un groupe de services 36
Configuration des objets et des groupes de service réseau 37
Lignes directrices relatives aux objets de service de réseau 37

Configurer des serveurs DNS de confiance 38
Configurer les objets de service réseau 39
Configurer les groupes d'objets de service réseau 40
Configurer les groupes d'utilisateurs locaux 42
Configurer les groupes d'objets de groupe de sécurité 43
Configurer les plages de temps 44
Objets de surveillance 45
Historique pour les objets 45

CHAPITRE 4 **Listes de contrôle d'accès 49**
À propos des ACL 49
Types d'ACL 49
Le gestionnaire d'ACL 51
Noms d'ACL 52
Ordre des entrées de contrôle d'accès 52
Autoriser/refuser ou mettre en correspondance/aucune correspondance 52
Refus implicite du contrôle d'accès 53
Adresses IP utilisées pour les listes de contrôle d'accès étendues lorsque vous utilisez la NAT 53
ACE temporelles 54
Licences pour les listes de contrôle d'accès 54
Lignes directrices pour les ACL 55
Configurer les ACL 56
Configurer les ACL étendues 56
Propriétés des ACE étendues 57
Caractéristiques de service dans les ACE étendues 59
Configurer les ACL standard 60
Configurer les ACL de type Web 61
Propriétés des ACE Webtype 62
Exemples d'ACL de type Web 64
Surveillance des ACL 64
Historique des ACL 65

CHAPITRE 5 **ASA et Cisco TrustSec 69**
À propos de Cisco TrustSec 69

À propos de la prise en charge de SGT et SXP dans Cisco TrustSec 70
Rôles dans la fonctionnalité Cisco TrustSec 71
Application de la politique de groupe de sécurité 72
Comment l'ASA applique les politiques basées sur les groupes de sécurité 73
Effets des modifications des groupes de sécurité sur l'ISE 74
Rôles de speaker et de listener sur l'ASA 75
Enregistrer l'ASA auprès de l'ISE 76
Créer un groupe de sécurité sur l'ISE 76
Générer le fichier PAC 77
Lignes directrices relatives à Cisco TrustSec 77
Configurer l'ASA pour s'intégrer à Cisco TrustSec 80
Configurer le serveur AAA pour l'intégration de Cisco TrustSec 81
Importer un fichier PAC 82
Configurer le protocole d'échange de sécurité 83
Ajouter un homologue de connexion SXP 85
Actualiser les données d'environnement 86
Configurer la politique de sécurité 86
Configurer l'imposition du balisage de groupe de sécurité de couche 2 87
Scénarios d'utilisation 88
Configurer une balise de groupe de sécurité sur une interface 89
Configurer manuellement les liaisons IP-SGT 90
Prise en charge de Cisco TrustSec pour les VPN Secure Client (services client sécurisés) 91
Ajouter une balise SGT aux politiques de groupe du VPN d'accès à distance et aux utilisateurs locaux 91
Surveillance de Cisco TrustSec 92
Historique de Cisco TrustSec 93

CHAPITRE 6 **Cisco Umbrella 95**
À propos de Cisco Umbrella Connector 95
Politique de sécurité entreprise Cisco Umbrella 95
Enregistrement de Cisco Umbrella 96
Exigences de licence pour Cisco Umbrella Connector 96
Lignes directrices et limites relatives à Cisco Umbrella 97
Configurer Cisco Umbrella Connector 99

Installer le certificat d'autorité de certification à partir du serveur d'enregistrement Cisco Umbrella 99
Configurer les paramètres globaux du connecteur Cisco Umbrella 100
Activer Cisco Umbrella dans la liste des politiques d'inspection DNS 102
Vérifier l'enregistrement de Cisco Umbrella 103
Surveillance du connecteur Cisco Umbrella 104
Surveillance des statistiques de politique de service Cisco Umbrella 104
Surveillance des messages Syslog Cisco Umbrella 105
Historique du connecteur Cisco Umbrella 107

PARTIE II **Services de pare-feu pour les environnements virtuels** 109

CHAPITRE 7 **Contrôle d'accès basé sur les attributs** 111
Lignes directrices relatives aux objets réseau basés sur les attributs 111
Configurer le contrôle d'accès basé sur les attributs 112
Configurer les attributs des machines virtuelles vCenter 112
Configurer un agent d'attribut de VM 114
Configurer les objets réseau basés sur les attributs 115
Configurer les règles d'accès à l'aide d'objets réseau basés sur les attributs 116
Surveillance des objets réseau basés sur les attributs 117
Historique du contrôle d'accès basé sur les attributs 117

PARTIE III **NAT (Network Address Translation; Translation d'adresses de réseau)** 119

CHAPITRE 8 **Traduction d'adresses réseau (NAT)** 121
Pourquoi utiliser la NAT? 121
Principes de base de la NAT 122
Terminologie NAT 122
Types de NAT 122
NAT objet de réseau et Twice NAT (NAT en double) 123
NAT objet de réseau 123
Twice NAT (NAT en double) 123
Comparaison de NAT objet de réseau et Twice NAT (NAT en double) 124
Ordre des règles NAT 125
Interfaces NAT 127

Directives pour la NAT 127
Lignes directrices sur le mode pare-feu pour la NAT 127
Lignes directrices relatives à la NAT IPv6 128
Bonnes pratiques pour la NAT IPv6 128
Lignes directrices supplémentaires pour la NAT 129
Lignes directrices de NAT d'objets réseau pour les objets d'adresses mappées 132
Lignes directrices pour le NAT Twice concernant les objets d'adresses réelles et mappées 133
Lignes directrices relatives aux destinations FQDN 134
Lignes directrices NAT Twice pour les objets de service pour les ports réels et mappés 135
Traduction d'adresses réseau dynamique 135
À propos de la NAT dynamique 136
Désavantages et avantages de la NAT dynamique 137
Configurer la NAT dynamique 137
Configurer la NAT Twice dynamique 139
PAT dynamique 144
À propos de la PAT dynamique 144
Avantages et inconvénients de la PAT dynamique 145
Lignes directrices relatives aux objets de regroupement PAT 145
Configurer la PAT d'objet réseau dynamique (Masquer) 146
Configurer la PAT d'objet réseau dynamique à l'aide d'un ensemble PAT 149
Configurer la PAT Twice dynamique (Masquer) 152
Configurer la PAT Twice dynamique à l'aide d'un ensemble PAT 157
Configurer PAT avec l'attribution de bloc de ports 163
Configurer la PAT par session ou la PAT multi-session (version 9.0(1) et versions ultérieures) 165
NAT statique 166
À propos de la NAT statique 166
NAT statique avec traduction de port 167
NAT statique un vers plusieurs 168
Autres scénarios de mappage (non recommandés) 169
Configurer la NAT d'objet réseau statique ou la NAT statique avec traduction de port 170
Configurer la NAT statique Twice ou la NAT statique avec traduction de port 173
NAT d'identité 178
Configurer la NAT d'objet de réseau d'identité 179
Configurer la NAT d'identité Twice 181

Surveillance de la NAT 186

Historique de la NAT 186

CHAPITRE 9 **Exemples et références de NAT 195**

Exemples de NAT d'objets réseau 195

Fournir l'accès à un serveur Web interne (NAT statique) 195

NAT pour les hôtes internes (NAT dynamique) et NAT pour un serveur Web externe (NAT statique) 198

Équilibreur de charge interne avec plusieurs adresses mappées (NAT statique, un à plusieurs) 202

Adresse unique pour FTP, HTTP et SMTP (NAT statique avec traduction de port) 204

Exemples relatifs à la NAT Twice 208

Traduction différente selon la destination (PAT manuelle dynamique) 208

Traduction différente selon l'adresse et le port de destination (PAT dynamique) 215

NAT en mode routé et transparent 221

NAT en mode routé 221

NAT en mode transparent ou dans un groupe de pont 222

Routage des paquets NAT 223

Adresses mappées et routage 224

Adresses sur le même réseau que l'interface mappée 224

Adresses sur un réseau unique 224

Même adresse que l'adresse réelle (NAT d'identité) 225

Exigences de routage en mode transparent pour les réseaux distants 226

Détermination de l'interface de sortie 226

NAT pour VPN 227

NAT et VPN d'accès à distance 227

NAT et VPN de site à site 229

Accès à la gestion de la NAT et du VPN 232

Dépannage de la NAT et du VPN 233

Traduction des réseaux IPv6 233

NAT64/46 : traduction d'adresses IPv6 en IPv4 234

Exemple NAT64/46 : réseau IPv6 interne avec Internet IPv4 externe 234

Exemple NAT64/46 : réseau interne IPv6 avec Internet IPv4 externe et traduction DNS 237

NAT66 : traduction d'adresses IPv6 en adresses différentes IPv6 240

Exemple de NAT66 : traduction statique entre réseaux 241

Exemple de NAT66, PAT d'interface IPv6 simple 242
Réécriture des requêtes et des réponses DNS à l'aide de la NAT 244
Modification de la réponse DNS, serveur DNS externe 245
Modification de la réponse DNS, serveur DNS, hôte et serveur sur des réseaux séparés 247
Modification de la réponse DNS, serveur DNS sur le réseau hôte 248
Modification de la réponse DNS64 250
Modification PTR, serveur DNS sur le réseau hôte 256

CHAPITRE 10 **Mappage de l'adresse et du port (MAP) 259**
Mappage de l'adresse et du port (MAP) 259
Traduction du mappage de l'adresse et du port (MAP-T) 259
Lignes directrices pour le mappage de l'adresse et du port (MAP) 260
Configurer les domaines MAP-T 262
Surveillance MAP 263
Vérification de la configuration du domaine MAP 263
Surveillance des messages Syslog 264
Historique de MAP 264

PARTIE IV **Politiques de service et inspection des applications 265**

CHAPITRE 11 **Politique de service 267**
À propos des politiques de service 267
Les composants d'une politique de service 267
Fonctionnalités configurées avec les politiques de service 269
Sens d'application de la fonctionnalité 270
Correspondance des fonctionnalités dans une politique de service 271
Ordre dans lequel plusieurs actions de fonctionnalité sont appliquées 272
Incompatibilité de certaines actions de fonctionnalité 272
Mise en correspondance des fonctionnalités pour plusieurs politiques de service 273
Lignes directrices pour les politiques de service 273
Par défaut pour les politiques de service 275
Configuration de la politique de service par défaut 275
Cartes de trafics par défaut (classes de trafic) 275
Configurer les politiques de service 276

Ajouter une règle de politique de service pour le trafic de transit 276
Ajouter une règle de politique de service pour le trafic de gestion 280
Gérer l'ordre des règles de politique de service 281
Historique des politiques de service 283

CHAPITRE 12 **Premiers pas avec l'inspection du protocole de la couche application 285**
Inspection des protocoles de la couche applicative 285
Quand utiliser l'inspection du protocole d'application 285
Listes des politiques d'inspection 286
Remplacement d'une liste des politiques d'inspection en cours d'utilisation 286
Comment plusieurs classes de trafic sont gérées 286
Lignes directrices relatives à l'inspection des applications 287
Valeurs par défaut pour l'inspection des applications 289
Inspections par défaut et limites de la NAT 289
Listes des politiques d'inspection par défaut 293
Configurer l'inspection du protocole de couche d'application 293
Configurer les expressions régulières 297
Créer une expression régulière 297
Créer une carte de trafic d'expression régulière 302
Surveillance des politiques d'inspection 302
Historique de l'inspection des applications 303

CHAPITRE 13 **Inspection des protocoles Internet de base 305**
Inspection DCERPC 305
Présentation de DCERPC 306
Configurer une liste des politiques d'inspection DCERPC 306
Inspection DNS 308
Valeurs par défaut pour l'inspection DNS 308
Configurer la liste des politiques d'inspection DNS 309
Inspection FTP 312
Présentation de l'inspection FTP 313
FTP strict 313
Configurer une liste des politiques d'inspection FTP 314
Inspection HTTP 317

Présentation de l’inspection HTTP 317
Configurer une liste des politiques d’inspection HTTP 318
Inspection ICMP 321
Inspection des erreurs ICMP 322
Inspection ILS 322
Inspection de la messagerie instantanée 323
Inspection des options IP 325
Valeurs par défaut pour l’inspection des options IP 325
Configurer une liste des politiques d’inspection des options IP 326
Inspection IPsec Pass Through 327
Aperçu de l’inspection de transmission directe IPsec 327
Configurer une liste des politiques d’inspection de transmission directe IPsec 327
Inspection IPv6 328
Valeurs par défaut pour l’inspection IPv6 329
Configurer une liste des politiques d’inspection IPv6 329
Inspection NetBIOS 330
Inspection PPTP 331
Inspection RSH 331
Inspection SMTP et SMTP étendue 332
Aperçu de l’inspection SMTP et ESMTP 332
Valeurs par défaut pour l’inspection ESMTP 333
Configurer une liste des politiques d’inspection ESMTP 333
Inspection SNMP 336
Inspection SQL*Net 337
Inspection Sun RPC 337
Aperçu de l'inspection Sun RPC 337
Gérer les services Sun RPC 338
Inspection TFTP 339
Inspection XDMCP 339
Inspection VXLAN 340
Historique de l'inspection du protocole Internet de base 340

CHAPITRE 14 **Inspection des protocoles vocaux et vidéo** 343
Inspection CTIQBE 343

Limites de l’inspection CTQBE 343
Inspection H.323 344
Survol de l’inspection H.323 344
Fonctionnement de H.323 344
Prise en charge H.239 dans les messages H.245 345
Limites de l’inspection H.323 346
Configurer la liste des politiques d’inspection H.323 346
Inspection MGCP 349
Aperçu de l'inspection MGCP 349
Configurer une liste des politiques d’inspection MGCP 350
Inspection RTSP 352
Survol de l’inspection RTSP 352
Exigences de configuration de RealPlayer 352
Limites de l’inspection RSTP 352
Configurer une liste des politiques d’inspection RTSP 353
Inspection SIP 355
Présentation de l’inspection SIP 355
Limites pour l’inspection SIP 356
Inspection SIP par défaut 357
Configurer une liste des politiques d’inspection SIP 357
Inspection Skinny (SCCP) 360
Aperçu de l’inspection SCCP 360
Prise en charge des téléphones IP Cisco 360
Limites de l’inspection SCCP 361
Inspection SCCP par défaut 361
Configurer une liste des politiques d’inspection Skinny (SCCP) 362
Inspection STUN 363
Historique de l’inspection des protocoles vocaux et vidéo 364

CHAPITRE 15 **Inspection des réseaux mobiles** 367
Aperçu de l’inspection du réseau mobile 367
Présentation de l’inspection GTP 367
Suivi des changements d’emplacement pour les stations mobiles 368
Limites d’inspection GTP 368

Inspection et contrôle d’accès SCTP (Stream Control Transmission Protocol) 369
Inspection dynamique SCTP 370
Contrôle d'accès SCTP 370
NAT SCTP 370
Inspection de la couche application SCTP 371
Limites de SCTP 371
Inspection Diameter 372
Inspection M3UA 372
Conformité au protocole M3UA 373
Limites d’inspection M3UA 374
Aperçu de l’inspection de comptabilité RADIUS 374
Licences pour l’inspection des protocoles de réseau mobile 375
Valeurs par défaut pour l’inspection GTP 375
Configurer l’inspection du réseau mobile 376
Configurer une liste des politiques d’inspection GTP 376
Configurer une liste des politiques d’inspection SCTP 380
Configurer une liste des politiques d’inspection Diameter 382
Créer une paire attribut-valeur (AVP) de Diameter personnalisée 385
Inspection des sessions Diameter chiffrées 386
Configurer la relation de confiance du serveur avec les clients Diameter 387
Configurer le proxy TLS complet avec un certificat client statique pour l’inspection Diameter 388
Configurer le proxy TLS complet avec des certificats dynamiques locaux pour l’inspection Diameter 390
Configurer le serveur mandataire TLS avec déchargement TLS pour l’inspection Diameter 392
Configurer une liste des politiques d’inspection M3UA 394
Configurer la politique de service d’inspection de réseau mobile 397
Configurer l’inspection de comptabilité RADIUS 398
Configurer une liste des politiques d’inspection de comptabilité RADIUS 398
Configurer la politique de service d’inspection de comptabilité RADIUS 399
Surveillance de l’inspection du réseau mobile 400
Surveillance de l'inspection GTP 400
Surveillance SCTP 402
Surveillance de Diameter 403
Surveillance M3UA 403

Historique de l’inspection du réseau mobile 404

PARTIE V **Gestion des connexions et détection des menaces 409**

CHAPITRE 16 **Paramètres de connexion 411**

Que sont les paramètres de connexion ? 411

Configurer les paramètres de connexion 412

Configurer les délais d’expiration globaux 413

Protéger les serveurs contre une attaque DoS par inondation SYN (interception de TCP) 416

Personnaliser le traitement anormal des paquets TCP (listes TCP, normaliseur TCP) 418

Contourner les vérifications de l’état TCP pour le routage asymétrique (TCP State Bypass) 421

Le problème du routage asymétrique 421

Lignes directrices et limites du contournement d'état TCP 422

Configurer le contournement d’état TCP 423

Désactiver la gestion aléatoire de la séquence TCP 423

Délester les flux volumineux 425

Limites de déchargement de flux 425

Configurer le déchargement de flux 427

Décharge de flux IPsec 428

Configurer le déchargement de flux IPsec 429

Configurer les paramètres de connexion pour des classes de trafic spécifiques (tous les services) 429

Configurer les options TCP 433

Supervision des connexions 434

Historique des paramètres de connexion 435

CHAPITRE 17 **Qualité de service 441**

À propos de QoS 441

Fonctionnalités QoS prises en charge 441

Qu’est-ce qu’un compartiment de jetons? 442

Police 442

File d’attente prioritaire 442

Comment les fonctionnalités QoS interagissent 443

Préservation DSCP (DiffServ) 443

Lignes directrices pour la QoS 443

Configurer QoS 444
Déterminer les limites de la file d'attente et de l'anneau TX pour une file d'attente prioritaire 444
Feuille de travail sur la limite de la file d'attente 444
Feuille de calcul des limites de l'anneau TX 445
Configurer la file d'attente prioritaire pour une interface 446
Configurer une règle de service pour la mise en file d'attente prioritaire et la régulation 447
Surveiller la QoS 448
Statistiques de régulation QoS 448
Statistiques de priorité QoS 449
Statistiques de file d'attente prioritaire QoS 449
Historique QoS 450

CHAPITRE 18 **Détection des menaces 451**
Détection des menaces 451
Statistiques de détection des menaces de base 452
Statistiques de détection avancée des menaces 452
Détection des menaces par analyse 453
Lignes directrices pour la détection des menaces 454
Paramètres par défaut pour la détection des menaces 454
Configurer la détection des menaces 455
Configurer les statistiques de base sur la détection des menaces 455
Configurer les statistiques de détection avancée des menaces 456
Configurer l'analyse de détection des menaces 457
Surveillance de la détection des menaces 458
Surveillance des statistiques de détection de base des menaces 458
Surveillance des statistiques de détection avancée des menaces 458
Historique de la détection des menaces 459



À propos de ce guide

Les rubriques suivantes expliquent comment utiliser ce guide.

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

Objectifs du document

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

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

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

Documentation associée

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

Conventions de document

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

Conventions de texte

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

Alertes adressées aux lecteurs

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



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



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



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

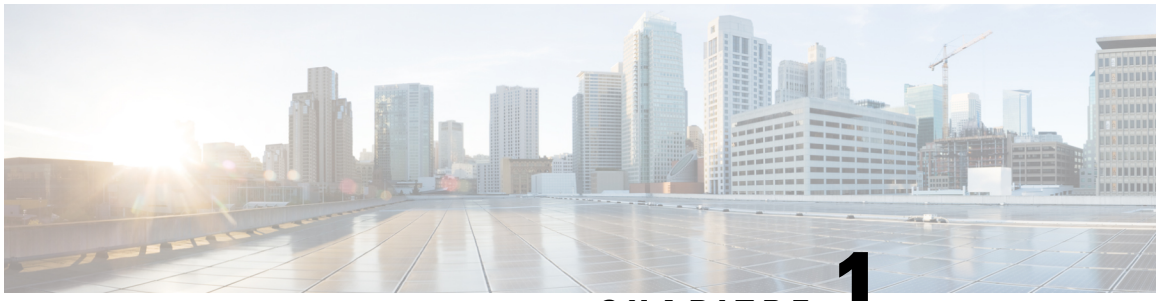
Économiseur de temps	Indique que *l'action décrite permet de gagner du temps.* Vous pouvez gagner du temps en exécutant l'action décrite dans le paragraphe.
Avertissement	**signifie que *le lecteur doit être averti.* Dans cette situation, vous pourriez effectuer une opération risquant d'entraîner des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

Communications, services et renseignements supplémentaires

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

Outil de recherche de bogues

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



CHAPITRE 1

Introduction aux services de pare-feu Secure Firewall ASA

Les services de pare-feu sont les fonctionnalités de l'ASA axées sur le contrôle de l'accès au réseau, y compris les services qui bloquent le trafic et les services qui permettent le flux du trafic entre les réseaux internes et externes. Ces services comprennent ceux qui protègent le réseau contre les menaces, telles que le déni de service (DoS) et d'autres attaques.

Les rubriques suivantes fournissent un aperçu des services de pare-feu.

- Comment mettre en œuvre les services de pare-feu, à la page 1
- Contrôle d'accès de base, à la page 2
- Filtrage URL, à la page 2
- Protection contre les menaces, à la page 2
- Services de pare-feu pour les environnements virtuels, à la page 3
- NAT (Network Address Translation; Translation d'adresses de réseau), à la page 4
- Inspection des applications, à la page 4
- Scénario d'utilisation : exposer un serveur au public, à la page 5

Comment mettre en œuvre les services de pare-feu

La procédure suivante fournit une séquence générale pour la mise en œuvre des services de pare-feu. Cependant, chaque étape est facultative et n'est nécessaire que si vous souhaitez fournir le service à votre réseau.

Avant de commencer

Configurez l'ASA conformément au guide de configuration sur les opérations générales, y compris au minimum les paramètres de base, la configuration de l'interface, le routage et l'accès de gestion.

Procédure

Étape 1 Implémentez le contrôle d'accès pour le réseau. Consultez Contrôle d'accès de base, à la page 2.

Étape 2 Implémentez le filtrage d'URL. Consultez Filtrage URL, à la page 2.

Étape 3 Implémentez la protection contre les menaces. Consultez Protection contre les menaces, à la page 2.

Étape 4 Implémentez des services de pare-feu adaptés aux environnements virtuels. Consultez Services de pare-feu pour les environnements virtuels, à la page 3.

Étape 5 Implémentez la traduction d'adresses réseau (NAT). Consultez NAT (Network Address Translation; Translation d'adresses de réseau), à la page 4.

Étape 6 Implémentez l'inspection d'application si les paramètres par défaut sont insuffisants pour votre réseau. Consultez Inspection des applications, à la page 4.

Contrôle d'accès de base

Les règles d'accès, appliquées par interface ou globalement, sont votre première ligne de défense. Vous pouvez abandonner, à l'entrée, des types de trafic spécifiques ou le trafic provenant d'hôtes ou de réseaux spécifiques, ou à destination de ceux-ci. Par défaut, l'ASA permet au trafic de circuler librement d'un réseau interne (niveau de sécurité supérieur) vers un réseau externe (niveau de sécurité inférieur).

Vous pouvez appliquer des critères d'accès pour limiter le trafic de l'intérieur vers l'extérieur ou autoriser le trafic de l'extérieur vers l'intérieur.

Les règles d'accès de base contrôlent le trafic à l'aide d'un « 5-tuple » de l'adresse source et du port, de l'adresse et du port de destination et du protocole. Consultez Règles d'accès, à la page 11 et Listes de contrôle d'accès, à la page 49.

Vous pouvez enrichir vos règles en les rendant compatibles avec l'identité. Pour mettre en œuvre le contrôle d'identité, installez Cisco Identity Services Engine (ISE) sur un serveur distinct pour mettre en œuvre Cisco TrustSec. Vous pouvez ensuite ajouter des critères de groupe de sécurité à vos règles d'accès. Consultez ASA et Cisco TrustSec, à la page 69.

Filtrage URL

Le filtrage d'URL refuse ou autorise le trafic en fonction de l'URL du site de destination.

Pour mettre en œuvre le filtrage d'URL, abonnez-vous au service Cisco Umbrella, où vous configurez la politique de sécurité entreprise pour bloquer les sites malveillants en fonction du nom de domaine complet (FQDN). Vous pouvez autoriser ou bloquer les connexions en fonction du FQDN ou, pour les FQDN suspects, vous pouvez rediriger l'utilisateur vers le mandataire intelligent Cisco Umbrella, qui peut effectuer le filtrage d'URL. Le service Cisco Umbrella fonctionne par la gestion des demandes de recherche DNS des utilisateurs, en renvoyant l'adresse IP d'une page de blocage ou l'adresse IP du serveur proxy intelligent. Le service renvoie l'adresse IP réelle d'un nom de domaine complet (FQDN) pour les domaines autorisés. Consultez Cisco Umbrella, à la page 95.

Protection contre les menaces

Vous pouvez mettre en œuvre un certain nombre de mesures pour vous protéger contre l'analyse, le déni de service (DoS) et d'autres attaques. Un certain nombre de fonctionnalités ASA aident à protéger contre les attaques en appliquant des limites de connexion et en abandonnant des paquets TCP anormaux. Certaines fonctionnalités sont automatiques, d'autres sont configurables, mais ont des valeurs par défaut appropriées dans la plupart des cas, tandis que d'autres sont entièrement facultatives et vous devez les configurer si vous le souhaitez.

Voici les services de protection contre les menaces disponibles avec l'ASA.

- Protection contre la fragmentation des paquets IP : l'ASA effectue le réassemblage complet de tous les messages d'erreur ICMP et le réassemblage virtuel des fragments IP restants qui sont acheminés par l'ASA, et rejette les fragments qui échouent au contrôle de sécurité. Aucune configuration n'est nécessaire.
- Limites de connexion, normalisation TCP et autres fonctionnalités liées à la connexion : configurez les services liés à la connexion tels que les limites et les délais d'expiration de connexion TCP et UDP, l'aléatoireisation du numéro de séquence TCP, la normalisation TCP et le contournement de l'état TCP. La normalisation TCP est conçue pour abandonner les paquets qui ne semblent pas normaux. Consultez Paramètres de connexion, à la page 411.

  Par exemple, vous pouvez limiter les connexions TCP et UDP et les connexions amorces (une demande de connexion qui n'a pas terminé l'établissement de liaison entre la source et la destination). La limitation du nombre de connexions et de connexions amorces vous protège contre les attaques DoS. L'ASA utilise la limite amorce pour déclencher l'interception TCP, qui protège les systèmes internes contre une attaque DoS perpétrée en inondant une interface de paquets SYN de TCP.
- Détection des menaces : mettez en œuvre la détection des menaces sur l'ASA pour recueillir des statistiques afin d'identifier les attaques. La détection de base des menaces est activée par défaut, mais vous pouvez mettre en œuvre des statistiques avancées et une détection des menaces d'analyse. Vous pouvez bloquer les hôtes identifiés comme une menace d'analyse. Consultez Détection des menaces, à la page 451.

Services de pare-feu pour les environnements virtuels

Les environnements virtuels déploient des serveurs en tant que machines virtuelles, par exemple, dans VMware ESXi. Les pare-feu dans un environnement virtuel peuvent être des périphériques matériels classiques ou des pare-feu de machines virtuelles, comme ASA virtuel.

Les services de pare-feu traditionnel et de nouvelle génération s'appliquent aux environnements virtuels de la même manière qu'ils s'appliquent aux environnements qui n'utilisent pas de serveurs de machines virtuelles. Cependant, les environnements virtuels peuvent présenter des défis supplémentaires, car il est facile de créer et de démonter des serveurs.

En outre, le trafic entre les serveurs au sein du centre de données peut nécessiter autant de protection que le trafic entre le centre de données et les utilisateurs externes. Par exemple, si un agresseur prend le contrôle d'un serveur dans le centre de données, cela pourrait ouvrir des attaques sur d'autres serveurs du centre de données.

Les services de pare-feu pour les environnements virtuels ajoutent des fonctionnalités pour appliquer une protection de pare-feu spécifiquement aux machines virtuelles. Voici les services de pare-feu disponibles pour les environnements virtuels :

- Contrôle d'accès basé sur les attributs : vous pouvez configurer des objets réseau pour qu'ils correspondent au trafic en fonction des attributs et utiliser ces objets dans les règles de contrôle d'accès. Cela vous permet de dissocier les règles de pare-feu de la topologie du réseau. Par exemple, vous pouvez autoriser tous les hôtes avec l'attribut Engineering à accéder aux hôtes avec l'attribut Lab Server. Vous pourriez ensuite ajouter ou supprimer des hôtes avec ces attributs et la politique de pare-feu serait appliquée automatiquement sans qu'il soit nécessaire de mettre à jour les règles d'accès. Pour en savoir plus, consultez Contrôle d'accès basé sur les attributs, à la page 111.

NAT (Network Address Translation; Translation d'adresses de réseau)

L'une des fonctions principales de la traduction d'adresses réseau (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 routé uniquement) : si vous souhaitez connecter un réseau IPv6 à un réseau IPv4, la NAT vous permet de traduire entre les deux types d'adresses.

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.

Voir :

- Traduction d'adresses réseau (NAT), à la page 121
- Exemples et références de NAT, à la page 195

Inspection des applications

Des plateformes d'inspection sont nécessaires pour les services qui intègrent des renseignements d'adressage IP dans le paquet de données des utilisateurs ou qui ouvrent des canaux secondaires sur des ports attribués de manière dynamique. Ces protocoles obligent l'ASA à effectuer une inspection approfondie des paquets, à ouvrir les passages requis et à appliquer la traduction d'adresses réseau (NAT).

La politique d'ASA par défaut applique déjà l'inspection globalement pour de nombreux protocoles courants, tels que DNS, FTP, SIP, ESMTP, TFTP, etc. Les inspections par défaut peuvent être tout ce dont vous avez besoin pour votre réseau.

Cependant, vous devrez peut-être activer l'inspection pour d'autres protocoles ou affiner une inspection. De nombreuses inspections comprennent des options détaillées qui vous permettent de contrôler les paquets en fonction de leur contenu. Si vous connaissez bien un protocole, vous pouvez appliquer un contrôle fin à ce trafic.

Vous utilisez des politiques de service pour configurer l'inspection des applications. Vous pouvez configurer une politique de service globale ou appliquer une politique de service à chaque interface, ou les deux.

Voir :

• Politique de service, à la page 267
• Premiers pas avec l'inspection du protocole de la couche application, à la page 285
• Inspection des protocoles Internet de base, à la page 305
• Inspection des protocoles vocaux et vidéo, à la page 343
• Inspection des réseaux mobiles, à la page 367.

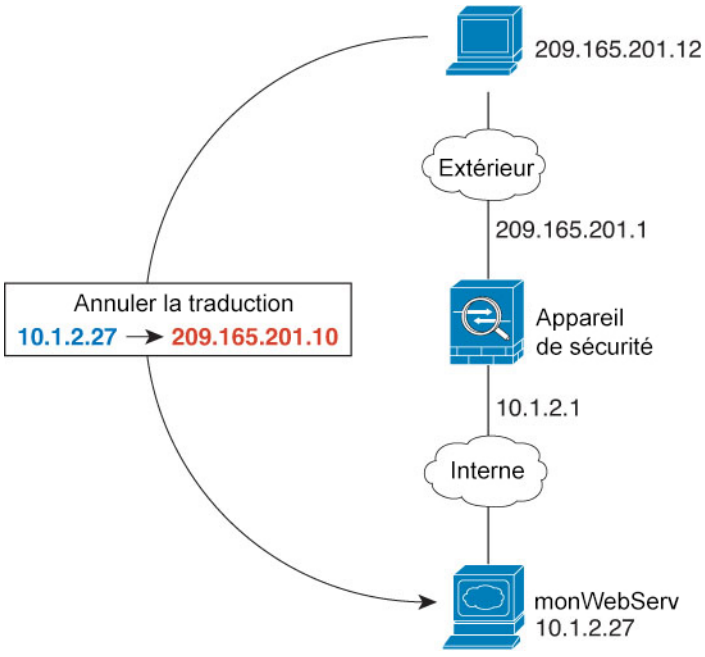
Scénario d'utilisation : exposer un serveur au public

Vous pouvez mettre certains services d'applications sur un serveur à la disposition du public. Par exemple, vous pourriez exposer un serveur Web, afin que les utilisateurs puissent se connecter aux pages Web, mais ne puissent effectuer aucune autre connexion au serveur.

Pour exposer un serveur au public, vous devez généralement créer des règles d'accès qui autorisent la connexion et des règles NAT qui assurent la traduction entre l'adresse IP interne du serveur et une adresse externe que le public peut utiliser. En outre, vous pouvez utiliser la traduction d'adresses de port (PAT) pour mapper un port interne à un port externe, si vous ne souhaitez pas que le service exposé à l'extérieur utilise le même port que le serveur interne. Par exemple, si le serveur Web interne ne fonctionne pas sur TCP/80, vous pouvez le mapper à TCP/80 pour faciliter les connexions pour les utilisateurs externes.

L'exemple suivant rend un serveur Web du réseau privé interne accessible au public.

Illustration 1 : NAT statique pour un serveur Web interne



ASDM comprend un raccourci pour configurer les règles d'accès et de NAT requises, afin de simplifier le processus d'exposition d'un service sur un serveur interne au public.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Public Servers (Serveurs publics)**.

Étape 2 Cliquez sur **Add** (ajouter).

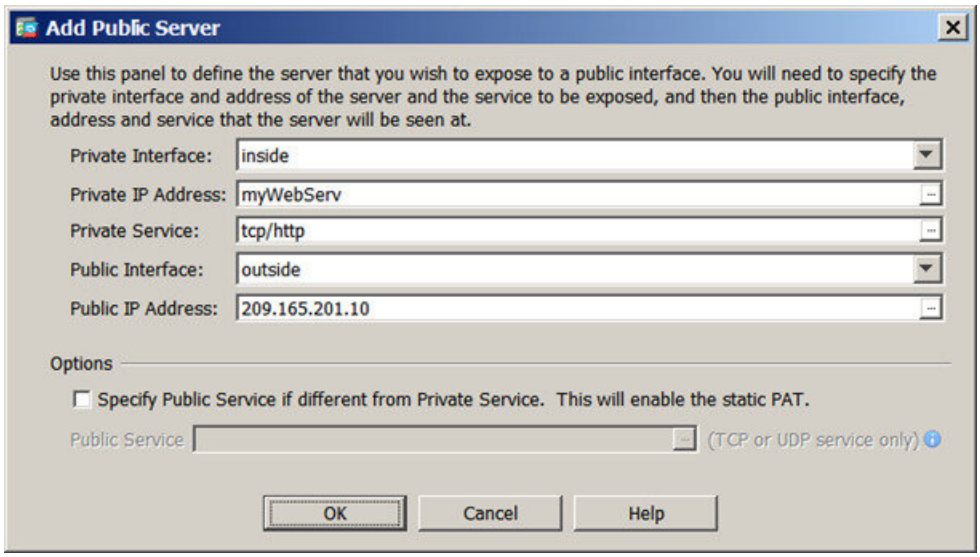
Étape 3 Définissez les caractéristiques privées et publiques du service que vous exposez.

- **Interface privée** : l'interface à laquelle le serveur réel est connecté. Dans cet exemple, « inside » (interne).
- **Adresse IP privée** : objet du réseau de l'hôte qui définit l'adresse IPv4 réelle du serveur. Vous ne pouvez pas préciser une adresse IPv6. Si vous n'avez pas encore d'objet contenant l'adresse, créez-en un en cliquant sur le bouton « ... », puis en cliquant sur **Add** (Ajouter). Dans cet exemple, le nom de l'objet serait MyWebServ et contiendrait l'adresse d'hôte 10.1.2.27.
- **Service privé** : le service réel qui est en cours d'exécution sur le serveur réel. Vous pouvez utiliser un service ou un objet de service prédéfini. Vous pouvez également utiliser un groupe d'objets de service, sauf si vous spécifiez également un service public auquel vous mappez le service privé.

  Vous pouvez exposer plusieurs services; toutefois, si vous spécifiez un service public, tous les ports sont mappés au même port public.

  Dans cet exemple, le port est **tcp/http**.
- **Interface publique** : l'interface par laquelle les utilisateurs externes peuvent accéder au serveur réel. Dans cet exemple, « outside » (externe).
- **Adresse publique** : l'adresse IPv4 vue par les utilisateurs externes. Vous pouvez spécifier l'adresse directement ou utiliser un objet réseau hôte. Dans cet exemple, l'adresse externe est 209.165.201.10.
- **Précisez le service public s'il est différent du service privé**, **le service public** : le service qui est en cours d'exécution sur l'adresse traduite. Précisez le service public uniquement s'il diffère du service privé. Par exemple, si le serveur Web privé fonctionne sur TCP/80 et que vous souhaitez utiliser le même port pour les utilisateurs externes, il n'est pas nécessaire de préciser le service public. Vous devez utiliser un service TCP ou UDP prédéfini si vous spécifiez un service public. Cet exemple n'utilise pas la traduction de port, alors ne sélectionnez pas cette option.

La boîte de dialogue doit ressembler à ce qui suit :



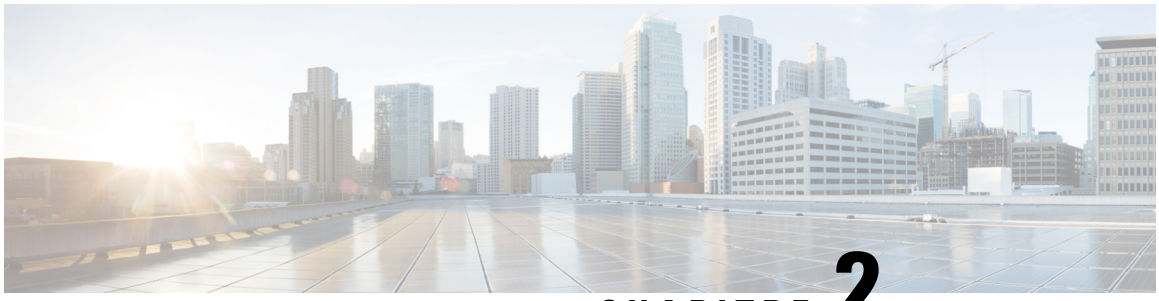
Étape 4 Cliquez sur **OK**, puis sur **Apply** (Appliquer).



PARTIE I

Contrôle d'accès

- Règles d'accès, à la page 11
- Objets pour le contrôle d'accès., à la page 33
- Listes de contrôle d'accès, à la page 49
- ASA et Cisco TrustSec, à la page 69
- Cisco Umbrella, à la page 95



CHAPITRE 2

Règles d'accès

Ce chapitre décrit comment contrôler l'accès au réseau par l'intermédiaire de l'ASA ou vers l'ASA à l'aide des règles d'accès. Vous utilisez des règles d'accès pour contrôler l'accès au réseau en mode de pare-feu routé et transparent. En mode transparent, vous pouvez utiliser à la fois des règles d'accès (pour le trafic de couche 3) et des règles EtherType (pour le trafic de couche 2).

Remarque Pour accéder à l'interface ASA pour l'accès de gestion, vous n'avez pas non plus besoin d'un critère d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès de gestion en suivant le guide de configuration sur les opérations générales.

- Contrôle d'accès au réseau, à la page 11
- Licences pour les règles d'accès, à la page 17
- Lignes directrices relatives au contrôle d'accès, à la page 17
- Configurer le contrôle d'accès, à la page 19
- Surveillance des règles d'accès, à la page 28
- Historique des règles d'accès, à la page 29

Contrôle d'accès au réseau

Les règles d'accès déterminent le trafic autorisé par l'ASA. Il existe plusieurs couches de règles qui fonctionnent ensemble pour mettre en œuvre votre politique de contrôle d'accès :

- Règles d'accès étendues (trafic de couche 3+) affectées aux interfaces : vous pouvez appliquer des ensembles de règles (ACL) distincts dans les directions entrantes et sortantes. Une règle d'accès étendue autorise ou refuse le trafic en fonction des critères du trafic de source et de destination.
- Règles d'accès étendues (trafic de couche 3+) attribuées aux interfaces virtuelles de pont (BVI; mode routé) : si vous nommez un BVI, vous pouvez appliquer des ensembles de règles distincts dans les sens entrant et sortant, et vous pouvez également appliquer des ensembles de règles aux interfaces de membre du groupe de pont. Lorsque la BVI et l'interface membre ont des règles d'accès, l'ordre de traitement dépend de la direction. En entrée, les règles d'accès de l'interface membre sont évaluées en premier, puis les règles d'accès de la BVI. En sortie, les règles de la BVI sont prises en compte en premier, puis les règles de l'interface membre.
- Règles d'accès étendues attribuées globalement : vous pouvez créer un seul ensemble de règles globales, qui sert de contrôle d'accès par défaut. Les règles globales sont appliquées après les règles d'interface.

- Règles d'accès de gestion (trafic de couche 3+) : vous pouvez appliquer un seul ensemble de règles pour couvrir le trafic dirigé vers une interface, qui est généralement le trafic de gestion. Dans l'interface de ligne de commande, il s'agit de groupes d'accès « plan de contrôle ». Pour le trafic ICMP dirigé vers le périphérique, vous pouvez également configurer les règles ICMP.
- Règles EtherType (trafic de couche 2) affectées aux interfaces (interfaces membres de groupes de ponts uniquement) : vous pouvez appliquer des ensembles de règles distincts dans les directions entrantes et sortantes. Les règles EtherType contrôlent l'accès réseau pour le trafic non IP. Une règle EtherType autorise ou refuse le trafic en fonction de l'EtherType. Vous pouvez également appliquer des règles d'accès étendues aux interfaces membres de groupes de ponts pour contrôler le trafic de couche 3+.

Renseignements généraux sur les règles

Les rubriques suivantes fournissent des renseignements généraux sur les règles d'accès et les règles EtherType.

Règles d'accès d'interface et règles d'accès globales

Vous pouvez appliquer une règle d'accès à une interface spécifique ou appliquer une règle d'accès globalement à toutes les interfaces. Vous pouvez configurer des règles d'accès globales en liaison avec les règles d'accès d'interface. Si vous le faites, les règles d'accès de l'interface entrante spécifiques sont toujours traitées avant les règles d'accès globales générales. Les règles d'accès globales s'appliquent uniquement au trafic entrant.

Règles entrantes et sortantes

Vous pouvez configurer des règles d'accès en fonction de la direction du trafic :

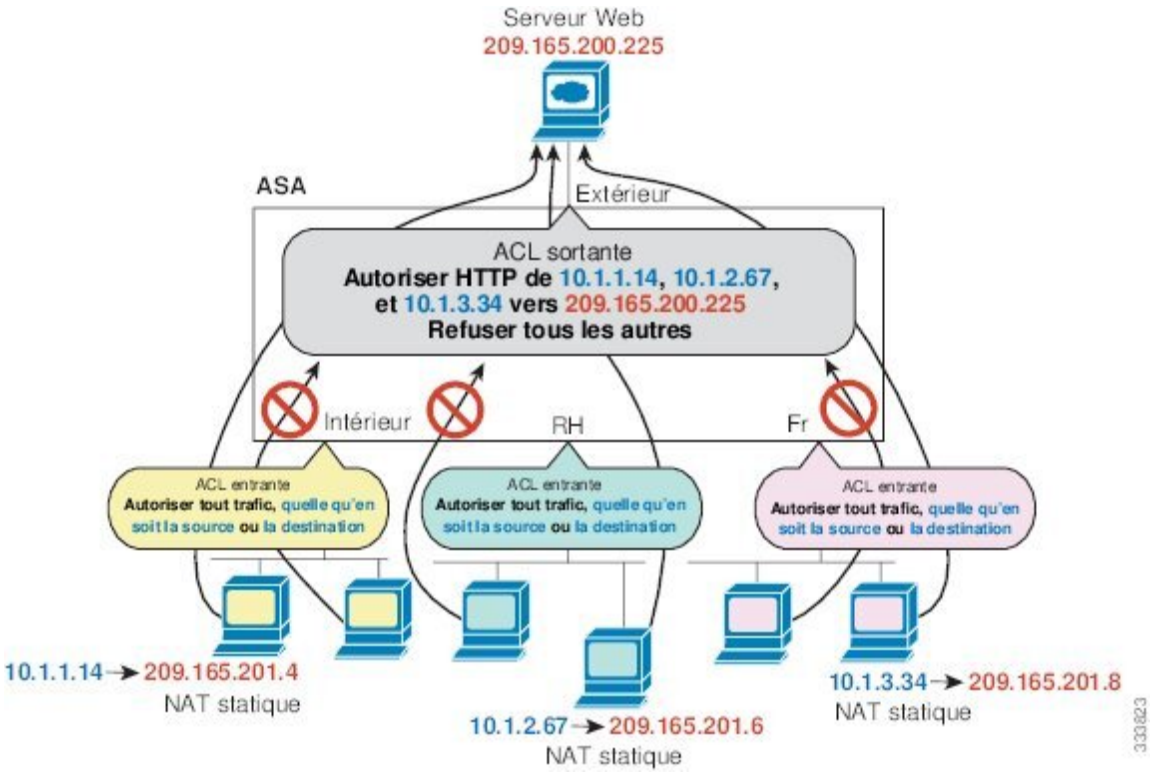
- Entrant : les règles entrantes s'appliquent au trafic lorsqu'il entre dans une interface. Les règles d'accès globales et de gestion sont toujours entrantes.
- Sortant : les règles sortantes s'appliquent au trafic lorsqu'il quitte une interface.



Remarque « entrantes » et « sortantes » font référence à l'application d'une liste de contrôle d'accès sur une interface, soit au trafic entrant dans l'ASA sur une interface, soit au trafic sortant de l'ASA sur une interface. Ces termes ne font pas référence au déplacement du trafic d'une interface de sécurité inférieure vers une interface de sécurité plus élevée, communément appelée entrante, ou d'une interface de niveau supérieur vers une interface de niveau inférieur, communément appelée sortante.

Une liste de contrôle d'accès sortante est utile, par exemple, si vous souhaitez autoriser uniquement certains hôtes des réseaux internes à accéder à un serveur Web sur le réseau externe. Plutôt que de créer plusieurs listes de contrôle d'accès entrantes pour restreindre l'accès, vous pouvez créer une seule liste de contrôle d'accès sortante qui autorise uniquement les hôtes spécifiés. (Voir la figure suivante.) L'ACL sortante empêche tout autre hôte d'atteindre le réseau externe.

Illustration 2 : ACL sortante



Ordre des règles

L'ordre des règles est important. Lorsque l'ASA décide de transférer ou d'abandonner un paquet, l'ASA teste le paquet par rapport à chaque règle dans l'ordre dans lequel les règles sont répertoriées dans l'ACL appliquée. Une fois qu'une correspondance est trouvée, aucune autre règle n'est vérifiée. Par exemple, si vous créez une règle d'accès au début qui autorise explicitement tout le trafic pour une interface, aucune autre règle n'est jamais vérifiée.

Autorisations implicites

Le trafic IPv4 et IPv6 de monodiffusion est autorisé par défaut d'une interface à sécurité supérieure vers une interface à sécurité inférieure. Cela inclut le trafic entre les interfaces routées standard et les interfaces virtuelles de pont (BVI) en mode routé.

Pour les interfaces de membre de groupes de ponts, cette autorisation implicite d'une interface de sécurité supérieure à inférieure s'applique aux interfaces du même groupe de ponts uniquement. Il n'y a pas d'autorisations implicites entre une interface de membre de groupe de ponts et une interface routée ou un membre d'un groupe de ponts différent.

Les interfaces de membre de groupe de ponts (mode routé ou transparent) autorisent également les éléments suivants par défaut :

- ARP dans les deux sens. (Vous pouvez contrôler le trafic ARP à l'aide de l'inspection ARP, mais vous ne pouvez pas le contrôler à l'aide de la règle d'accès.)
- BPDU dans les deux sens. (Vous pouvez les contrôler à l'aide des règles Ethertype.)

Pour les autres trafics, vous devez utiliser une règle d'accès étendue (IPv4 et IPv6) ou une règle EtherType (non IP).

Refus implicite

Les listes de contrôle d'accès ont un refus implicite à la fin de la liste, donc, sauf si vous l'autorisez explicitement, le trafic ne peut pas passer. Par exemple, si vous souhaitez autoriser tous les utilisateurs à accéder à un réseau par l'intermédiaire de l'ASA, à l'exception d'adresses particulières, vous devez refuser les adresses particulières, puis autoriser tous les autres.

Pour les listes de contrôle d'accès de gestion (plan de commande), qui contrôlent le trafic vers le boîtier, il n'y a pas de refus implicite à la fin d'un ensemble de règles de gestion pour une interface. Au lieu de cela, toute connexion qui ne correspond pas à une règle d'accès de gestion est ensuite évaluée par des règles de contrôle d'accès normales.

Pour les listes de contrôle d'accès EtherType, le refus implicite à la fin de la liste de contrôle d'accès n'affecte pas le trafic IP ni les ARP ; par exemple, si vous autorisez EtherType 8037, le refus implicite à la fin de l'ACL ne bloque pas le trafic IP que vous avez précédemment autorisé avec une liste de contrôle d'accès étendue (ou implicitement autorisé d'une interface de haute sécurité à une interface de sécurité faible). Toutefois, si vous refusez explicitement tout le trafic avec une règle EtherType, le trafic IP et ARP est refusé; seul le trafic de protocole physique, tel que la négociation automatique, est toujours autorisé.

Si vous configurez une règle d'accès globale, le refus implicite survient *après* le traitement de la règle globale. Consultez l'ordre des opérations suivant :

1. Critères d'accès de l'interface
2. Pour les interfaces de membre de groupes de ponts, la règle d'accès de l'interface virtuelle de pont (BVI).
3. Critères d'accès globaux
4. Refus implicite.

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).

Interfaces de niveau de sécurité identiques et règles d'accès

Chaque interface a un niveau de sécurité, et la vérification du niveau de sécurité est effectuée avant que les règles d'accès ne soient prises en compte. Ainsi, même si vous autorisez une connexion dans une règle d'accès, elle peut être bloquée en raison d'une vérification de même niveau de sécurité au niveau de l'interface. Vous pouvez vous assurer que votre configuration autorise les connexions au même niveau de sécurité afin que vos règles d'accès soient toujours prises en compte dans les décisions en matière d'autorisation ou de refus.

- Les connexions entre les interfaces d'entrée et de sortie de même niveau de sécurité sont soumises à la vérification same-security-traffic inter-interface.

  Pour autoriser ces connexions, entrez la commande **same-security-traffic permit inter-interface**.

  Pour autoriser ces connexions, choisissez **Configuration** > **Device Setup (Configuration du périphérique)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** puis sélectionnez l'option

Enable traffic between two or more interfaces which are configured with the same security levels (Activer le trafic entre deux interfaces ou plus qui sont configurées avec les mêmes niveaux de sécurité).

- Les connexions avec les mêmes interfaces d'entrée et de sortie sont soumises à la même vérification intra-interface de sécurité et de trafic.

  Pour autoriser ces connexions, entrez la commande **same-security-traffic permit intra-interface**.

  Pour autoriser ces connexions, choisissez **Configuration Device Setup (Configuration du périphérique)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** , puis sélectionnez l'option **Enable traffic between two or more hosts connected to the same interface (Activer le trafic entre deux hôtes ou plus connectés à la même interface)**.

Règles d'accès étendues

Cette section décrit les renseignements sur les règles d'accès étendues.

Règles d'accès étendues pour le retour du trafic

Pour les connexions TCP, UDP et SCTP en mode routé et transparent, vous n'avez pas besoin de règle d'accès pour autoriser le retour, car l'ASA autorise tout le trafic de retour pour les connexions bidirectionnelles établies.

Pour les protocoles sans connexion tels que ICMP, cependant, l'ASA établit des sessions unidirectionnelles. Vous avez donc besoin de règles d'accès pour autoriser ICMP dans les deux sens (en appliquant des listes de contrôle d'accès aux interfaces de source et de destination), ou vous devez activer le moteur d'inspection ICMP. Le moteur d'inspection ICMP traite les sessions ICMP comme des connexions bidirectionnelles. Par exemple, pour contrôler ping, spécifiez **echo-reply** (**0**) (ASA to host) ou **echo** (**8**) (host to ASA).

Autoriser le trafic de diffusion et de multidiffusion

En mode de pare-feu routé, le trafic de diffusion et de multidiffusion est bloqué même si vous l'autorisez dans un critère d'accès, y compris les protocoles de routage dynamique non pris en charge et le DHCP. Vous devez configurer les protocoles de routage dynamique ou le relais DHCP pour autoriser ce trafic.

Pour les interfaces membres du même groupe de ponts en mode transparent ou de pare-feu routé, vous pouvez autoriser tout trafic IP à l'aide des règles d'accès.



Remarque Étant donné que ces types spéciaux de trafic sont sans connexion, vous devez appliquer une règle d'accès aux interfaces de trafic entrant et sortant, afin que le trafic de retour soit autorisé à passer.

Le tableau suivant répertorie les types de trafic courants que vous pouvez autoriser à l'aide de règles d'accès entre les interfaces membres du même groupe de ponts.

Tableau 1 : Trafic spécial pour les règles d'accès entre les membres d'un même groupe de ponts

Type de trafic	Protocole ou port	Notes
DHCP (protocole de configuration dynamique des hôtes)	Ports UDP 67 et 68	Si vous activez le serveur DHCP, l'ASA ne transmet pas les paquets DHCP.
EIGRP	Protocole 88	—
OSPF	Protocole 89	—
Flux de multidiffusion	Les ports UDP varient selon l'application.	Les flux de multidiffusion sont toujours destinés à une adresse de classe D (224.0.0.0 à 239.x.x.x).
RIP (v1 ou v2)	Port UDP 520	—

Règles d'accès de gestion

Vous pouvez configurer des règles d'accès qui contrôlent le trafic de gestion destiné à l'ASA. Les règles de contrôle d'accès pour le trafic de gestion vers le boîtier (comme les connexions HTTP, Telnet et SSH à une interface) ont une priorité plus élevée qu'une règle d'accès de gestion . Par conséquent, ce trafic de gestion autorisé sera autorisé à entrer même s'il est explicitement refusé par la liste de contrôle d'accès vers le boîtier.

Contrairement aux règles d'accès standard, il n'y a pas de refus implicite à la fin d'un ensemble de règles de gestion pour une interface. Au lieu de cela, toute connexion qui ne correspond pas à une règle d'accès de gestion est ensuite évaluée par des règles de contrôle d'accès normales.

Vous pouvez également utiliser des règles ICMP pour contrôler le trafic ICMP vers le périphérique. Utilisez des règles d'accès étendues normales pour contrôler le trafic ICMP qui passe par le périphérique.

Règles EtherType

Cette section décrit les règles EtherType.

EtherTypes pris en charge et autres types de trafic

Une règle EtherType contrôle les éléments suivants :

- EtherType identifié par un numéro hexadécimal de 16 bits, y compris les types courants IPX et MPLS de monodiffusion ou de multidiffusion.
- Trames Ethernet V2.
- Les BPDU, qui sont autorisés par défaut. Les BPDU sont encapsulés dans le protocole SNAP et l'ASA est conçu pour gérer spécifiquement les BPDU.
- BPDU de port de liaison (propriétaire Cisco). Les BPDU de ligne principale ont des informations VLAN dans la charge utile, de sorte que l'ASA modifie la charge utile avec le VLAN sortant si vous autorisez les BPDU.
- Intermediate System-to-Intermediate System (IS-IS)

- Le paquet de contrôle de liaison logique IEEE 802.2. Vous pouvez contrôler l'accès en fonction de l'adresse du point d'accès du service de destination.

Les types de trafic suivants ne sont pas pris en charge :

- Trames au format 802.3 : ces trames ne sont pas gérées par la règle, car elles utilisent un champ de longueur par opposition à un champ de type.

Règles EtherType pour le retour du trafic

Comme les EtherTypes sont sans connexion, vous devez appliquer la règle aux deux interfaces si vous souhaitez que le trafic passe dans les deux sens.

Autoriser MPLS

Si vous autorisez MPLS, assurez-vous que les connexions TCP du protocole de distribution d'étiquette et du protocole de distribution de balise sont établies par l'ASA en configurant les deux routeurs MPLS connectés à l'ASA pour utiliser l'adresse IP sur l'interface de l'ASA comme ID de routeur pour les sessions LDP ou TDP. (LDP et TDP permettent aux routeurs MPLS de négocier les étiquettes (adresses) utilisées pour transférer les paquets.)

Sur les routeurs Cisco IOS, saisissez la commande appropriée pour votre protocole, LDP ou TDP. L' *interface* est l'interface connectée à l'ASA.

mpls ldp router-id *interface* **force**

Ou

tag-switching tdp router-id *interface* **force**

Licences pour les règles d'accès

Les règles de contrôle d'accès ne nécessitent pas de licence spéciale.

Cependant, pour utiliser **sctp** comme protocole dans une règle, vous devez avoir une licence d'opérateur.

Lignes directrices relatives au contrôle d'accès

Directives IPv6

Prend en charge IPv6. (9.0 et versions ultérieures) Les adresses de source et de destination peuvent inclure n'importe quelle combinaison d'adresses IPv4 et IPv6. Pour les versions antérieures à la version 9.0, vous devez créer une règle d'accès IPv6 distincte.

Lignes directrices d'ACL par utilisateur

- La liste de contrôle d'accès par utilisateur utilise la valeur dans la commande **timeout uauth**, mais elle peut être remplacée par la valeur de délai d'expiration de session par utilisateur d'AAA.
- Si le trafic est refusé en raison d'une liste de contrôle d'accès par utilisateur, le message syslog 109025 est enregistré. Si le trafic est autorisé, aucun message syslog n'est généré. L'option **log** dans la liste de contrôle d'accès par utilisateur n'a aucun effet.

Directives et limites additionnelles

- Au fil du temps, votre liste de règles d'accès peut s'allonger pour inclure de nombreuses règles obsolètes. À la longue, les listes de contrôle d'accès des groupes d'accès peuvent devenir si importantes qu'elles ont une incidence sur les performances globales du système. Si vous constatez que le système rencontre des problèmes pour envoyer des messages syslog, communiquer pour la synchronisation de basculement, établir et maintenir les connexions d'accès de gestion SSH/HTTPS, etc., vous devrez peut-être élaguer vos règles d'accès. En général, vous devez maintenir activement vos listes de règles pour supprimer les règles obsolètes, les règles qui ne sont jamais touchées, les objets FQDN qui ne peuvent plus être résolus, etc. Envisagez également de mettre en œuvre la recherche de groupe d'objets.

- La recherche de groupe d'objets est activée par défaut pour les nouveaux déploiements.

  Vous pouvez réduire la mémoire requise pour la recherche des règles d'accès en activant la recherche de groupe d'objets, mais cela se fait au détriment des performances de recherche et d'une utilisation accrue du processeur. Lorsqu'elle est activée, la recherche par groupe d'objets ne développe pas les objets de réseau ou de service, mais recherche dans les critères d'accès les correspondances basées sur les définitions de ces groupes. Vous pouvez définir cette option en cliquant sur le bouton **Advanced** (Avancé) sous le tableau des règles d'accès.

  Vous pouvez utiliser la commande **object-group-search threshold** pour activer un seuil afin d'éviter la dégradation des performances. Lorsqu'elle fonctionne avec un seuil, pour chaque connexion, les adresses IP source et de destination sont comparées aux objets réseau. Si le nombre d'objets correspondant à l'adresse source multiplié par le nombre correspondant à l'adresse de destination dépasse 10 000, la connexion est abandonnée. Configurez vos règles pour éviter un nombre excessif de correspondances.



Remarque La recherche de groupe d'objets fonctionne uniquement avec les objets de réseau et de service. Il ne fonctionne pas avec des groupes de sécurité ou des objets utilisateur. N'activez pas cette fonctionnalité si les listes de contrôle d'accès comprennent des groupes de sécurité. Le résultat peut être des listes de contrôle d'accès inactives ou un autre comportement inattendu.

- Vous pouvez améliorer les performances et la fiabilité du système en utilisant le modèle de validation transactionnelle pour les groupes d'accès. Cependant, la validation transactionnelle n'est pas recommandée si vous utilisez des objets FQDN pour des noms d'hôte dont la résolution peut changer fréquemment, car la compilation du groupe d'accès pourrait ne jamais aboutir complètement. Pour plus d'informations, consultez le chapitre sur les paramètres de base dans le guide de configuration des opérations générales. L'option se trouve sous **Configurations (Configurations) > Device Management (gestion des périphériques) > Advanced (Avancé) > Rule Engine (moteur de règles)**.

- Dans ASDM, les descriptions de règles sont basées sur les remarques de liste d'accès qui précèdent la règle dans l'ACL; pour les nouvelles règles que vous créez dans ASDM, toutes les descriptions sont également configurées en tant que remarques avant la règle associée. Cependant, le traceur de paquets dans ASDM correspond à la remarque configurée après la règle de correspondance dans l'interface de ligne de commande.

- Lorsque vous saisissez plusieurs éléments dans l'adresse source ou de destination, ou dans le service source ou de destination, ASDM crée automatiquement un groupe d'objets pour eux avec le préfixe DM_INLINE. Ces objets sont automatiquement développés jusqu'à leurs composants dans la vue du tableau de règles, mais vous pouvez voir les noms des objets si vous désélectionnez la préférence **Auto-expand network and service objects with specified prefix** (Développer automatiquement les

objets réseau et de service avec le préfixe spécifié) du tableau de règles dans **Tools (Outils)** > **Preferences (Préférences)**.

- 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.

  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.
  - 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.

Configurer le contrôle d'accès

Les rubriques suivantes expliquent comment configurer le contrôle d'accès.

Configurer les règles d'accès

Pour appliquer une règle d'accès, procédez comme suit :

Procédure

Étape 1 Choose **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Règles d'accès)**.

Les règles sont classées par interface et direction, avec un groupe distinct pour les règles globales. Si vous configurez des règles d'accès de gestion, elles sont répétées sur cette page. Ces groupes sont équivalents à la liste de contrôle d'accès étendue qui est créée et affectée à l'interface ou globalement en tant que groupe d'accès. Ces ACL apparaissent également sur la page ACL Manager (Gestionnaire d'ACL).

Étape 2 Effectuez l'une des actions suivantes :

- Pour ajouter une nouvelle règle, choisissez Add (Ajouter) > **Add Access Rule** (Ajouter une règle d'accès).
- Pour insérer une règle à un emplacement spécifique dans un conteneur, sélectionnez une règle existante et choisissez **Add (Ajouter) > Insert (Insérer)** pour ajouter la règle au-dessus, ou choisissez **Add (Ajouter) > Insert After (Insérer après)**.
- Pour modifier une règle, sélectionnez-la et cliquez sur **Edit** (Modifier).

Étape 3 Renseignez les propriétés de la règle. Les principales options à sélectionner sont :

- **Interface** : l'interface à laquelle la règle s'applique. Sélectionnez Any (Tous) pour créer une règle globale. Pour les groupes de ponts en mode routé, vous pouvez créer des règles d'accès pour l'interface virtuelle de pont (BVI) et chaque interface de membre de groupe de ponts.
- **Action : Permit/Deny (Autoriser/Refuser)** : précisez si vous autorisez le trafic décrit ou si vous le bloquez.
- **Source/Destination criteria** (Critères source/destination) : définissez la source (adresse d'origine) et la destination (adresse cible du flux de trafic). Vous configurez généralement des adresses IPv4 ou IPv6 d'hôtes ou de sous-réseaux, que vous pouvez représenter avec des groupes d'objets réseau ou des groupes d'objets de service réseau. Vous pouvez également préciser un nom d'utilisateur ou de groupe d'utilisateurs pour la source. En outre, vous pouvez utiliser le champ Service pour identifier le type spécifique de trafic si vous souhaitez cibler la règle de manière plus étroite que tout le trafic IP. Si vous incluez des spécifications de service dans un objet de service réseau, précisez IP dans le champ Service. Si vous mettez en œuvre Cisco TrustSec, vous pouvez utiliser des groupes de sécurité pour définir la source et la destination.

Pour des informations détaillées sur les options, consultez Propriétés de la règle d'accès, à la page 20.

Lorsque vous avez terminé de définir la règle, cliquez sur **OK** pour l'ajouter au tableau.

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer la règle d'accès dans votre configuration.

Propriétés de la règle d'accès

Lorsque vous ajoutez ou modifiez une règle d'accès, vous pouvez configurer les propriétés suivantes. Dans de nombreux champs, vous pouvez cliquer sur le bouton « ... » à droite de la zone d'édition pour sélectionner, créer ou modifier des objets disponibles pour le champ.

Interface

L'interface à laquelle la règle s'applique. Sélectionnez Any (Tous) pour créer une règle globale. Pour les groupes de ponts en mode routé, vous puvez sélectionner l'interface virtuelle de pont (BVI) ou les interfaces de membre du groupe de ponts.

Action : Autoriser/refuser

Indique si vous autorisez le trafic décrit ou si vous le refusez.

Critères de source

Les caractéristiques de l'initiateur du trafic que vous tentez de mettre en correspondance. Vous devez configurer la source, mais les autres propriétés sont facultatives.

Source

Adresse IPv4 ou IPv6 de la source. La valeur par défaut est **any**, qui correspond à toutes les adresses IPv4 ou IPv6 ; vous pouvez utiliser **any4** pour cibler IPv4 uniquement, ou **any6** pour cibler IPv6 uniquement. Vous pouvez spécifier une adresse d'hôte unique (comme 10.100.10.5 ou 2001:DB8::0DB8:800:200C:417A), un sous-réseau (au format 10.100.10.0/24 ou 10.100.10.0/255.255.255.0, ou pour IPv6, 2001:DB8:0:CD30::/60), le nom d'un objet réseau ou d'un groupe d'objets réseau, le nom d'un groupe d'objets de service réseau, ou le nom d'une interface.

Utilisateur

Si vous activez le pare-feu d'identité, vous pouvez spécifier un utilisateur ou un groupe d'utilisateurs comme source du trafic. L'adresse IP que l'utilisateur utilise actuellement correspondra à la règle. Vous pouvez spécifier un nom d'utilisateur (DOMAIN\user), un groupe d'utilisateurs (DOMAIN\group, notez que le double \ indique un nom de groupe) ou un groupe d'objets utilisateur. Pour ce champ, il est beaucoup plus facile de cliquer sur «**...**» pour sélectionner des noms à partir de votre groupe de serveurs AAA que de les taper.

Groupe sécurité

Si vous activez Cisco Trustsec, vous pouvez spécifier un nom ou une balise de groupe de sécurité (1 à 65 533), ou un objet de groupe de sécurité.

More Options (Plus d'options) > Source Service (Service source)

Notez que si vous définissez le service source, le protocole du service de destination doit lui correspondre (par exemple, TCP, avec ou sans définition de port). En règle générale, vous définissez le service de destination uniquement et non le service source.

Critères de destination

Les caractéristiques de la cible du trafic que vous tentez de mettre en correspondance. Vous devez configurer la destination, mais les autres propriétés sont facultatives.

Destination

L'adresse IPv4 ou IPv6 de destination. La valeur par défaut est **any**, qui correspond à toutes les adresses IPv4 ou IPv6 ; vous pouvez utiliser **any4** pour cibler IPv4 uniquement, ou **any6** pour cibler IPv6 uniquement. Vous pouvez spécifier une adresse d'hôte unique (comme 10.100.10.5 ou 2001:DB8::0DB8:800:200C:417A), un sous-réseau (au format 10.100.10.0/24 ou 10.100.10.0/255.255.255.0, ou pour IPv6, 2001:DB8:0:CD30::/60), le nom d'un objet réseau ou d'un groupe d'objets réseau, le nom d'un groupe d'objets de service réseau, ou le nom d'une interface.

Groupe sécurité

Si vous activez Cisco Trustsec, vous pouvez spécifier un nom ou une balise de groupe de sécurité (1-65533), ou un objet de groupe de sécurité.

Service

Le protocole du trafic, par exemple IP, TCP, UDP, et éventuellement les ports pour TCP, UDP ou SCTP. La valeur par défaut est IP, mais vous pouvez sélectionner un protocole plus précis pour cibler le trafic avec plus de granularité. En règle générale, vous sélectionnez un type d'objet de service. Pour TCP, UDP, et SCTP, vous pouvez spécifier des ports, par exemple, tcp/80, tcp/http, tcp/10-20 (pour une plage de ports), tcp-udp/80 (correspond à tout trafic TCP ou UDP sur le port 80), sctp/diameter, etc. Si vous incluez des spécifications de service dans un objet de service réseau, précisez IP dans le champ Service.

Description

Une explication de l'objectif de la règle, jusqu'à 100 caractères par ligne. Vous pouvez saisir plusieurs lignes; chaque ligne est ajoutée en tant que remarque dans l'interface de ligne de commande, et les remarques sont placées avant la règle.



Remarque Si vous ajoutez des remarques avec des caractères non anglais sur une plateforme (comme Windows), puis essayez de les supprimer d'une autre plateforme (comme Linux), vous ne pourrez peut-être pas les modifier ou les supprimer, car les caractères d'origine peuvent ne pas être correctement reconnus. Cette limitation est due à une dépendance de plateforme sous-jacente qui code différents caractères linguistiques de différentes manières.

Enable Logging (Activer la journalisation) ; Logging Level (Niveau de journalisation) ; More Options (Plus d'options) > Logging Interval (Intervalle de journalisation)

Les options de journalisation définissent la façon dont les messages syslog seront générés pour les règles. Vous pouvez implémenter les options de journalisation suivantes :

Désélectionnez Enable Logging (Activer la journalisation)

Cela désactivera la journalisation pour la règle. Aucun message de journal système d'aucun type ne sera émis pour les connexions qui correspondent à cette règle.

Sélectionnez Enable Logging (Activer la journalisation) avec Logging Level (Niveau de journalisation) = Default (Par défaut)

Il fournit la journalisation par défaut pour les règles. Le message de journal système 106023 est émis pour chaque connexion refusée. Si le périphérique est soumis à une attaque, la fréquence d'émission de ce message peut avoir une incidence sur les services.

Sélectionnez Enable Logging (Activer la journalisation) avec Non-Default Logging Level (Niveau de journalisation autre que celui par défaut)

Cela fournit un message de journal système résumé, 106100, au lieu de 106023. Le message 106100 est émis lors du premier impact, puis à chaque intervalle configuré dans **Plus d'options > Intervalle de journalisation** (par défaut toutes les 300 secondes, vous pouvez spécifier 1-600), montrant le nombre d'impacts pendant cet intervalle. Le niveau de journalisation conseillé est **Informational** (Informations).

Le résumé des messages de refus peut réduire l'impact des attaques et éventuellement faciliter l'analyse des messages. Si vous subissez une attaque par déni de service, vous pourriez voir le message 106101, qui indique que le nombre de flux de refus en cache utilisés pour produire le nombre de correspondances pour le message 106100 a dépassé le maximum pour un intervalle. À ce stade, le périphérique arrête de collecter des statistiques jusqu'au prochain intervalle pour maîtriser l'attaque.

Indique si la règle s'applique à la direction In (Entrée) ou Out (Sortie).

Si la règle s'applique à la direction **In** ou **Out**. **In** est la valeur par défaut et il s'agit de la seule option pour les règles d'accès globales et de gestion.

More Options (Plus d'options) > Enable Rule (Activer la règle)

Si la règle est active sur le périphérique. Les règles désactivées s'affichent avec du texte barré dans le tableau de règles. La désactivation d'une règle vous permet d'arrêter son application au trafic sans la supprimer, de sorte que vous pouvez la réactiver ultérieurement si vous décidez que vous en avez besoin.

More Options (Plus d'options) > Time Range (Plage de temps)

Le nom de l'objet de plage temporelle qui définit les heures du jour et les jours de la semaine où la règle doit être active. Si vous ne spécifiez pas de plage temporelle, la règle est toujours active.

Configurer les options avancées pour les règles d'accès

Les options de règles d'accès avancées vous permettent de personnaliser certains aspects du comportement des règles, mais ces options ont des valeurs par défaut appropriées dans la plupart des cas.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Règles d'accès)** .

Étape 2 Cliquez sur le bouton **Advanced** (Avancé) sous le tableau de règles.

Étape 3 Configurez les options suivantes :

- **Advanced Logging Settings** (Paramètres de journalisation avancée) : si vous configurez une journalisation différente des valeurs par défaut, le système met en cache les flux refusés afin d'établir des statistiques pour le message 106100, comme expliqué dans Évaluation des messages Syslog pour les règles d'accès, à la page 28. Pour éviter une consommation illimitée des ressources mémoire et processeur, l'ASA limite le nombre de flux *refusés* simultanés, car ceux-ci peuvent indiquer une attaque. Le message 106101 est généré lorsque cette limite est atteinte. Vous pouvez contrôler les paramètres suivants relatifs au message 106101.
  - Nombre maximal de flux refusés : nombre maximal de flux refusés autorisés avant que l'ASA cesse de les mettre en cache, entre 1 et 4 096. La valeur par défaut est 4 096.
  - Intervalle d'alerte : la durée (de 1 à 3 600 secondes) entre l'émission du message de journal système 106101, qui indique que le nombre maximal de flux de refus a été atteint. La valeur par défaut est de 300 secondes.

- **Per User Override (tableau de remplacement d'utilisateur)** : s'il faut autoriser une liste de contrôle d'accès d'utilisateur dynamique téléchargée pour l'autorisation de l'utilisateur à partir d'un serveur RADIUS de remplacer l'ACL attribuée à l'interface. Par exemple, si l'ACL de l'interface refuse tout le trafic provenant de 10.0.0.0, mais que l'ACL dynamique autorise tout le trafic provenant de 10.0.0.0, l'ACL dynamique remplace l'ACL de l'interface pour cet utilisateur. Cochez la case **Per User Override** (Remplacement par utilisateur) pour chaque interface qui doit autoriser les remplacements par l'utilisateur (direction entrante uniquement). Si la fonctionnalité de remplacement par utilisateur est désactivée, la règle d'accès fournie par le serveur RADIUS est combinée avec la règle d'accès configurée sur cette interface.

  Par défaut, le trafic VPN d'accès à distance n'est pas comparé aux ACL d'interface. Toutefois, si vous désélectionnez l'option **Enable inbound VPN sessions to bypass interface access lists (Activer les sessions VPN entrantes pour** contourner les listes d'accès d'interface) dans Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Connection Profiles (Profils de connexion) Secure Client (services client sécurisés), le comportement dépend de la présence d'un filtre VPN dans la stratégie de groupe (voir le champ Filter (Filtre) dans Configuration (Configuration) > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Group Policies (Stratégies de groupe) > Add/Edit (Ajouter/Modifier) > General (Général) > More Options (Plus d'options)), ainsi que du paramètre Per User Override.
  - Aucun remplacement par utilisateur, pas de filtre VPN : le trafic est comparé à l'ACL de l'interface.

- Aucun remplacement par utilisateur, filtre VPN : le trafic est d'abord comparé à l'ACL de l'interface, puis au filtre VPN.
- Par remplacement d'utilisateur, filtre VPN : le trafic est comparé au filtre VPN uniquement.

- **Object Group Search Setting** (Paramètre de recherche des groupes d'objets) : vous pouvez réduire la mémoire requise pour rechercher les règles d'accès utilisant des groupes d'objets en sélectionnant **Enable Object Group Search Algorithm** (Activer l'algorithme de recherche des groupes d'objets), mais cela se fait au détriment des performances de recherche des règles. Lorsqu'elle est activée, la recherche par groupe d'objets ne développe pas les objets de réseau, mais recherche dans les règles d'accès les correspondances basées sur les définitions de ces groupes.

  Sélectionnez **Enable Object Group Search Threshold** (Activer le seuil de recherche des groupes d'objets) afin de définir un seuil permettant d'éviter une dégradation des performances. Lorsqu'elle fonctionne avec un seuil, pour chaque connexion, les adresses IP source et de destination sont comparées aux objets réseau. Si le nombre d'objets correspondant à l'adresse source multiplié par le nombre correspondant à l'adresse de destination dépasse 10 000, la connexion est abandonnée. Configurez vos règles pour éviter un nombre excessif de correspondances.

  Remarque
  La recherche de groupe d'objets fonctionne uniquement avec les objets de réseau et de service. Elle ne fonctionne pas avec des objets de groupe de sécurité. N'activez pas cette fonctionnalité si les listes de contrôle d'accès comprennent des groupes de sécurité. Le résultat peut être des listes de contrôle d'accès inactives ou un autre comportement inattendu.

- **Forward Reference Setting** (Paramètre de référence anticipée) **— (Versions antérieures à 7.18 uniquement.)** Normalement, vous ne pouvez pas référencer un objet ou un groupe d'objets qui n'existe pas dans une ACL ou un groupe d'objets, ni supprimer un objet actuellement référencé. Vous ne pouvez pas non plus référencer une liste de contrôle d'accès qui n'existe pas dans une commande **access-group** (pour appliquer les règles d'accès). Cependant, vous pouvez modifier ce comportement par défaut afin d'autoriser les références anticipées (« forward references ») vers des objets ou des ACL avant leur création. Jusqu'à ce que vous créiez les objets ou les listes de contrôle d'accès, toutes les règles ou tous les groupes d'accès qui les référencent sont ignorés. Sélectionnez **Enable the Forward Reference of Objects and Object-Groups** (Activer les références anticipées des objets et des groupes d'objets) pour activer cette fonctionnalité. Sachez que si vous activez le référencement vers l'avant, ASDM ne peut pas faire la différence entre une référence type à un objet existant et une référence vers l'avant.

  Remarque
  Ce paramètre est activé par défaut et n'est plus configurable à partir de l'ASA 9.18(1).

Étape 4 Cliquez sur **OK**.

Configurer les règles d'accès de gestion

Vous pouvez configurer une liste de contrôle d'accès d'interface qui contrôle le trafic de gestion jusqu'au boîtier d'un homologue spécifique (ou d'un ensemble d'homologues) vers l'ASA. Un scénario dans lequel ce type d'ACL serait utile est lorsque vous souhaitez bloquer les attaques par déni de service IKE.

Contrairement aux règles d'accès standard, il n'y a pas de refus implicite à la fin d'un ensemble de règles de gestion pour une interface. Au lieu de cela, toute connexion qui ne correspond pas à une règle d'accès de gestion est ensuite évaluée par des règles de contrôle d'accès normales.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **Règles d'accès de gestion**.

Les règles sont classées par interface. Chaque groupe équivaut à la liste de contrôle étendue qui est créée et affectée à l'interface en tant qu'ACL de plan de commande. Ces listes de contrôle d'accès apparaissent également dans les pages Access Rules (Règles d'accès) et ACL Manager (Gestionnaire d'ACL).

Étape 2 Effectuez l'une des actions suivantes :

- Pour ajouter une nouvelle règle, choisissez **Add (Ajouter) > Add Management Access Rule (Ajouter une règle d'accès de gestion)**.
- Pour insérer une règle à un emplacement spécifique dans un conteneur, sélectionnez une règle existante et choisissez **Add (Ajouter) > Insert (Insérer)** pour ajouter la règle au-dessus, ou choisissez **Add (Ajouter) > Insert After (Insérer après)**.
- Pour modifier une règle, sélectionnez-la et cliquez sur **Edit** (Modifier).

Étape 3 Renseignez les propriétés de la règle. Les principales options à sélectionner sont :

- **Interface** : l'interface à laquelle la règle s'applique. Pour les groupes de ponts en mode routé, vous pouvez créer des règles d'accès pour l'interface virtuelle de pont (BVI) et chaque interface de membre de groupe de ponts.
- **Action : Permit/Deny (Autoriser/Refuser)** : précisez si vous autorisez le trafic décrit ou si vous le bloquez.
- **Source/Destination criteria** (Critères source/destination) : définissez la source (adresse d'origine) et la destination (adresse cible du flux de trafic). Vous configurez généralement l'adresse IPv4 ou IPv6 des hôtes ou des sous-réseaux, que vous pouvez représenter avec des groupes d'objets réseau. Vous pouvez également préciser un nom d'utilisateur ou de groupe d'utilisateurs pour la source. En outre, vous pouvez utiliser le champ Service pour identifier le type spécifique de trafic si vous souhaitez cibler la règle de manière plus étroite que tout le trafic IP. Si vous mettez en œuvre Cisco TrustSec, vous pouvez utiliser des groupes de sécurité pour définir la source et la destination.

Pour des informations détaillées sur les options, consultez Propriétés de la règle d'accès, à la page 20.

Lorsque vous avez terminé de définir la règle, cliquez sur **OK** pour l'ajouter au tableau.

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer la règle dans votre configuration.

Configurer les règles EtherType

Les règles EtherType s'appliquent au trafic de couche 2 non IP sur les interfaces membres de groupes de ponts (en mode de pare-feu routé ou transparent). Vous pouvez utiliser ces règles pour autoriser ou abandonner le trafic en fonction de la valeur EtherType dans le paquet de couche 2. Les règles EtherType vous permettent de contrôler le flux du trafic non IP dans l'ASA.

Vous pouvez appliquer des règles d'accès étendues et EtherType à une interface membre d'un groupe de ponts. Les règles EtherType prévalent sur les règles d'accès étendues.

Procédure

Étape 1 Choisissez **ConfigurationFirewall (Pare-feu)EtherType Rules (Règles EtherType)**

Les règles sont classées par interface et par direction. Chaque groupe équivaut à l'ACL EtherType créée et affectée à l'interface.

Étape 2 Effectuez l'une des actions suivantes :

- Pour ajouter une nouvelle règle, choisissez **Add (Ajouter)** > **Add EtherType Rule (Ajouter une règle EtherType)** .
- Pour insérer une règle à un emplacement spécifique dans un conteneur, sélectionnez une règle existante et choisissez **Add (Ajouter)** > **Insert (Insérer)** pour ajouter la règle au-dessus, ou choisissez **Add (Ajouter)** > **Insert After (Insérer après)** .
- Pour modifier une règle, sélectionnez-la et cliquez sur **Edit** (Modifier).

Étape 3 Renseignez les propriétés de la règle. Les principales options à sélectionner sont :

- **Interface** : l'interface à laquelle la règle s'applique.
- **Action : Permit/Deny (Autoriser/Refuser)** : précisez si vous autorisez le trafic décrit ou si vous le bloquez.
- EtherType : vous pouvez mettre en correspondance le trafic en utilisant les options suivantes :
  - **any** : correspond à tout le trafic.
  - **bpdu** : unités de données de protocole de pont, qui sont autorisées par défaut. Lorsque vous appliquez la configuration, ce mot-clé est converti en **dsap bpdu** sur le périphérique.
  - **dsap** : l'adresse du point d'accès au service de destination du paquet de contrôle de liaison logique IEEE 802.2. Vous devez également inclure l'adresse que vous souhaitez autoriser ou refuser en hexadécimal, de 0x01 à 0xff, dans **DSAP Value** (Valeur DSAP). Voici les valeurs de certaines adresses courantes :
    - **0x42** : unités de données de protocole de pont (BPDU). Lorsque vous appliquez la configuration, celle-ci est convertie en **dsap bpdu** sur le périphérique.
    - **0xe0** : Internet Packet Exchange (IPX) 802.2 LLC. Lorsque vous appliquez la configuration, celle-ci est convertie en **dsap ipx** sur le périphérique.
    - **0xfe** : Intermediate System to Intermediate System (IS-IS). Lorsque vous appliquez la configuration, celle-ci est convertie en **dsap isis** sur le périphérique.
    - **0xff** : format brut IPX 802.3. Lorsque vous appliquez la configuration, celle-ci est convertie en **dsap raw-ipx** sur le périphérique.
  - **eii-ipx** : format IPX Ethernet II, EtherType 0x8137.

- **ipx** : Internet Packet Exchange (IPX). Ce mot-clé est un raccourci pour configurer trois règles distinctes, pour **dsap ipx** , **dsap raw-ipx** , et **eii-ipx** . La conversion est effectuée lorsque vous appliquez la configuration au périphérique.
- **isis** : Intermediate System to Intermediate System (IS-IS). Lorsque vous appliquez la configuration, ce mot-clé est converti en **dsap isis** sur le périphérique.
- **mpls-multicast** : multidiffusion MPLS.
- **mpls-unicast :** monodiffusion MPLS.
- *hex_number* —Tout EtherType qui peut être identifié par un nombre hexadécimal de 16 bits de 0x600 à 0xffff. Consultez la RFC 1700, « Nombres attribués », à l'adresse http://www.ietf.org/rfc/rfc1700.txt pour obtenir la liste des EtherTypes.

- **Description** : une explication de l'objectif de la règle, jusqu'à 100 caractères par ligne. Vous pouvez saisir plusieurs lignes; chaque ligne est ajoutée en tant que remarque dans l'interface de ligne de commande, et les remarques sont placées avant la règle.
- **More Options (Autres options)** > **Direction** : indique si la règle s'applique à la direction **In** (Entrée) ou **Out** (Sortie). **In (Entrée)** est le paramètre par défaut.

Lorsque vous avez terminé de définir la règle, cliquez sur **OK** pour l'ajouter au tableau.

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer la règle dans votre configuration.

Configurer les règles d'accès ICMP

Par défaut, vous pouvez envoyer des paquets ICMP vers n'importe quelle interface IPv4 ou IPv6, avec les exceptions suivantes

- L'ASA ne répond pas aux demandes ECHO ICMP dirigées vers une adresse de diffusion.
- L'ASA répond uniquement au trafic ICMP envoyé à l'interface par laquelle le trafic entre; vous ne pouvez pas envoyer de trafic ICMP par une interface vers une interface distante.

Pour protéger le périphérique contre les attaques, vous pouvez utiliser des règles ICMP pour limiter l'accès ICMP aux interfaces à des hôtes, des réseaux ou des types ICMP particuliers. Les règles ICMP fonctionnent comme des règles d'accès, où les règles sont classées, et la première règle qui correspond à un paquet définit l'action.

Si vous configurez une règle ICMP pour une interface, une règle ICMP de refus implicite est ajoutée à la fin de la liste de règles ICMP, modifiant le comportement par défaut. Par conséquent, si vous souhaitez simplement refuser certains types de messages, vous devez inclure une règle autoriser tout à la fin de la liste de règles ICMP pour autoriser les autres types de messages.

Nous vous recommandons de toujours accorder l'autorisation pour le type de message ICMP « unreachable » (inaccessible) (type 3). Le refus des messages ICMP inaccessibles désactive la découverte de la MTU du chemin ICMP, ce qui peut interrompre le trafic IPsec et PPTP. De plus, les paquets ICMP dans IPv6 sont utilisés dans le processus de découverte de voisin IPv6.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Management Access (Accès de gestion)** > **ICMP**.

Étape 2 Configurez les règles ICMP.

a) Ajoutez une règle (**Add (Ajouter) > Rule (Règle)**, **Add (Ajouter) > IPv6 Rule (Règle IPv6)** ou **Add (Ajouter) > Insert (Insérer)**), ou sélectionnez une règle et modifiez-la.
b) Sélectionnez le type ICMP que vous souhaitez contrôler, ou **any** pour appliquer la règle à tous les types.
c) Sélectionnez l'interface à laquelle la règle s'applique. Vous devez créer des règles distinctes pour chaque interface.
d) Choisissez si vous autorisez ou refusez l'accès pour le trafic correspondant.
e) Sélectionnez **Any Address** (Toute adresse) pour appliquer la règle à tout le trafic. Sinon, saisissez l'adresse et le masque (pour IPv4) ou l'adresse et la longueur du préfixe (pour IPv6) de l'hôte ou du réseau que vous essayez de contrôler.
f) Cliquez sur **OK**.

Étape 3 (Facultatif) Pour définir les limites de messages ICMP inaccessibles, définissez les options suivantes. L'augmentation de la limite de débit, ainsi que l'activation de l'option **Decrement time to live for a connection (Décrémenter la durée de vie d'une connexion)** dans une politique de service (dans la boîte de dialogue Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service) > Rule Actions (Actions de règle) > Connection Settings (Paramètres de connexion)), est nécessaire pour permettre un traceroute à travers l'ASA qui affiche l'ASA comme l'un des sauts.

- Limitation de débit— : définit la limite de débit des messages unreachable, entre 1 et 100 messages par seconde. La valeur par défaut est de 1 message par seconde.
- Taille de la rafale—définit le débit en rafale, entre 1 et 10. Le système envoie ce nombre de réponses, mais les réponses suivantes ne sont pas envoyées tant que la limite de débit n'est pas atteinte.

Étape 4 Cliquez sur **Apply**.

Surveillance des règles d'accès

La page Règles d'accès comprend le nombre de résultats pour chaque règle. Passez le pointeur sur le nombre d'accès pour afficher l'heure de mise à jour et l'intervalle du compteur. Pour réinitialiser le nombre d'accès, cliquez avec le bouton droit sur la règle et sélectionnez **Clear Hit Count** (Effacer le nombre d'accès), mais sachez que cela efface le compteur de toutes les règles appliquées à la même interface dans la même direction.

Évaluation des messages Syslog pour les règles d'accès

Utilisez une visionneuse d'événements syslog, comme celle dans ASDM, pour afficher les messages liés aux règles d'accès.

Si vous utilisez la journalisation par défaut, le message syslog 106023 s'affiche pour les flux explicitement refusés uniquement. Le trafic qui correspond à l'entrée « refuser implicite » qui termine la liste de règles n'est pas journalisé.

En cas d'attaque de l'ASA, le nombre de messages de journal système pour les paquets refusés peut être très élevé. Nous vous recommandons d'activer plutôt la journalisation à l'aide du message syslog 106100, qui fournit des statistiques pour chaque règle (y compris les règles d'autorisation) et vous permet de limiter le nombre de messages syslog produits. Sinon, vous pouvez désactiver toute la journalisation pour une règle donnée.

Lorsque vous activez la journalisation pour le message 106100, si un paquet correspond à une ACE, l'ASA crée une entrée de flux pour suivre le nombre de paquets reçus dans un intervalle spécifique. L'ASA génère un message syslog au premier résultat et à la fin de chaque intervalle, identifiant le nombre total de résultats au cours de l'intervalle et l'horodatage du dernier résultat. À la fin de chaque intervalle, l'ASA réinitialise le nombre de résultats à 0. Si aucun paquet ne correspond à l'ACE pendant un intervalle, l'ASA supprime l'entrée de flux. Lorsque vous configurez la journalisation pour une règle, vous pouvez contrôler l'intervalle et même le niveau de gravité du message de journal, par règle.

Un flux est défini par les adresses IP source et de destination, les protocoles et les ports. Comme le port source peut différer pour une nouvelle connexion entre les deux mêmes hôtes, vous pourriez ne pas voir le même incrément de flux, car un nouveau flux a été créé pour la connexion.

Les paquets autorisés qui appartiennent à des connexions établies n'ont pas besoin d'être vérifiés par rapport aux listes de contrôle d'accès; seul le paquet initial est journalisé et inclus dans le nombre de résultats. Pour les protocoles sans connexion, comme ICMP, tous les paquets sont journalisés, même s'ils sont autorisés, et tous les paquets refusés sont journalisés.

Consultez le *guide des messages de journal système* pour obtenir des renseignements sur les messages de journal système.

Astuces

Lorsque vous activez la journalisation pour le message 106100, si un paquet correspond à une ACE, l'ASA crée une entrée de flux pour suivre le nombre de paquets reçus dans un intervalle spécifique. L'ASA dispose d'un maximum de 32 K flux de journalisation pour les ACE. Un grand nombre de flux peuvent exister simultanément à tout moment. Pour éviter une utilisation illimitée des ressources de mémoire et de processeur, l'ASA impose une limite au nombre de flux *de refus* simultanés; la limite est placée sur les flux de refus uniquement (et non sur les flux d'autorisation), car ils peuvent indiquer une attaque. Lorsque la limite est atteinte, l'ASA ne crée pas de nouveau flux de refus pour la journalisation jusqu'à ce que les flux existants expirent et envoie le message 106101. Vous pouvez contrôler la fréquence de ce message et le nombre maximal de flux de refus mis en cache dans les paramètres avancés; voir Configurer les options avancées pour les règles d'accès, à la page 23.

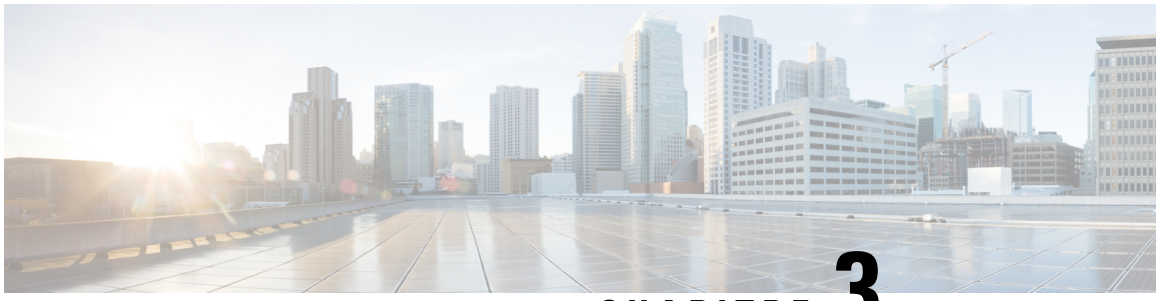
Historique des règles d'accès

Nom de la caractéristique	Versions de plateforme	Description
Critères d'accès de l'interface	7.0(1)	Contrôle de l'accès au réseau par l'intermédiaire de l'ASA à l'aide des ACL. Nous avons introduit l'écran suivant : Configuration > Firewall (Pare-feu) > Access Rules (Règles d'accès).

Nom de la caractéristique	Versions de plateforme	Description
Critères d'accès globaux	8.3(1)	Des règles d'accès globales ont été introduites. Nous avons modifié l'écran suivant : Configuration > Firewall (Pare-feu) > Access Rules (Règles d'accès).
Prise en charge du pare-feu d'identité	8.4(2)	Vous pouvez maintenant utiliser des utilisateurs et des groupes de pare-feu d'identité pour la source et la destination. Vous pouvez utiliser une liste de contrôle d'accès de pare-feu d'identité avec des règles d'accès, des règles AAA et pour l'authentification VPN.
Prise en charge des ACL EtherType pour le trafic IS-IS	8.4(5), 9.1(2)	En mode de pare-feu transparent, l'ASA peut désormais transmettre le trafic IS-IS à l'aide d'une liste de contrôle d'accès EtherType. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > EtherType Rules (Règles EtherType).
Prise en charge de TrustSec	9.0(1)	Vous pouvez maintenant utiliser les groupes de sécurité TrustSec pour la source et la destination. Vous pouvez utiliser une liste de contrôle d'accès de pare-feu d'identité avec des règles d'accès.
ACL unifiée pour IPv4 et IPv6	9.0(1)	Les ACL prennent désormais en charge les adresses IPv4 et IPv6. Vous pouvez même spécifier une combinaison d'adresses IPv4 et IPv6 pour la source et la destination. Le mot-clé **any** a été modifié pour représenter le trafic IPv4 et IPv6. Les mots-clés **any4** et **any6** ont été ajoutés pour représenter le trafic IPv4 uniquement et IPv6 uniquement, respectivement. Les ACL propres à IPv6 sont obsolètes. Les ACL IPv6 existantes sont migrées vers des ACL étendues. Pour en savoir plus, consultez les notes de mise à jour. Nous avons modifié les écrans suivants : Configuration > Firewall (Pare-feu) > Access Rules (Règles d'accès) Configuration (Configuration) > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Group Policies (Stratégies de groupe) > General (Général) > More Options (Autres options)
Amélioration des ACL étendues et des objets pour filtrer le trafic ICMP par code ICMP	9.0(1)	Le trafic ICMP peut maintenant être autorisé ou refusé en fonction du code ICMP. Nous avons introduit ou modifié les écrans suivants : Configuration > Firewall (Pare-feu) > Objects (Objets) > Service Objects/Groups (Objets/groupes de service) Configuration (Configuration) > Firewall (Pare-feu) > Access Rule (Règle d'accès)

Nom de la caractéristique	Versions de plateforme	Description
Modèle de validation transactionnelle sur le moteur de règles de groupe d'accès	9.1(5)	Lorsque cette option est activée, une mise à jour de règle est appliquée une fois la compilation de la règle terminée, sans affecter les performances de correspondance de la règle. Nous avons introduit l'écran suivant : Configuration (Configuration) > Device Management (Gestion des périphériques) > Advanced (Avancé) > Rule Engine (Moteur de règles).
Session de configuration pour modifier les ACL et les objets. Référencement ultérieur des objets et desACL dans les règles d'accès.	9.3(2)	Vous pouvez maintenant modifier les ACL et les objets dans une session de configuration isolée. Vous pouvez également référencer des objets et des ACL à l'avance, c'est-à-dire configurer des règles et des groupes d'accès pour des objets ou des ACL qui n'existent pas encore.
Prise en charge des règles d'accès pour le protocole Stream Control Transmission Protocol (SCTP)	9.5(2)	Vous pouvez maintenant créer des règles d'accès à l'aide du protocole **sctp**, y compris des spécifications de port. Nous avons modifié les boîtes de dialogue d'ajout/modification des règles d'accès sur la page **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Règles d'accès)**.
Prise en charge de la règle Ethertype pour l'adresse du point d'accès au service de destination du paquet de contrôle de liaison logique IEEE 802.2.	9.6(2)	Vous pouvez maintenant écrire des règles de contrôle d'accès Ethertype pour l'adresse du point d'accès de service de destination du paquet de contrôle de liaison logique IEEE 802.2. En raison de cet ajout, le mot clé **bpdu** ne correspond plus au trafic prévu. Réécrivez les règles **bpdu** pour utiliser **dsap 0x42**. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **EtherType Rules (Règles EtherType)**.
Prise en charge en mode routé des règles EtherType sur les interfaces membres de groupes de ponts et des règles d'accès étendues sur les interfaces virtuelles de pont (BVI).	9.7(1)	Vous pouvez maintenant créer des ACL EtherType et les appliquer aux interfaces membres de groupes de ponts en mode routé. Vous pouvez également appliquer des règles d'accès étendues à l'interface virtuelle de pont (BVI) en plus des interfaces membres. Nous avons modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Règles d'accès)**, **Configuration** > **Firewall (Pare-feu)** > **Ethertype Rules (Règles Ethertype)**.
Modifications de la liste de contrôle d'accès Ethertype.	9.9(1)	Les listes de contrôle d'accès EtherType prennent désormais en charge Ethernet II IPX (EII IPX). En outre, de nouveaux mots clés sont ajoutés au mot clé DSAP pour prendre en charge les valeurs DSAP courantes : BPDU (0x42), IPX (0xE0), IPX brut (0xFF) et ISIS (0xFE). Par conséquent, les entrées de contrôle d'accès EtherType existantes qui utilisent les mots-clés BPDU ou ISIS seront converties automatiquement pour utiliser la spécification DSAP, et les règles pour IPX seront converties en trois règles (DSAP IPX, DSAP brut IPX et EII IPX). De plus, la capture de paquets qui utilise IPX comme valeur EtherType est obsolète, car IPX correspond à trois EtherTypes distincts. Nous avons modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **EtherType Rules (Règles EtherType)**.

Nom de la caractéristique	Versions de plateforme	Description
Le seuil de recherche du groupe d'objets est désormais désactivé par défaut.	9.12(1)	Si vous avez activé la recherche par groupe d'objets, la fonctionnalité a été soumise à un seuil pour aider à empêcher la dégradation des performances. Ce seuil est désormais désactivé par défaut. Vous pouvez l'activer en utilisant la commande **object-group-search threshold**. Nous avons modifié l'écran suivant : **Configuration** > **Access Rules (Critères d'accès)** > **Advanced (Avancé)**.
Le référencement direct des ACL et des objets est toujours activé. De plus, la recherche de groupes d'objets pour le contrôle d'accès est désormais activée par défaut.	9.18(1)	Vous pouvez faire référence à des ACL ou à des objets réseau qui n'existent pas encore lors de la configuration de groupes d'accès ou de critères d'accès. De plus, la recherche de groupes d'objets est désormais activée par défaut pour le contrôle d'accès pour les *nouveaux* déploiements. Cette commande restera désactivée lors de la mise à niveau des périphériques. Si vous souhaitez l'activer (conseillé), vous devez le faire manuellement. Nous avons supprimé la commande **forward-reference enable** et modifié la valeur par défaut pour **object-group-search access-control** afin de l'activer.



CHAPITRE 3

Objets pour le contrôle d'accès.

Les objets sont des composants réutilisables dans votre configuration. Vous pouvez les définir et les utiliser dans les configurations ASA à la place des adresses IP en ligne, des services, des noms, etc. Les objets facilitent la maintenance de vos configurations, car vous pouvez modifier un objet à un seul emplacement et répercuter cette modification dans tous les autres emplacements qui y font référence. Sans objets, vous devriez modifier les paramètres pour chaque fonctionnalité en cas de besoin, plutôt qu'une seule fois. Par exemple, si un objet réseau définit une adresse IP et un masque de sous-réseau et que vous souhaitez modifier l'adresse, vous n'avez qu'à la modifier dans la définition de l'objet, et non dans toutes les fonctionnalités qui font référence à cette adresse IP.

- Lignes directrices relatives aux objets, à la page 33
- Configurer les objets., à la page 34
- Objets de surveillance, à la page 45
- Historique pour les objets, à la page 45

Lignes directrices relatives aux objets

Directives IPv6

Prend en charge IPv6 avec les restrictions suivantes :

- Vous pouvez combiner les entrées IPv4 et IPv6 dans un groupe d'objets réseau, mais vous ne pouvez pas utiliser un groupe d'objets mixtes pour la NAT.

Directives et limites additionnelles

- Les objets doivent avoir des noms uniques, car les objets et les groupes d'objets partagent le même espace de nom. Bien que vous puissiez créer un groupe d'objets réseau nommé « Engineering » et un groupe d'objets de service nommé « Engineering », vous devez ajouter un identifiant (ou « tag ») à la fin d'au moins un nom de groupe d'objets pour le rendre unique. Par exemple, vous pouvez utiliser les noms « Engineering_admins » et « Engineering_hosts » pour rendre les noms de groupes d'objets uniques et faciliter l'identification.
- Lorsque vous saisissez plusieurs éléments dans l'adresse source ou de destination, ou dans le service source ou de destination, dans une ACL ou une règle d'accès, ASDM crée automatiquement un groupe d'objets pour eux avec le préfixe DM_INLINE. Ces objets ne sont pas affichés dans la page des objets, mais ils sont définis sur le périphérique.

- Les noms d'objets sont limités à 64 caractères, y compris les lettres, les chiffres et les caractères suivants : .!@#$%^&()-_{}. Les noms des objets sont sensibles à la casse.

Configurer les objets.

Les sections suivantes décrivent comment configurer les objets principalement utilisés pour le contrôle d'accès.

Configurer les objets et groupes de réseau

Les objets et les groupes de réseau identifient les adresses IP ou les noms d'hôtes. Utilisez ces objets dans les listes de contrôle d'accès pour simplifier vos règles.

Configurer un objet réseau

Un objet réseau peut contenir un hôte, une adresse IP de réseau, une plage d'adresses IP, ou un nom de domaine complet (FQDN).

Vous pouvez également activer les règles NAT sur l'objet (à l'exception des objets FQDN). Pour en savoir plus sur la configuration des objets NAT, consultez Traduction d'adresses réseau (NAT), à la page 121.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Objects/Groups (Objets/groupes de services réseau)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add (Ajouter) > Network Object (Objet réseau)** pour ajouter un nouvel objet. Saisissez un nom et, éventuellement, une description.
- Choisissez un objet existant et cliquez sur **Edit** (Modifier).

Étape 3 Configurez l'adresse de l'objet en fonction des champs **Type** et **IP Version** (Version IP).

- **Hôte** : adresse IPv4 ou IPv6 d'un seul hôte. Par exemple, 10.1.1.1 ou 2001:DB8::0DB8:800:200C:417A.
- **Réseau** : l'adresse d'un réseau. Pour IPv4, incluez le masque, par exemple, **adresse IP** = 10.0.0.0 **masque réseau** = 255.0.0.0. Pour IPv6, incluez le préfixe, tel que **adresse IP** = 2001:DB8:0:CD30:: **longueur du préfixe** = 60.
- **Plage** : une plage d'adresses. Vous pouvez définir des plages IPv4 ou IPv6. N'incluez pas de masque ni de préfixe.
- **FQDN** : un seul nom de domaine complet, tel que www.exemple.com.

Étape 4 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Vous pouvez maintenant utiliser cet objet réseau lorsque vous créez une règle. Si vous modifiez un objet, la modification est automatiquement héritée par toutes les règles qui utilisent l'objet.

Configurer un groupe d'objets réseau

Les groupes d'objets réseau peuvent contenir plusieurs objets réseau, ainsi que des réseaux en ligne ou des hôtes. Les groupes d'objets réseau peuvent inclure une combinaison d'adresses IPv4 et IPv6.

Cependant, vous ne pouvez pas utiliser un groupe d'objets IPv4 et IPv6 mixtes pour la NAT, ou des groupes d'objets qui comprennent des objets FQDN.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Objects/Groups (Objets/groupes de services réseau)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add (Ajouter) > Network Object Group** (Groupe d'objets réseau) pour ajouter un nouvel objet. Saisissez un nom et éventuellement, une description.
- Choisissez un objet existant et cliquez sur **Edit** (Modifier).

Étape 3 Ajoutez des objets réseau au groupe en utilisant n'importe quelle combinaison des techniques suivantes :

- **Existing Network Objects/Groups** (Objets/groupes réseau existants) : sélectionnez un objet ou un groupe réseau déjà défini, puis cliquez sur **Add** (Ajouter) pour l'inclure dans le groupe.
- **Create New Network Object Member** (Créer un membre d'objet réseau) : saisissez les critères d'un nouvel objet réseau et cliquez sur **Add** (Ajouter).

Étape 4 Après avoir ajouté tous les objets membres, cliquez sur **OK**, puis sur **Apply** (Appliquer).

Vous pouvez maintenant utiliser cet objet réseau lorsque vous créez une règle. Pour un groupe d'objets modifié, la modification est transmise automatiquement par toutes les règles utilisant le groupe.

Configurer des objets de service et des groupes de services

Les objets et les groupes de service identifient les protocoles et les ports. Utilisez ces objets dans les listes de contrôle d'accès pour simplifier vos règles.

Configurer un objet de service

Un objet de service ne peut contenir qu'une seule spécification de protocole.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Service Object/Group (Objet/groupe de services)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add (Ajouter) > Service Object (Objet de service)** pour ajouter un nouvel objet. Saisissez un nom et, éventuellement, une description.
- Choisissez un objet existant et cliquez sur **Edit** (Modifier).

Étape 3 Choisissez le type de service et complétez les détails au besoin :

- Protocol (Protocole) : un numéro entre 0-255, ou un nom connu, tel que **ip**, **tcp**, **udp**, **gre**, etc.
- ICMP, ICMP6 : vous pouvez laisser les champs de type de message et de code vides pour correspondre à n'importe quel message ICMP ou ICMP version 6. Vous pouvez éventuellement spécifier le type ICMP par nom ou par numéro (0 à 255) pour limiter l'objet à ce type de message. Si vous spécifiez un type, vous pouvez éventuellement spécifier un code ICMP pour ce type (de 1 à 255). Si vous ne spécifiez pas de code, tous les codes sont utilisés.
- TCP, UDP, SCTP : vous pouvez éventuellement spécifier des ports pour la source, la destination ou les deux. Vous pouvez préciser le port par son nom ou son numéro. Vous pouvez inclure les opérateurs suivants :
  - **<** : inférieur à. Par exemple, <80.
  - **>** : supérieur à. Par exemple, >80.
  - **!=** : différent de. Par exemple, !=80.
  - **-** (trait d'union) : une plage inclusive de valeurs. Par exemple, 100-200.

Étape 4 Cliquez sur **OK**, puis sur **Apply**(appliquer).

Configurer un groupe de services

Un groupe d'objets de service comprend un ensemble de protocoles, si nécessaire, y compris des ports source et de destination facultatifs pour les protocoles qui les utilisent, ainsi que le type et le code ICMP.

Avant de commencer

Vous pouvez modéliser tous les services à l'aide du groupe d'objets de service générique, qui est expliqué ici. Cependant, vous pouvez toujours configurer les types d'objets de groupe de services qui étaient disponibles avant l'ASA 8.3(1). Ces objets existants comprennent des groupes de ports TCP/UDP/TCP-UDP, des groupes de protocoles et des groupes ICMP. Le contenu de ces groupes est équivalent à la configuration associée dans le groupe d'objets de service générique, à l'exception des groupes ICMP, qui ne prennent pas en charge les codes ICMP6 ou ICMP. Si vous souhaitez toujours utiliser ces objets existants, pour obtenir des instructions détaillées, consultez la description de la commande **object-service** dans la référence de commande sur Cisco.com.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Service Objects/Groups (Objets/groupes de services)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add (Ajouter) > Service Group (Groupe de services)** pour ajouter un nouvel objet. Saisissez un nom et, éventuellement, une description.
- Choisissez un objet existant et cliquez sur **Edit** (Modifier).

Étape 3 Ajoutez des objets de service au groupe en utilisant n'importe quelle combinaison des techniques suivantes :

- **Existing Service/Service Group** (Service/groupe de services existant) : sélectionnez un service, un objet de service ou un groupe déjà défini, puis cliquez sur **Add** (Ajouter) pour l'inclure dans le groupe.
- **Create New Member** (Créer un membre) : saisissez les critères d'un nouvel objet de service et cliquez sur **Add** (Ajouter). Si vous donnez un nom à l'objet, lorsque vous appliquez les modifications, le nouvel objet est créé et ajouté au groupe; sinon, les objets sans nom sont membres de ce groupe uniquement. Vous ne pouvez pas nommer les objets TCP-UDP; ceux-ci sont membres du groupe seulement.

Étape 4 Après avoir ajouté tous les objets membres, cliquez sur **OK**, puis sur **Apply** (Appliquer).

Vous pouvez maintenant utiliser ce groupe d'objets de service lorsque vous créez une règle. Pour un groupe d'objets modifié, la modification est transmise automatiquement par toutes les règles utilisant le groupe.

Configuration des objets et des groupes de service réseau

Un objet ou un groupe de service réseau définit une application. Une application peut consister en un nom de domaine DNS (comme exemple.com), un sous-réseau IP et, éventuellement, un protocole et un port, comme TCP/80. Ainsi, un objet ou un groupe de service réseau peut combiner le contenu d'objets de réseau et de service distincts en un seul objet.

Vous pouvez utiliser le groupe d'objets de service réseau dans une liste de contrôle d'accès étendue à utiliser avec les listes de routage (dans le routage basé sur les politiques), les règles de contrôle d'accès et le filtre VPN. Notez que vous ne pouvez pas utiliser directement un objet de service réseau (et non un groupe) dans une liste de contrôle d'accès : vous devez d'abord placer des objets dans un objet de groupe, puis vous pouvez utiliser l'objet de groupe.

Lorsque vous utilisez des spécifications de nom de domaine, le système utilise la surveillance DNS pour obtenir les adresses IP obtenues par la demande DNS de l'utilisateur avant le début de la connexion. Cela garantit qu'une adresse IP est disponible au début d'une connexion, afin que la connexion soit gérée correctement, par des listes de routage et des règles de contrôle d'accès, à partir du premier paquet.

Lignes directrices relatives aux objets de service de réseau

- L'inspection DNS est requise si vous incluez des spécifications de nom de domaine DNS dans un objet de service réseau. L'inspection DNS est activée par défaut. Ne la désactivez pas si vous utilisez des objets de service réseau.
- La surveillance de trafic DNS est effectuée uniquement sur les paquets DNS UDP et n'est pas effectuée sur les paquets DNS TCP ou HTTP. Contrairement aux objets de nom de domaine complets, les spécifications de domaine de service de réseau sont détectées immédiatement, même si vous n'utilisez pas l'objet dans une liste d'accès.
- Vous ne pouvez pas activer dnscrypt dans la liste des politiques d'inspection DNS ; il n'est pas compatible avec la surveillance DNS nécessaire pour obtenir les adresses IP des domaines utilisés dans les objets

de service réseau. Tous les objets de service réseau qui comprennent des spécifications de domaine deviendront inopérants et les entrées de contrôle d'accès connexes ne correspondront pas.

- Vous pouvez définir un maximum de 1024 groupes de services réseau. Cependant, cette limite est partagée avec les groupes d'utilisateurs locaux de pare-feu d'identité. Pour chaque groupe de service de réseau défini, vous pouvez créer 2 groupes d'utilisateurs de moins.
- Les contenus des groupes de services réseau peuvent se chevaucher, mais vous ne pouvez pas créer la copie complète d'un groupe de services réseau.
- Si un objet ou un groupe de service réseau est utilisé dans une liste de contrôle d'accès, la suppression de l'objet efface simplement le contenu de l'objet. L'objet lui-même reste défini dans la configuration.
- Le mot-clé **dynamic** sur un objet ou un groupe indique que l'objet ne sera pas enregistré dans la configuration en cours d'exécution, il sera affiché uniquement dans la sortie **show object**. Ne configurez pas directement ce mot-clé. Il est principalement utilisé par les gestionnaires d'appareils externes.
- La commande **app-id** pour un objet de service réseau définit un numéro attribué par Cisco pour une application particulière, dans la plage de 1 à 4 294 967 295. Ne configurez pas directement cette commande. Cette commande est principalement destinée à l'utilisation de gestionnaires d'appareils externes.

Configurer des serveurs DNS de confiance

Si vous configurez les noms de domaine dans les objets de service réseau, le système espionne le trafic de demande/réponse DNS pour recueillir les adresses IP des noms de domaine DNS et mettre les résultats en cache. Toute demande/réponse DNS peut être espionnée.

Les enregistrements espionnés sont A, AAAA et MX. La durée de vie (TTL) de chaque nom résolu est prise en compte dans les limites suivantes : le TTL minimal est de 2 minutes, et le maximum est de 24 heures. Cela garantit que le cache ne devient pas périmé.

Pour des raisons de sécurité, vous pouvez limiter la portée de la surveillance DNS en définissant quels serveurs DNS doivent être considérés comme de confiance. Tout trafic DNS vers des serveurs DNS non de confiance est ignoré et n'est pas utilisé pour obtenir des mappages pour les objets de service réseau. Par défaut, tous les serveurs DNS configurés et appris sont de confiance; vous ne devez modifier ce réglage que si vous souhaitez limiter la liste de confiance.

Remarque La clé est que vous définissez les serveurs DNS utilisés par vos clients comme serveurs de confiance.

Avant de commencer

La surveillance DNS dépend de l'inspection DNS, qui est activée par défaut. Assurez-vous de ne pas désactiver l'inspection. En outre, la surveillance DSN est incompatible avec la fonctionnalité **dnscrypt**, donc n'activez pas cette commande dans la liste des politiques d'inspection DNS.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **DNS Client (Client DNS)**.

Étape 2 Sous **Trusted DNS Server** (Serveur DNS de confiance), configurez les options permettant de déterminer quels serveurs sont considérés comme fiables.

a) (Facultatif) Ajoutez ou supprimez des serveurs DNS de confiance configurés de manière explicite.

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau serveur, sélectionnez le type d'adresse IP (IPv4 ou IPv6), saisissez l'adresse IP du serveur et cliquez sur **OK**.
- Sélectionnez un serveur et cliquez sur **Edit** (Modifier) pour modifier l'adresse.
- Sélectionnez un serveur et cliquez sur **Delete** (Supprimer) pour le supprimer de la liste des serveurs de confiance.

b) Sélectionnez ou désélectionnez les options suivantes :

- **Any** (Tous) : faites confiance à tous les serveurs DNS, surveillez-les tous. Cette option est désactivée par défaut.
- **Configured-Servers** (Serveurs configurés) : indique si les serveurs configurés dans les groupes de serveurs DNS doivent être considérés comme fiables. Par défaut, cette option est activée.
- **DHCP-Client** (Client DHCP) : indique si les serveurs identifiés par la surveillance des messages entre un client DHCP et un serveur DHCP sont considérés comme des serveurs DNS de confiance. Par défaut, cette option est activée.
- **DHCP-Pools** (Ensembles DHCP) : indique si les serveurs DNS configurés dans les ensembles DHCP pour les clients qui obtiennent des adresses par l'intermédiaire des serveurs DHCP exécutés sur les interfaces d'appareils doivent être considérés comme fiables. Par défaut, cette option est activée.
- **DHCP-Relay** (Relais DHCP) : indique si les serveurs identifiés par la surveillance des messages de relais DHCP entre un client DHCP et un serveur DHCP sont considérés comme des serveurs DNS de confiance. Par défaut, cette option est activée.

Étape 3 Cliquez sur **Apply** (Appliquer).

Configurer les objets de service réseau

Un objet de service réseau définit une seule application. Il définit l'emplacement de l'application par la spécification du sous-réseau ou, plus communément, par le nom de domaine DNS. Vous pouvez également inclure le protocole et le port pour restreindre la portée de l'application.

Vous ne pouvez utiliser ces objets que dans des objets de groupe de services réseau; vous ne pouvez pas utiliser directement un objet de service réseau dans une entrée de liste de contrôle d'accès (ACE).

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Services Objects/Groups (Objets/groupes de services réseau)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add (Ajouter)** > **Network Services Objects (Objets de services réseau)** pour ajouter un nouvel objet. Saisissez un nom et, éventuellement, une description.

- Choisissez un objet existant et cliquez sur **Edit** (Modifier).

Étape 3 (Non recommandé). Ajoutez l'ID de l'application dans le champ **App-ID**.

Il s'agit d'un numéro unique attribué par Cisco pour une application particulière, dans la plage de 1 à 4 294 967 295. Cette option est principalement destinée à l'utilisation de gestionnaires de périphérique externes. Vous ne devez pas configurer cette valeur.

Étape 4 Ajoutez un ou plusieurs membres à l'objet :

a) Sélectionnez l'une des options suivantes dans **Create New Member** (Créer un nouveau membre), puis remplissez les informations d'adresse appropriées :

- **domain** (domaine) : nom du DNS, jusqu'à 253 caractères. Il peut s'agir d'un nom complet (comme www.example.com) ou partiel (comme example.com), auquel cas l'objet correspond à tous les sous-domaines, c'est-à-dire les serveurs avec le nom partiel (comme www.example.com, www1.example.com, long.server.name.example.com, etc.). Les connexions seront comparées au nom le plus long si une correspondance exacte est disponible. Le nom de domaine peut se résoudre en plusieurs adresses IP.
- **subnet** (sous-réseau) : l'adresse d'un réseau. Pour les sous-réseaux IPv4, incluez l'adresse et le masque réseau, par exemple, 10.0.0.0 255.0.0.0. Pour IPv6, incluez l'adresse et le préfixe, par exemple 2001:DB8:0:CD30::/60. Saisissez les valeurs appropriées dans les champs suivants :

b) Sélectionnez l'une des options suivantes dans Type de service, puis remplissez les champs appropriés :

- **protocol (protocole)** : le protocole utilisé dans la connexion, tel que tcp, udp, ip, etc. Pour rendre l'objet indépendant du service, saisissez simplement **ip**.
- **tcp** ou **udp** : saisissez le numéro de port, 1 à 65 535 ou un mnémonique, tel que www. Pour un port unique, saisissez simplement le numéro de port. Pour plusieurs ports, vous pouvez inclure le nombre après les opérateurs suivants :
  - < signifie tout port inférieur au numéro de ports spécifiés.
  - > désigne tout port supérieur au numéro de ports spécifiés.
  - **range** désigne tout port entre les deux ports spécifiés. Le premier numéro de port doit être inférieur au deuxième numéro de port.

c) Cliquez sur **Add** (ajouter) pour ajouter l'entrée à l'objet. Pour supprimer un service, sélectionnez-le et cliquez sur **Delete** (Supprimer).

d) Répétez le processus jusqu'à ce que l'objet contienne toutes les spécifications dont vous avez besoin.

Étape 5 Cliquez sur **OK**.

Configurer les groupes d'objets de service réseau

Les groupes de services réseau peuvent contenir des objets de service réseau et des spécifications explicites de sous-réseau ou de domaine. Vous pouvez utiliser des objets de service réseau dans les entrées de liste de contrôle d'accès (ACE) pour le routage basé sur les politiques, le contrôle d'accès et le filtre VPN.

Utilisez des groupes de services réseau pour définir une catégorie d'applications qui doivent être gérées de la même manière. Par exemple, vous pouvez créer un groupe unique qui définit les applications dont le trafic

doit être dirigé vers Internet plutôt que vers le tunnel VPN de site à site vers la plateforme centrale de l'entreprise.

Il n'y a aucune limite au nombre d'applications que vous incluez dans un groupe d'objets de service réseau, que ce soit explicitement ou par référence à des objets de service réseau.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Services Objects/Groups (Objets/groupes de services réseau)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add (Ajouter)** > **Network Services Objects (Objets de services réseau)** pour ajouter un nouvel objet. Saisissez un nom et, éventuellement, une description.
- Choisissez un groupe existant et cliquez sur **Edit** (Modifier).

Étape 3 Pour ajouter un objet de service réseau existant au groupe :

a) Sélectionnez **Existing Network-Services Objects** (Objets de services réseau existants).
b) Cliquez sur **Add** (Ajouter) pour ajouter l'objet au groupe. Pour supprimer un objet, sélectionnez-le et cliquez sur **Delete** (Supprimer).
c) Répétez le processus jusqu'à ce que le groupe contienne tous les objets dont vous avez besoin.

Étape 4 Pour définir un ou plusieurs membres directement dans le groupe :

a) Sélectionnez **Create New Network-Services Object Member** (Créer un membre d'objet de services réseau).
b) Sélectionnez l'une des options suivantes, puis complétez les informations d'adresse appropriées :

- **domain** (domaine) : nom du DNS, jusqu'à 253 caractères. Il peut s'agir d'un nom complet (comme www.example.com) ou partiel (comme example.com), auquel cas l'objet correspond à tous les sous-domaines, c'est-à-dire les serveurs avec le nom partiel (comme www.example.com, www1.example.com, long.server.name.example.com, etc.). Les connexions seront comparées au nom le plus long si une correspondance exacte est disponible. Le nom de domaine peut se résoudre en plusieurs adresses IP.
- **subnet** (sous-réseau) : l'adresse d'un réseau. Pour les sous-réseaux IPv4, incluez l'adresse et le masque réseau, par exemple, 10.0.0.0 255.0.0.0. Pour IPv6, incluez l'adresse et le préfixe, par exemple 2001:DB8:0:CD30::/60. Saisissez les valeurs appropriées dans les champs suivants :

c) Sélectionnez l'une des options suivantes dans Type de service, puis remplissez les champs appropriés :

- **protocol (protocole)** : le protocole utilisé dans la connexion, tel que tcp, udp, ip, etc. Pour rendre l'objet indépendant du service, saisissez simplement **ip**.
- **tcp** ou **udp** : saisissez le numéro de port, 1 à 65 535 ou un mnémonique, tel que www. Pour un port unique, saisissez simplement le numéro de port. Pour plusieurs ports, vous pouvez inclure le nombre après les opérateurs suivants :
  - < signifie tout port inférieur au numéro de ports spécifiés.
  - > désigne tout port supérieur au numéro de ports spécifiés.

- **range** désigne tout port entre les deux ports spécifiés. Le premier numéro de port doit être inférieur au deuxième numéro de port.

d) Cliquez sur **Add** pour ajouter le service réseau au groupe. Pour supprimer un service, sélectionnez-le et cliquez sur **Delete** (Supprimer).
e) Répétez le processus jusqu'à ce que le groupe contienne toutes les spécifications dont vous avez besoin.

Étape 5 Cliquez sur **OK**.

Configurer les groupes d'utilisateurs locaux

Vous pouvez créer des groupes d'utilisateurs locaux à utiliser dans les fonctionnalités qui prennent en charge le pare-feu d'identité en incluant le groupe dans une liste de contrôle d'accès étendue, qui peut à son tour être utilisée dans une règle d'accès, par exemple.

L'ASA envoie une requête LDAP au serveur Active Directory pour les groupes d'utilisateurs globalement définis dans le contrôleur de domaine Active Directory. L'ASA importe ces groupes pour les règles basées sur l'identité. Cependant, l'ASA peut avoir des ressources réseau locales qui ne sont pas définies globalement, ce qui nécessite des groupes d'utilisateurs locaux avec des politiques de sécurité locales. Les groupes d'utilisateurs locaux peuvent contenir des groupes imbriqués et des groupes d'utilisateurs importés d'Active Directory. L'ASA consolide les groupes locaux et Active Directory.

Un utilisateur peut appartenir à des groupes d'utilisateurs locaux et à des groupes d'utilisateurs importés d'Active Directory.

Comme vous pouvez utiliser les noms d'utilisateurs et les noms de groupes d'utilisateurs directement dans une liste de contrôle d'accès, vous ne devez configurer les groupes d'utilisateurs locaux que si :

- Vous souhaitez créer un groupe d'utilisateurs défini dans la base de données LOCAL.
- Vous souhaitez créer un groupe d'utilisateurs ou de groupes d'utilisateurs qui ne sont pas capturés dans un seul groupe d'utilisateurs défini sur le serveur AD.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Local User Groups (Groupes d'utilisateurs locaux)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add** (Ajouter) pour ajouter un nouvel objet. Saisissez un nom et éventuellement, une description.
- Choisissez un objet existant et cliquez sur **Edit** (Modifier).

Étape 3 Ajoutez des utilisateurs ou des groupes à l'objet à l'aide de l'une des méthodes suivantes :

- **Sélectionner les utilisateurs ou les groupes existants** : sélectionnez le domaine qui contient l'utilisateur ou le groupe, puis choisissez le nom de l'utilisateur ou du groupe dans les listes et cliquez sur **Add** (Ajouter). Pour les listes longues, utilisez la zone Find (Rechercher) pour aider à localiser l'utilisateur. Les noms sont extraits du serveur pour le domaine sélectionné.

- **Saisir manuellement les noms d'utilisateur** : vous pouvez simplement saisir les noms d'utilisateur ou de groupe dans la zone d'édition du bas et cliquer sur **Add** (Ajouter). Lorsque vous utilisez cette méthode, le nom de domaine sélectionné est ignoré et le domaine par défaut est utilisé si vous n'en spécifiez pas. Pour les utilisateurs, le format est *domain_name**username* ; pour les groupes, une double barre oblique inverse est utilisée : *domain_name**group_name*.

Étape 4 Après avoir ajouté tous les objets membres, cliquez sur **OK**, puis sur **Apply** (Appliquer).

Vous pouvez maintenant utiliser ce groupe d'objets utilisateur lorsque vous créez une règle. Pour un groupe d'objets modifié, la modification est transmise automatiquement par toutes les règles utilisant le groupe.

Configurer les groupes d'objets de groupe de sécurité

Vous pouvez créer des groupes d'objets de groupe de sécurité pour une utilisation dans les fonctionnalités qui prennent en charge Cisco TrustSec en incluant le groupe dans une liste de contrôle d'accès étendue, qui peut à son tour être utilisée dans une règle d'accès, par exemple.

Lorsqu'il est intégré à Cisco TrustSec, l'ASA télécharge les informations de groupe de sécurité à partir d'ISE. L'ISE agit comme un référentiel d'identité en fournissant un mappage d'identité balise Cisco TrustSec à utilisateur et un mappage de ressource balise à serveur Cisco TrustSec. Vous provisionnez et gérez les listes de contrôle d'accès de groupe de sécurité de manière centralisée sur ISE.

Cependant, l'ASA peut avoir des ressources réseau locales qui ne sont pas définies globalement et qui nécessitent des groupes de sécurité locaux avec des politiques de sécurité locales. Les groupes de sécurité locaux peuvent contenir des groupes de sécurité imbriqués qui sont téléchargés à partir d'ISE. L'ASA consolide les groupes de sécurité locaux et centraux.

Pour créer des groupes de sécurité locaux sur l'ASA, vous créez un groupe d'objets de sécurité local. Un groupe d'objets de sécurité local peut contenir un ou plusieurs groupes d'objets de sécurité imbriqués ou des identifiants de sécurité ou des noms de groupes de sécurité. Vous pouvez également créer un nouvel ID de sécurité ou un nom de groupe de sécurité qui n'existe pas sur l'ASA.

Vous pouvez utiliser les groupes d'objets de sécurité que vous créez sur l'ASA pour contrôler l'accès aux ressources réseau. Vous pouvez utiliser le groupe d'objets de sécurité dans le cadre d'un groupe d'accès ou d'une politique de service.

Astuces Si vous créez un groupe avec des balises ou des noms qui ne sont pas connus de l'ASA, toutes les règles qui utilisent le groupe seront inactives jusqu'à ce que les balises ou les noms soient résolus avec ISE.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Security Group Object Groups (Groupes d'objets de groupe de sécurité)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add** (Ajouter) pour ajouter un nouvel objet. Saisissez un nom et, éventuellement, une description.

- Choisissez un objet existant et cliquez sur **Edit** (Modifier).

Étape 3 Ajoutez des groupes de sécurité à l'objet à l'aide de l'une des méthodes suivantes :

- **Select existing local security group object groups** (Sélectionner des groupes d'objets de groupe de sécurité locaux existants) : choisissez dans la liste des objets déjà définis et cliquez sur **Add** (Ajouter). Pour les listes longues, utilisez la zone Rechercher pour aider à localiser l'objet.
- **Select security groups discovered from ISE** (Sélectionner des groupes de sécurité découverts à partir de l'ISE) : choisissez des groupes dans la liste des groupes existants et cliquez sur **Add** (Ajouter).
- **Manually add security tags or names** (Ajouter manuellement des balises ou des noms de sécurité) : vous pouvez simplement saisir le numéro de balise ou le nom du groupe de sécurité dans la zone de modification du bas et cliquer sur **Add** (Ajouter). Une balise est un nombre de 1 à 65 533 et est attribuée à un périphérique par l'authentification IEEE 802.1X, l'authentification Web ou le contournement de l'authentification MAC (MAB) par ISE. Les noms de groupes de sécurité sont créés sur l'ISE et fournissent des noms conviviaux pour les groupes de sécurité. La table des groupes de sécurité mappe les balises SGT aux noms de groupes de sécurité. Consultez votre configuration ISE pour connaître les balises et les noms valides.

Étape 4 Après avoir ajouté tous les objets membres, cliquez sur **OK**, puis sur **Apply** (Appliquer).

Vous pouvez maintenant utiliser ce groupe d'objets de groupe de sécurité lorsque vous créez une règle. Pour un groupe d'objets modifié, la modification est transmise automatiquement par toutes les règles utilisant le groupe.

Configurer les plages de temps

Un objet de plage temporelle définit une durée spécifique composée d'une heure de début, d'une heure de fin et d'entrées récurrentes facultatives. Vous utilisez ces objets dans les règles ACL pour fournir un accès défini dans le temps à certaines fonctionnalités ou ressources. Par exemple, vous pouvez créer une règle d'accès qui autorise l'accès à un serveur particulier pendant les heures de travail uniquement.

Remarque Vous pouvez inclure plusieurs entrées périodiques dans un objet de plage temporelle. Si une plage temporelle comporte à la fois des valeurs absolues et des valeurs périodiques, les valeurs périodiques ne sont exploitées qu'une fois l'heure de début absolue atteinte et ne sont plus exploitées une fois l'heure de fin absolue atteinte.

La création d'une plage temporelle ne restreint pas l'accès au périphérique. Cette procédure définit uniquement la plage temporelle. Vous devez ensuite utiliser l'objet dans une règle de contrôle d'accès.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Time Ranges (Plages de temps)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add** (Ajouter) pour ajouter une nouvelle plage temporelle. Saisissez un nom et éventuellement, une description.
- Choisissez une plage temporelle existante et cliquez sur **Edit** (Modifier).

Étape 3 Choisissez les heures globales de début et de fin.

La valeur par défaut est de commencer maintenant et de ne jamais terminer, mais vous pouvez définir des dates et des heures spécifiques. La plage temporelle comprend les heures que vous saisissez.

Étape 4 (Facultatif) Configurez les périodes récurrentes dans la durée active globale, telles que les jours de la semaine ou l'intervalle hebdomadaire récurrent pendant lequel la plage temporelle sera active.

a) Cliquez sur **Add** (Ajouter), ou sélectionnez une période existante et cliquez sur **Edit** (Modifier).

b) Effectuez l'une des opérations suivantes :

- Cliquez **sur Specify days of the week and times on which this recurring range will be active** (Préciser les jours de la semaine et les heures auxquelles cette plage récurrente sera active), et choisissez les jours et les heures dans les listes.
- Cliquez sur **Specify a weekly interval when this recurring range will be active** (Préciser un intervalle hebdomadaire pendant lequel cette plage récurrente sera active), et choisissez les jours et les heures dans les listes.

c) Cliquez sur **OK**.

Étape 5 Cliquez sur **OK**, puis sur **Apply**(appliquer).

Objets de surveillance

Pour les objets de réseau, de service et de groupes de sécurité, vous pouvez analyser l'utilisation d'un objet individuel. À partir de leur page dans le dossier **Configuration > Firewall > Objects** (Configuration > Pare-feu > Objets), cliquez sur le bouton **Where Used** (Où utilisé).

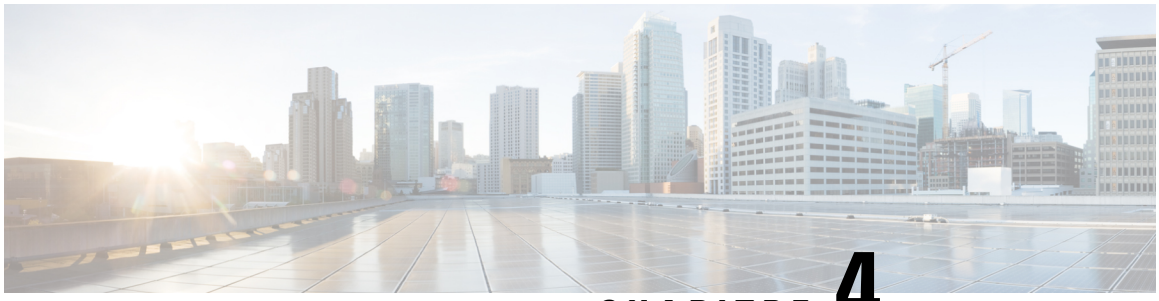
Pour les objets réseau, vous pouvez également cliquer sur le bouton Not Used (Non utilisé) pour rechercher les objets qui ne sont utilisés dans aucune règle ni aucun autre objet. Cet affichage vous donne un raccourci pour supprimer ces objets inutilisés.

Historique pour les objets

Nom de la caractéristique	Observations Versions	Description
Groupes d'objets	7.0(1)	Les groupes d'objets simplifient la création et la maintenance des listes de contrôle d'accès.
Expressions régulières et listes des politiques	7.2(1)	Les expressions régulières et les listes des politiques ont été introduites pour être utilisées dans les listes des politiques d'inspection. Les commandes suivantes ont été introduites : **class-map type regex**, **regex**, **match regex**.

Nom de la caractéristique	Observations Versions	Description
Objets	8.3(1)	La prise en charge des objets a été introduite.
Groupes d'objets utilisateur pour le pare-feu d'identité	8.4(2)	Les groupes d'objets utilisateur pour le pare-feu d'identité ont été introduits.
Groupes d'objets de groupe de sécurité pour Cisco TrustSec	8.4(2)	Les groupes d'objets de groupe de sécurité pour Cisco TrustSec ont été introduits.
Groupes d'objets réseau mixtes IPv4 et IPv6	9.0(1)	Auparavant, les groupes d'objets réseau ne pouvaient contenir que toutes les adresses IPv4 ou toutes les adresses IPv6. Les groupes d'objets réseau peuvent désormais prendre en charge une combinaison d'adresses IPv4 et IPv6. **Remarque** Vous ne pouvez pas utiliser un groupe d'objets mixtes pour la NAT.
Amélioration étendue de l'ACL et des objets pour filtrer le trafic ICMP par code ICMP	9.0(1)	Le trafic ICMP peut maintenant être autorisé ou refusé en fonction du code ICMP. Nous avons introduit ou modifié les écrans suivants : Configuration > Firewall (Pare-feu) > Objects (Objets) > Service Objects/Groups (Objets/groupes de service), Configuration (Configuration) > Firewall (Pare-feu) > Access Rule (Règle d'accès)
Prise en charge des objets de service pour le protocole SCTP (Stream Control Transmission Protocol)	9.5(2)	Vous pouvez maintenant créer des objets de service et des groupes qui spécifient des ports SCTP. Nous avons modifié les boîtes de dialogue d'ajout/modification des objets et groupes de service sur la page **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Service Objects/Groups (Objets/groupes de service)**.

Nom de la caractéristique	Observations Versions	Description
Objets de service réseau et leur utilisation dans le routage et le contrôle d'accès basés sur des politiques	9.17(1)	Vous pouvez configurer des objets de service de réseau et les utiliser dans des listes de contrôle d'accès étendues pour les utiliser dans les cartes de routage basées sur des politiques et les groupes de contrôle d'accès. Les objets de service de réseau comprennent les spécifications de sous-réseau IP ou de nom de domaine DNS, ainsi que les spécifications de protocole et de port, qui combinent notamment des objets de réseau et de service. Cette fonctionnalité comprend également la possibilité de définir des serveurs DNS de confiance, pour s'assurer que toutes les résolutions de noms de domaine DNS acquièrent des adresses IP de sources de confiance. Nous avons ajouté ou modifié les écrans suivants. • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Route Maps (Cartes de routage)**, boîtes de dialogue Add/Edit (Ajouter/modifier). • **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**, boîtes de dialogue Add/Edit (Ajouter/modifier). • **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Services Objects/Groups (Objets/groupes de services réseau)**. • **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **DNS Client (Client DNS)**.
Prise en charge des groupes de services réseau	9.19(1)	Vous pouvez désormais définir un maximum de 1 024 groupes de services réseau.



CHAPITRE 4

Listes de contrôle d'accès

Les listes de contrôle d'accès (ACL) sont utilisées par de nombreuses fonctions différentes. Lorsqu'elles sont appliquées aux interfaces ou globalement en tant que règles d'accès, elles autorisent ou refusent le trafic qui passe par le périphérique. Pour les autres fonctionnalités, l'ACL sélectionne le trafic auquel la fonctionnalité s'appliquera, en effectuant un service de correspondance plutôt qu'un service de contrôle.

Les sections suivantes expliquent les bases des listes de contrôle d'accès et comment les configurer et les surveiller. Les règles d'accès, les listes de contrôle d'accès appliquées globalement ou aux interfaces, sont expliquées plus en détail dans Règles d'accès, à la page 11.

- À propos des ACL, à la page 49
- Licences pour les listes de contrôle d'accès, à la page 54
- Lignes directrices pour les ACL, à la page 55
- Configurer les ACL, à la page 56
- Surveillance des ACL, à la page 64
- Historique des ACL, à la page 65

À propos des ACL

Les listes de contrôle d'accès (ACL) identifient les flux de trafic en fonction d'une ou de plusieurs caractéristiques, notamment l'adresse IP source et de destination, le protocole IP, les ports, EtherType et d'autres paramètres, selon le type d'ACL. Les ACL sont utilisées dans une variété de fonctionnalités. Les listes de contrôle d'accès sont composées d'une ou de plusieurs entrées de contrôle d'accès (ACE).

Types d'ACL

L'ASA utilise les types d'ACL suivants :

- ACL étendues : les listes de contrôle d'accès étendues sont le principal type que vous utiliserez. Ces listes de contrôle d'accès sont utilisées pour les critères d'accès afin d'autoriser et de refuser le trafic via le périphérique, ainsi que pour la correspondance du trafic de nombreuses fonctionnalités, notamment les politiques de service, les règles AAA, WCCP, le filtre de trafic de réseau de zombies, les stratégies de groupe VPN et les politiques DAP. Dans ASDM, bon nombre de ces fonctionnalités possèdent leurs propres pages de règles et ne peuvent pas utiliser les listes de contrôle d'accès étendues que vous définissez dans ACL Manager, bien qu'ACL Manager affiche les listes de contrôle d'accès créées sur ces pages. Consultez Configurer les ACL étendues, à la page 56.

- ACL EtherType : les listes de contrôle d'accès EtherType s'appliquent uniquement au trafic de couche 2 non IP sur les interfaces de membre de groupe de ponts. Vous pouvez utiliser ces règles pour autoriser ou abandonner le trafic en fonction de la valeur EtherType dans le paquet de couche 2. Les listes de contrôle d'accès EtherType vous permettent de contrôler le flux du trafic non IP sur le périphérique. Voir Configurer les règles EtherType, à la page 25.
- ACL de type Web : les listes de contrôle d'accès de type Web sont utilisées pour filtrer le trafic VPN SSL sans client. Ces listes de contrôle d'accès peuvent refuser l'accès en fonction des URL ou des adresses de destination. Consultez Configurer les ACL de type Web, à la page 61.
- ACL standard : les listes de contrôle d'accès standard identifient le trafic par adresse de destination uniquement. Il existe peu de fonctionnalités qui les utilisent : listes de routage et filtres VPN. Comme les filtres VPN permettent également des listes d'accès étendues, limitez l'utilisation de l'ACL standard aux listes de routage. Consultez Configurer les ACL standard, à la page 60.

Le tableau suivant répertorie certaines utilisations courantes des listes de contrôle d'accès et le type à utiliser.

Tableau 2 : Types d'ACL et utilisations courantes

Utilisation de l'ACL	Type d'ACL	Description
Contrôler l'accès au réseau pour le trafic IP (mode routé et transparent)	Étendu	L'ASA n'autorise aucun trafic d'une interface de sécurité inférieure vers une interface de sécurité supérieure, à moins qu'il ne soit explicitement autorisé par une liste de contrôle d'accès étendue. En mode routé, vous devez utiliser une liste de contrôle d'accès pour autoriser le trafic entre une interface membre d'un groupe de ponts et une interface située à l'extérieur du même groupe de ponts. **Remarque** Pour accéder à l'interface ASA pour l'accès de gestion, vous n'avez pas non plus besoin d'une liste de contrôle d'accès autorisant l'adresse IP de l'hôte. Il vous suffit de configurer l'accès de gestion en suivant le guide de configuration sur les opérations générales.
Identifier le trafic pour les règles AAA	Étendu	Les règles AAA utilisent des listes de contrôle d'accès pour identifier le trafic.
Augmenter le contrôle d'accès au réseau pour le trafic IP d'un utilisateur donné	Étendue, téléchargée à partir d'un serveur AAA pour chaque utilisateur	Vous pouvez configurer le serveur RADIUS pour télécharger une liste de contrôle d'accès dynamique à appliquer à l'utilisateur, ou le serveur peut envoyer le nom d'une liste de contrôle d'accès que vous avez déjà configurée sur l'ASA.
Accès et filtrage au VPN	Étendu Standard	Les stratégies de groupe pour l'accès à distance et les VPN de site à site utilisent des listes de contrôle d'accès standard ou étendues pour le filtrage. Les VPN d'accès à distance utilisent également des listes de contrôle d'accès étendues pour les configurations de pare-feu client et les politiques d'accès dynamique.

Utilisation de l'ACL	Type d'ACL	Description
Identifier le trafic dans une mise en correspondance des cartes de classes de trafic pour le cadre de politiques modulaires	Étendu	Les listes de contrôle d'accès peuvent être utilisées pour identifier le trafic dans une carte de trafic, utilisée par les fonctionnalités qui prennent en charge le cadre de politiques modulaires. Les fonctionnalités qui prennent en charge le cadre de politique modulaire comprennent les paramètres TCP et généraux, ainsi que l'inspection.
Pour les interfaces membres d'un groupe de ponts, contrôler l'accès au réseau pour le trafic non IP	EtherType	Vous pouvez configurer une liste de contrôle d'accès qui contrôle le trafic en fonction de son EtherType pour toute interface membre d'un groupe de ponts.
Identifier le filtrage et la redistribution des routes	Standard Étendue	Divers protocoles de routage utilisent des listes de contrôle d'accès standard pour le filtrage et la redistribution (au moyen de listes de routage) pour les adresses IPv4 et des listes de contrôle d'accès étendues pour IPv6.
Filtrage pour le VPN SSL sans client	Type Web	Vous pouvez configurer une liste de contrôle d'accès de type Web pour filtrer les URL et les destinations.

Le gestionnaire d'ACL

Le gestionnaire d'ACL apparaît sous deux formes :

- Dans la fenêtre principale, par exemple, en sélectionnant **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **ACL Manager (Gestionnaire d'ACL)**. Dans ce cas, le gestionnaire d'ACL affiche uniquement les listes d'accès étendues. Ces listes de contrôle d'accès comprennent celles générées par les règles que vous créez dans les pages des règles d'accès, des règles de politique de service et des règles AAA. Veillez à ce que les modifications que vous apportez dans le gestionnaire d'ACL n'affectent pas négativement ces règles; les modifications que vous apportez ici seront répercutées sur ces autres pages.
- À partir d'une politique qui nécessite une ACL, en cliquant sur le bouton **Manage** (Gérer) à côté du champ. Dans ce cas, le gestionnaire d'ACL peut avoir des onglets distincts pour les listes d'ACL standard et étendues, si la politique autorise l'un ou l'autre de ces types. Sinon, l'affichage est filtré pour afficher uniquement les listes de contrôle d'accès standard, étendues ou de type Web. Le gestionnaire d'ACL n'affiche jamais les listes de contrôle d'accès EtherType.

Il existe des pages distinctes pour les listes de contrôle d'accès standard et les listes de contrôle d'accès de type Web, afin que vous puissiez les configurer dans la fenêtre principale. Ces pages sont fonctionnellement équivalentes au gestionnaire d'ACL sans le nom :

- ACL standard : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Standard ACL (ACL standard)**.
- ACL de type Web : **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Clientless SSL VPN Access (Accès VPN SSL sans client)** > **Advanced (Avancé)** > **Web ACLs (ACL Web)**.

Noms d'ACL

Chaque liste de contrôle d'accès (ACL) est associée à un nom ou à un ID numérique, tel que outside_in, OUTSIDE_IN ou 101. Limitez les noms à 241 caractères ou moins. Envisagez d'utiliser toutes les lettres majuscules pour faciliter la recherche du nom lors de l'affichage d'une configuration en cours d'exécution.

Développez une convention de dénomination qui vous aidera à identifier l'objectif prévu de la liste de contrôle d'accès. Par exemple, ASDM utilise la convention *interface-name_purpose_direction*, telle que « outside_access_in », pour une liste de contrôle d'accès appliquée à l'interface « externe » dans la direction entrante.

Traditionnellement, les identifiants d'ACL étaient des numéros. Les listes de contrôle d'accès standard étaient dans la plage de 1 à 99 ou de 1 300 à 1 999. Les listes de contrôle d'accès étendues étaient dans la plage 100-199 ou 2 000-2 699. L'ASA n'applique pas ces plages, mais si vous souhaitez utiliser des chiffres, vous pouvez vous en tenir à ces conventions pour maintenir la cohérence avec les routeurs exécutant le logiciel IOS.

Ordre des entrées de contrôle d'accès

Une ACL est composée d'une ou de plusieurs ACE. Sauf si vous insérez explicitement une ACE à une ligne donnée, chaque ACE que vous saisissez pour un nom d'ACL donné est ajoutée à la fin de l'ACL.

L'ordre des ACE est important. Lorsque l'ASA décide de transférer ou d'abandonner un paquet, l'ASA teste le paquet 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.

Ainsi, si vous placez une règle plus spécifique après une règle plus générale, la règle la plus spécifique pourrait ne jamais être atteinte. Par exemple, si vous souhaitez autoriser le réseau 10.1.1.0/24, mais abandonner le trafic de l'hôte 10.1.1.15 sur ce sous-réseau, l'ACE qui refuse 10.1.1.15 doit venir avant celle qui autorise 10.1.1.0/24. Si l'ACE d'autorisation 10.1.1.0/24 arrive en premier, 10.1.1.15 sera autorisé et l'ACE de refus ne correspondra jamais.

Utilisez les boutons Haut et Bas pour repositionner les règles si nécessaire.

Autoriser/refuser ou mettre en correspondance/aucune correspondance

Les entrées de contrôle d'accès « autorisent » ou « refusent » le trafic qui correspond à la règle. Lorsque vous appliquez une liste de contrôle d'accès à une fonctionnalité qui détermine si le trafic est autorisé par l'ASA ou est abandonné, comme les règles d'accès globales et d'interface, « autoriser » et « refuser » signifient ce qu'elles indiquent.

Pour d'autres fonctionnalités, telles que les règles de politique de service, « autoriser » et « refuser » signifient en fait « correspondance » ou « aucune correspondance ». Dans ces cas, la liste de contrôle d'accès sélectionne le trafic qui doit recevoir les services de cette fonctionnalité, tels que l'inspection d'application ou le redirection vers un module de service. Le trafic « refusé » est simplement le trafic qui ne correspond pas à la liste de contrôle d'accès et ne recevra donc pas le service. (Dans ASDM, les règles de politique de service utilisent en fait Match/Do Not Match (Correspondance/Aucune correspondance), et les règles AAA utilisent Authenticate/Do Not Authenticate (Authentifier/Ne pas authentifier), par exemple, mais dans la CLI, il s'agit toujours de permit/deny.)

Refus implicite du contrôle d'accès

Les listes de contrôle d'accès utilisées pour les règles d'accès de transit comportent une instruction de refus implicite à la fin. Ainsi, pour les listes de contrôle d'accès de contrôle du trafic telles que celles appliquées aux interfaces, si vous n'autorisez pas explicitement un type de trafic, ce trafic est abandonné. Par exemple, si vous souhaitez autoriser tous les utilisateurs à accéder à un réseau par l'intermédiaire de l'ASA, à l'exception d'une ou de plusieurs adresses particulières, vous devez refuser ces adresses particulières, puis autoriser toutes les autres.

Pour les listes de contrôle d'accès de gestion (plan de commande), qui contrôlent le trafic vers le boîtier, il n'y a pas de refus implicite à la fin d'un ensemble de règles de gestion pour une interface. Au lieu de cela, toute connexion qui ne correspond pas à une règle d'accès de gestion est ensuite évaluée par des règles de contrôle d'accès normales.

Pour les listes de contrôle d'accès utilisées pour sélectionner le trafic pour un service, vous devez « autoriser » explicitement le trafic ; tout trafic non « autorisé » ne sera pas mis en correspondance pour le service ; le trafic « refuser » contourne le service.

Pour les listes de contrôle d'accès EtherType, le refus implicite à la fin de la liste de contrôle d'accès n'affecte pas le trafic IP ni les ARP ; par exemple, si vous autorisez EtherType 8037, le refus implicite à la fin de l'ACL ne bloque pas le trafic IP que vous avez précédemment autorisé avec une liste de contrôle d'accès étendue (ou implicitement autorisé d'une interface de haute sécurité à une interface de sécurité faible). Toutefois, si vous refusez *explicitement* tout le trafic avec une commande EtherType ACE, le trafic IP et ARP est refusé ; seul le trafic de protocole physique, tel que la négociation automatique, est toujours autorisé.

Adresses IP utilisées pour les listes de contrôle d'accès étendues lorsque vous utilisez la NAT

Lorsque vous utilisez la NAT ou la PAT, vous traduisez des adresses ou des ports, en faisant généralement correspondre les adresses internes et externes. Si vous devez créer une liste de contrôle d'accès étendue qui s'applique à des adresses ou des ports qui ont été traduits, vous devez déterminer s'il faut utiliser les adresses ou les ports réels (non traduits) ou ceux mappés. Les exigences varient en fonction de la fonctionnalité.

L'utilisation de l'adresse et du port réels signifie que si la configuration de la NAT change, vous n'avez pas besoin de modifier les listes de contrôle d'accès.

Fonctionnalités qui utilisent des adresses IP réelles

Les commandes et fonctionnalités suivantes utilisent des adresses IP réelles dans les listes de contrôle d'accès, même si l'adresse vue sur une interface est l'adresse mappée :

- Règles d'accès (ACL étendues référencées par la commande **access-group**)
- Règles de politique de service (commande **match access-list** de Modular Policy Framework)
- Classification du trafic du filtre de trafic de zombie (commande**Dynamic-filter enable classify-list**)
- Règles AAA (commandes **aaa ... match**)
- WCCP (commande **wccp redirect-list group-list**)

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).

Fonctionnalités qui utilisent des adresses IP mappées

Les fonctionnalités suivantes utilisent des ACL, mais ces ACL utilisent les valeurs mappées comme elles sont vues sur une interface :

- ACL IPsec
- ACL de commande **capture**
- ACL par utilisateur
- ACL de protocole de routage
- Toutes les autres ACL de fonctionnalité.

ACE temporelles

Vous pouvez appliquer des objets de plage temporelle aux ACE étendues et de type Web afin que les règles soient actives pendant des périodes spécifiques uniquement. Ces types de règles vous permettent de faire la différence entre les activités acceptables à certaines heures de la journée et inacceptables à d'autres heures. Par exemple, vous pouvez appliquer des restrictions supplémentaires pendant les heures de travail et les assouplir après les heures de travail ou pendant le repas. Inversement, vous pourriez essentiellement arrêter votre réseau en dehors des heures de travail.

Vous ne pouvez pas créer des règles basées sur le temps qui ont exactement les mêmes critères de protocole, de source, de destination et de service d'une règle qui n'inclut pas d'objet de plage temporelle. La règle non basée sur le temps remplace toujours la règle basée sur le temps en double, car elles sont redondantes.



Remarque Les utilisateurs peuvent connaître un retard d'environ 80 à 100 secondes après l'heure de fin spécifiée pour que la liste de contrôle d'accès devienne inactive. Par exemple, si l'heure de fin spécifiée est 3:50, comme l'heure de fin est inclusive, la commande est récupérée n'importe où entre 3:51:00 et 3:51:59. Une fois la commande reçue, l'ASA termine toute tâche en cours d'exécution, puis prend en charge la commande pour désactiver l'ACL.

Licences pour les listes de contrôle d'accès

Les listes de contrôle d'accès ne nécessitent pas de licence spéciale.

Cependant, pour utiliser **sctp** comme protocole dans une entrée, vous devez avoir une licence Carrier.

Lignes directrices pour les ACL

Mode pare-feu

- Les listes de contrôle d'accès étendues et standard sont prises en charge dans les modes de pare-feu routé et transparent.
- Les listes de contrôle d'accès de type Web sont prises en charge en mode routé uniquement.
- Les listes de contrôle d'accès EtherType sont prises en charge pour les interfaces de membre de groupe de ponts uniquement, en modes routé et transparent.

Basculement et mise en grappe

Les sessions de configuration ne sont pas synchronisées sur les unités de basculement ou en grappe. Lorsque vous validez les modifications dans une session, elles sont appliquées normalement dans toutes les unités de basculement et de grappe.

IPv6

- Les listes de contrôle d'accès étendues et de type Web permettent une combinaison d'adresses IPv4 et IPv6.
- Les listes de contrôle d'accès standard n'autorisent pas les adresses IPv6.
- Les listes de contrôle d'accès EtherType ne contiennent pas d'adresses IP.

Directives supplémentaires

- Lorsque vous spécifiez un masque réseau, la méthode est différente de la commande **access-list** du logiciel IOS de Cisco. L'ASA utilise un masque réseau (par exemple, 255.255.255.0 pour un masque de classe C). Le masque IOS de Cisco utilise des caractères génériques (par exemple, 0.0.0.255).
- Lorsque vous saisissez plusieurs éléments dans l'adresse source ou de destination, ou dans le service source ou de destination, ASDM crée automatiquement un groupe d'objets pour eux avec le préfixe DM_INLINE. Ces objets sont automatiquement développés jusqu'à leurs composants dans la vue du tableau de règles, mais vous pouvez voir les noms des objets si vous désélectionnez la préférence **Auto-expand network and service objects with specified prefix** (Développer automatiquement les objets réseau et de service avec le préfixe spécifié) du tableau de règles dans **Tools (Outils)** > **Preferences (Préférences)**.
- (ACL étendue uniquement) Les fonctionnalités suivantes utilisent des listes de contrôle d'accès, mais ne peuvent pas accepter une liste de contrôle d'accès avec pare-feu d'identité (précisant les noms d'utilisateur ou de groupe), FQDN (noms de domaine complets) ou valeurs Cisco TrustSec :
  - commande **crypto map** du VPN
  - commande **group-policy** de VPN, sauf pour **vpn-filter**
  - WCCP
  - DAP

Configurer les ACL

Les sections suivantes expliquent comment configurer les différents types d'ACL génériques, à l'exception de ceux utilisés comme règles d'accès (y compris EtherType), règles de politique de service, règles AAA et autres utilisations pour lesquelles ASDM fournit une page à usage spécial pour ces politiques basées sur des règles.

Configurer les ACL étendues

Une ACL étendue est représentée comme un conteneur nommé d'ACE. Pour créer une nouvelle ACL, vous devez d'abord créer le conteneur. Ensuite, vous pouvez ajouter des ACE, modifier les ACE existantes et réorganiser les ACE à l'aide du tableau dans ACL Manager.

La liste de contrôle d'accès étendue peut inclure une combinaison d'adresses IPv4 et IPv6.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **ACL Manager (Gestionnaire d'ACL)**.

Étape 2 Si vous créez une nouvelle liste de contrôle d'accès, choisissez **Add (Ajouter)** > **Add ACL (Ajouter une ACL)**, saisissez un nom et cliquez sur OK (**OK**).

Le conteneur d'ACL est ajouté à la table. Vous pouvez la renommer ultérieurement en la sélectionnant et en cliquant sur **Edit** (Modifier).

Étape 3 Effectuez l'une des actions suivantes :

- Pour ajouter une ACE à la fin de la liste de contrôle d'accès, sélectionnez le nom de l'ACL ou toute ACE dans celui-ci, puis choisissez **Add> Add ACE (Ajouter> Ajouter une ACE)**.
- Pour insérer une ACE à un emplacement spécifique, sélectionnez une ACE existante et choisissez **Add> Insert (ajouter> insérer)** pour ajouter l'ACE au-dessus de la règle, ou choisissez **Add> Insert After (ajouter> insérer après)**.
- Sélectionnez une règle et cliquez sur **Edit** (Modifier).

Étape 4 Renseignez les propriétés de l'ACE. Les principales options à sélectionner sont :

- **Action : Permit/Deny (Autoriser/Refuser)** : indique si vous autorisez (en sélectionnant) le trafic décrit ou si vous le refusez (en le désélectionnant, aucune correspondance).
- **Source/Destination criteria** (Critères source/destination) : définissez la source (adresse d'origine) et la destination (adresse cible du flux de trafic). Vous configurez généralement des adresses IPv4 ou IPv6 d'hôtes ou de sous-réseaux, que vous pouvez représenter avec des groupes d'objets réseau ou des groupes d'objets de service réseau. Vous pouvez également préciser un nom d'utilisateur ou de groupe d'utilisateurs pour la source. En outre, vous pouvez utiliser le champ Service pour identifier le type spécifique de trafic si vous souhaitez cibler la règle de manière plus étroite que tout le trafic IP. Si vous incluez des spécifications de service dans un objet de service réseau, précisez IP dans le champ Service. Si vous mettez en œuvre Cisco TrustSec, vous pouvez utiliser des groupes de sécurité pour définir la source et la destination.

Pour des informations détaillées sur les options, consultez Propriétés des ACE étendues, à la page 57.

Lorsque vous avez terminé de définir l'ACE, cliquez sur **OK** pour ajouter la règle au tableau.

Étape 5 Cliquez sur **Apply** (Appliquer).

Propriétés des ACE étendues

Lorsque vous ajoutez ou modifiez une ACE dans une liste de contrôle d'accès étendue, vous pouvez configurer les propriétés suivantes. Dans de nombreux champs, vous pouvez cliquer sur le bouton « ... » à droite de la zone de modification pour sélectionner, créer ou modifier des objets disponibles pour le champ.

Action : Permit/Deny (Autoriser/Refuser)

Indique si vous autorisez (en sélectionnant) le trafic décrit ou si vous le refusez (en le désélectionnant, aucune correspondance).

Critères de source

Les caractéristiques de l'initiateur du trafic que vous tentez de mettre en correspondance. Vous devez configurer la source, mais les autres propriétés sont facultatives.

Source

Adresse IPv4 ou IPv6 de la source. La valeur par défaut est **any**, qui correspond à toutes les adresses IPv4 ou IPv6 ; vous pouvez utiliser **any4** pour cibler IPv4 uniquement, ou **any6** pour cibler IPv6 uniquement. Vous pouvez spécifier une adresse d'hôte unique (comme 10.100.10.5 ou 2001:DB8::0DB8:800:200C:417A), un sous-réseau (au format 10.100.10.0/24 ou 10.100.10.0/255.255.255.0, ou pour IPv6, 2001:DB8:0:CD30::/60), le nom d'un objet réseau ou d'un groupe d'objets réseau, le nom d'un groupe d'objets de service réseau, ou le nom d'une interface.

Utilisateur

Si vous activez le pare-feu d'identité, vous pouvez spécifier un utilisateur ou un groupe d'utilisateurs comme source du trafic. L'adresse IP que l'utilisateur utilise actuellement correspondra à la règle. Vous pouvez spécifier un nom d'utilisateur (DOMAIN\user), un groupe d'utilisateurs (DOMAIN\group, notez que le double \ indique un nom de groupe) ou un groupe d'objets utilisateur. Pour ce champ, il est beaucoup plus facile de cliquer sur « **...** » pour sélectionner les noms de votre groupe de serveurs AAA que de les saisir.

Groupe sécurité

Si vous activez Cisco TrustSec, vous pouvez spécifier un nom ou une balise de groupe de sécurité (1-65533), ou un objet de groupe de sécurité.

More Options (Plus d'options) > Source Service (Service source)

Notez que si vous définissez le service source, le protocole du service de destination doit lui correspondre (par exemple, TCP, avec ou sans définition de port). En règle générale, vous définissez le service de destination uniquement et non le service source.

Critères de destination

Les caractéristiques de la cible du trafic que vous tentez de mettre en correspondance. Vous devez configurer la destination, mais les autres propriétés sont facultatives.

Destination

L'adresse IPv4 ou IPv6 de destination. La valeur par défaut est **any**, qui correspond à toutes les adresses IPv4 ou IPv6 ; vous pouvez utiliser **any4** pour cibler IPv4 uniquement, ou **any6** pour cibler IPv6 uniquement. Vous pouvez spécifier une adresse d'hôte unique (comme 10.100.10.5 ou 2001:DB8::0DB8:800:200C:417A), un sous-réseau (au format 10.100.10.0/24 ou 10.100.10.0/255.255.255.0, ou pour IPv6, 2001:DB8:0:CD30::/60), le nom d'un objet réseau ou d'un groupe d'objets réseau, le nom d'un groupe d'objets de service réseau, ou le nom d'une interface.

Groupe sécurité

Si vous activez Cisco Trustsec, vous pouvez spécifier un nom ou une balise de groupe de sécurité (1 à 65 533), ou un objet de groupe de sécurité.

Service

Le protocole du trafic, par exemple IP, TCP, UDP, et éventuellement les ports pour TCP, UDP ou SCTP. La valeur par défaut est IP, mais vous pouvez sélectionner un protocole plus précis pour cibler le trafic avec plus de granularité. En règle générale, vous sélectionnez un type d'objet de service. Pour TCP, UDP et SCTP, vous pouvez préciser les ports, par exemple, tcp/80, tcp/http, tcp/10-20 (pour une plage de ports), tcp-udp/80 (correspond à tout trafic TCP ou UDP sur le port 80), sctp/diameter, etc. Si vous incluez des spécifications de service dans un objet de service réseau, précisez IP dans le champ Service. Pour des informations détaillées sur la spécification des services, consultez Caractéristiques de service dans les ACE étendues, à la page 59.

Description

Une explication de l'objectif de l'ACE, jusqu'à 100 caractères par ligne. Vous pouvez saisir plusieurs lignes ; chaque ligne est ajoutée en tant que remarque dans l'interface de ligne de commande, et les remarques sont placées avant l'ACE.

Remarque Si vous ajoutez des remarques avec des caractères non anglais sur une plateforme (comme Windows), puis essayez de les supprimer d'une autre plateforme (comme Linux), vous ne pourrez peut-être pas les modifier ou les supprimer, car les caractères d'origine peuvent ne pas être correctement reconnus. Cette limitation est due à une dépendance de plateforme sous-jacente qui code différents caractères linguistiques de différentes manières.

Enable Logging (Activer la journalisation) ; Logging Level (Niveau de journalisation) ; More Options (Plus d'options) > Logging Interval (Intervalle de journalisation)

Les options de journalisation définissent la façon dont les messages syslog seront générés pour les règles. Ces options s'appliquent uniquement aux listes de contrôle d'accès, c'est-à-dire à celles associées aux interfaces ou appliquées globalement. Les options sont ignorées pour les listes de contrôle d'accès utilisées pour d'autres fonctionnalités. Vous pouvez implémenter les options de journalisation suivantes :

Désélectionnez Enable Logging (Activer la journalisation)

Cela désactivera la journalisation pour la règle. Aucun message de journal système d'aucun type ne sera émis pour les connexions qui correspondent à cette règle.

Sélectionnez Enable Logging (Activer la journalisation) avec Logging Level (Niveau de journalisation) = Default (Par défaut)

Il fournit la journalisation par défaut pour les règles. Le message de journal système 106023 est émis pour chaque connexion refusée. Si le périphérique est soumis à une attaque, la fréquence d'émission de ce message peut avoir une incidence sur les services.

Sélectionnez Enable Logging (Activer la journalisation) avec Non-Default Logging Level (Niveau de journalisation autre que celui par défaut)

Cela fournit un message de journal système résumé, 106100, au lieu de 106023. Le message 106100 est émis lors du premier impact, puis à chaque intervalle configuré dans **Plus d'options > Intervalle de journalisation** (par défaut toutes les 300 secondes, vous pouvez spécifier 1-600), montrant le nombre d'impacts pendant cet intervalle. Le niveau de journalisation conseillé est **« Information »** .

Le résumé des messages de refus peut réduire l'impact des attaques et éventuellement faciliter l'analyse des messages. Si vous subissez une attaque par déni de service, vous pourriez voir le message 106101, qui indique que le nombre de flux de refus en cache utilisés pour produire le nombre de correspondances pour le message 106100 a dépassé le maximum pour un intervalle. À ce stade, le périphérique arrête de collecter des statistiques jusqu'au prochain intervalle pour maîtriser l'attaque.

More Options (Plus d'options) > Enable Rule (Activer la règle)

Si la règle est active sur le périphérique. Les règles désactivées s'affichent avec du texte barré dans le tableau de règles. La désactivation d'une règle vous permet d'arrêter son application au trafic sans la supprimer, de sorte que vous pouvez la réactiver ultérieurement si vous décidez que vous en avez besoin.

More Options (Plus d'options) > Time Range (Plage de temps)

Le nom de l'objet de plage temporelle qui définit les heures du jour et les jours de la semaine où la règle doit être active. Si vous ne spécifiez pas de plage temporelle, la règle est toujours active.

Caractéristiques de service dans les ACE étendues

Pour le service de destination dans une ACE étendue, vous pouvez spécifier l'un des critères suivants. Les options sont similaires, mais plus limitées, pour le service source, qui se limite aux critères TCP, UDP, TCP-UDP ou SCTP. Si vous incluez des spécifications de service dans un objet de service réseau, précisez IP dans le champ Service.

Nom de l'objet

Le nom de tout type d'objet de service ou de groupe d'objets de service. Ces objets peuvent inclure bon nombre des spécifications expliquées ci-dessous, vous permettant de réutiliser facilement les définitions de service parmi les listes de contrôle d'accès. Il existe de nombreux objets prédéfinis, vous pouvez donc trouver ce dont vous avez besoin sans avoir à saisir manuellement les spécifications ou à créer vos propres objets.

Protocole

Un nombre entre 1-255, ou un nom bien connu, tel que **ip**, **tcp**, **udp**, **gre**, etc.

Ports TCP, UDP, TCP-UDP, SCTP

Vous pouvez inclure des spécifications de port dans les mots-clés **tcp**, **udp**, **tcp-udp** et **sctp**. Le mot-clé tcp-udp vous permet de définir des ports pour les deux protocoles sans avoir à les spécifier séparément. Vous pouvez utiliser les méthodes suivantes pour préciser les ports :

- Port unique : tcp/80, udp/80, tcp-udp/80, sctp/3868, ou un nom de service bien connu, tel que tcp/www, udp/snmp ou sctp/diameter.
- Plage de ports : tcp/1-100, udp/1-100, tcp-udp/1-100, sctp/1-100 correspond aux ports 1 à 100 inclus.
- Non égal à un port : ajoutez != au début de la spécification, par exemple, !=tcp/80 pour correspondre à tout trafic TCP, à l'exception du port TCP 80 (HTTP).
- Moins d'un numéro de port : ajoutez <, par exemple <tcp/150 pour faire correspondre le trafic TCP pour tout port inférieur à 150.
- Supérieur à un numéro de port : ajoutez >, par exemple, >tcp150 pour faire correspondre le trafic TCP pour tout port supérieur à 150.

Remarque DNS, Discard, Echo, Ident, NTP, RPC, SUNRPC et Talk nécessitent chacun une définition pour TCP et une pour UDP. TACACS+ nécessite une définition pour le port 49 sur TCP.

Messages ICMP et ICMP6

Vous pouvez cibler des messages spécifiques (comme les messages de demande d'écho et de réponse ping) et même des codes de message. Il existe de nombreux objets prédéfinis qui couvrent ICMP (pour IPv4) et ICMP6 (pour IPv6), de sorte que vous n'aurez peut-être pas besoin de définir manuellement les critères. Le format est le suivant :

icmp/*icmp_message_type*[/*icmp_message_code*]

icmp6/*icmp6_message_type*[/*icmp6_message_code*]

Où le type de message est 1-255 ou un nom bien connu, et le code est 0-255. Assurez-vous que le numéro que vous sélectionnez correspond à un type ou à un code réel, sinon l'ACE ne sera jamais mise en correspondance.

Configurer les ACL standard

Une ACL standard est représentée comme un conteneur nommé d'ACE. Pour créer une nouvelle liste de contrôle d'accès, vous devez d'abord créer le conteneur. Ensuite, vous pouvez ajouter des ACE, modifier les ACE existantes et réorganiser les ACE à l'aide de la table d'ACL standard. Le tableau peut apparaître sous forme d'onglet dans ACL Manager (Gestionnaire d'ACL) lorsque vous configurez les ACL tout en configurant les politiques qui les utilisent. Si c'est le cas, les procédures sont les mêmes, à l'exception de la manière dont vous accédez à la fenêtre.

Une liste de contrôle d'accès standard utilise uniquement des adresses IPv4 et définit uniquement les adresses de destination.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Standard ACL (ACL standard)**.

Étape 2 Si vous créez une nouvelle liste de contrôle d'accès, choisissez **Add (Ajouter)** > **Add ACL (Ajouter une ACL)**, saisissez un nom et cliquez sur OK (**OK**).

Le conteneur d'ACL est ajouté à la table. Vous ne pouvez pas renommer une liste de contrôle d'accès standard.

Étape 3 Effectuez l'une des actions suivantes :

- Pour ajouter une ACE à la fin de la liste de contrôle d'accès, sélectionnez le nom de l'ACL ou toute ACE dans celui-ci, puis choisissez **Add> Add ACE (Ajouter> Ajouter une ACE)**.
- Pour insérer une ACE à un emplacement spécifique, sélectionnez une ACE existante et choisissez **Add> Insert (ajouter> insérer)** pour ajouter l'ACE au-dessus de la règle, ou choisissez **Add> Insert After (ajouter> insérer après)**.
- Pour modifier une règle, sélectionnez-la et cliquez sur **Edit** (Modifier).

Étape 4 Renseignez les propriétés de l'ACE. Les options sont les suivantes :

- **Action : Permit/Deny (Autoriser/Refuser)** : indique si vous autorisez (en sélectionnant) le trafic décrit ou si vous le refusez (en le désélectionnant, aucune correspondance).
- **Address** (Adresse) : une définition de la destination ou de l'adresse cible du flux de trafic. Vous pouvez spécifier une adresse d'hôte telle que 10.100.1.1, un réseau (au format 10.100.1.0/24 ou 10.100.1.0/255.255.255.0), ou vous pouvez sélectionner un objet réseau (qui charge simplement le contenu de l'objet dans le champ d'adresse).
- **Description : une explication de l'objectif de l'ACE, jusqu'à 100 caractères par ligne.** Vous pouvez saisir plusieurs lignes ; chaque ligne est ajoutée en tant que remarque dans l'interface de ligne de commande, et les remarques sont placées avant l'ACE.

  Remarque
  Si vous ajoutez des remarques avec des caractères non anglais sur une plateforme (comme Windows), puis essayez de les supprimer d'une autre plateforme (comme Linux), vous ne pourrez peut-être pas les modifier ou les supprimer, car les caractères d'origine peuvent ne pas être correctement reconnus. Cette limitation est due à une dépendance de plateforme sous-jacente qui code différents caractères linguistiques de différentes manières.

Lorsque vous avez terminé de définir l'ACE, cliquez sur **OK** pour ajouter la règle au tableau.

Étape 5 Cliquez sur **Apply** (Appliquer).

Configurer les ACL de type Web

Les listes de contrôle d'accès de type Web sont utilisées pour filtrer le trafic VPN SSL sans client, ce qui restreint l'accès des utilisateurs à des réseaux, des sous-réseaux, des hôtes et des serveurs Web spécifiques. Si vous ne définissez pas de filtre, toutes les connexions sont autorisées. Une liste de contrôle d'accès de type Web est représentée comme un conteneur nommé d'ACE. Pour créer une nouvelle liste de contrôle d'accès, vous devez d'abord créer le conteneur. Vous pouvez ensuite ajouter des ACE, modifier les ACE existantes et réorganiser les ACE à l'aide de la table d'ACL Web. La table apparaît en tant que gestionnaire d'ACL lorsque vous configurez les listes de contrôle d'accès de type Web tout en configurant les politiques qui les utilisent. Si c'est le cas, les procédures sont les mêmes, à l'exception de la manière dont vous accédez à la fenêtre.

L'ACL de type Web peut inclure une combinaison d'adresses IPv4 et IPv6 en plus des spécifications d'URL.

Procédure

Étape 1 Choisissez **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Advanced** > **Web** > **ACLs** > **(Configuration** > **VPN d'accès à distance** > **Accès VPN SSL sans client** > **Avancé** > **ACL Web)**.

Étape 2 Si vous créez une nouvelle liste de contrôle d'accès, choisissez **Add** > **Add ACL** (Ajouter > Ajouter une ACL), saisissez un nom et cliquez sur OK (**OK**).

Le conteneur d'ACL est ajouté à la table. Vous pouvez la renommer ultérieurement en la sélectionnant et en cliquant sur **Edit** (Modifier).

Étape 3 Effectuez l'une des actions suivantes :

- Pour ajouter une ACE à la fin de la liste de contrôle d'accès, sélectionnez le nom de l'ACL ou une ACE qu'elle contient, puis choisissez **Add > Add ACE** (Ajouter > Ajouter une ACE).
- Pour insérer une ACE à un emplacement précis, sélectionnez une ACE existante et choisissez **Add > Insert** (Ajouter > Insérer) pour ajouter l'ACE au-dessus de la règle, ou **Add > Insert After** (Ajouter > Insérer après).
- Pour modifier une règle, sélectionnez-la et cliquez sur **Edit** (Modifier).

Étape 4 Renseignez les propriétés de l'ACE. Les principales options à sélectionner sont :

- **Action : Permit (Autoriser)/Deny (Refuser)** : indique si vous autorisez (en sélectionnant) le trafic décrit ou si vous le refusez (en le désélectionnant; il ne correspond alors pas).
- **Filter** (Filtre) : critères de correspondance du trafic en fonction de la destination. Vous pouvez soit spécifier une URL en sélectionnant le protocole et en saisissant le nom du serveur et, éventuellement, le chemin d'accès et le nom du fichier, ou vous pouvez spécifier une adresse de destination IPv4 ou IPv6 et un service TCP.

Pour des informations détaillées sur les options, consultez Propriétés des ACE Webtype, à la page 62.

Lorsque vous avez terminé de définir l'ACE, cliquez sur **OK** pour ajouter la règle au tableau.

Étape 5 Cliquez sur **Apply** (Appliquer).

Propriétés des ACE Webtype

Lorsque vous ajoutez ou modifiez une ACE dans une liste de contrôle d'accès de type Web, vous pouvez configurer les propriétés suivantes. Dans de nombreux champs, vous pouvez cliquer sur le bouton « ... » à droite de la zone d'édition pour sélectionner, créer ou modifier des objets disponibles pour le champ.

Pour une ACE donnée, vous pouvez filtrer par URL ou adresse, mais pas les deux.

- **Action : Permit/Deny (Autoriser/Refuser)** : indique si vous autorisez (en sélectionnant) le trafic décrit ou si vous le refusez (en le désélectionnant, aucune correspondance).
  - **Filter on URL** (Filtrer sur l'URL) : correspondance du trafic en fonction de l'URL de destination. Sélectionnez le protocole et saisissez le nom du serveur et, éventuellement, le chemin d'accès et le

nom du fichier. Par exemple, http://www.example.com ou, pour couvrir tous les serveurs, http://*.example.com. Voici quelques conseils et limites sur la spécification des URL :

- Sélectionnez **any** pour faire correspondre toutes les URL.
- La fonction « permit url any » autorisera toutes les URL qui ont le format protocole://server-ip/path et bloquera le trafic qui ne correspond pas à ce modèle, comme le transfert de port. Il doit y avoir une commande ACE pour autoriser les connexions au port requis (port 1494 dans le cas de Citrix) afin qu'un refus implicite ne se produise pas.
- Les modules d'extension de tunnel Smart et ica ne sont pas touchés par une liste de contrôle d'accès avec « autoriser l'URL n'importe quel », car ils correspondent uniquement aux types smart-tunnel:// et ica://.
- Vous pouvez utiliser les protocoles suivants : cifs://, citrix://, citrixs://, ftp://, http://, https://, imap4://, nfs://, pop3://, smart-tunnel:// et smtp://. Vous pouvez également utiliser des caractères génériques dans le protocole; par exemple, htt* correspond à http et https, et un astérisque * correspond à tous les protocoles. Par exemple, ://.example.com correspond à tout trafic de type URL vers le réseau example.com.
- Si vous spécifiez une URL smart-tunnel://, vous pouvez inclure le nom du serveur uniquement. L'URL ne peut pas contenir de chemin. Par exemple, smart-tunnel://www.example.com est acceptable, mais smart-tunnel://www.example.com/index.html ne l'est pas.
- Un astérisque * correspond à zéro ou à un nombre quelconque de caractères. Pour faire correspondre une URL http, saisissez http://*/*.
- Un point d'interrogation ? correspond exactement à un caractère.
- Les crochets [] sont des opérateurs de plage, correspondant à n'importe quel caractère dans la plage. Par exemple, pour faire correspondre à la fois http://www.cisco.com:80/ et http://www.cisco.com:81/, saisissez **http://www.cisco.com:8[01]/**.

- **Filter on Address and Service** (Filtrer sur l'adresse et le service) : correspondance du trafic en fonction de l'adresse de destination et du service.
  - **Address** (Adresse) : adresse IPv4 ou IPv6 de la destination. Pour faire correspondre toutes les adresses, vous pouvez utiliser **any**, qui correspond à toutes les adresses IPv4 ou IPv6, **any4** pour correspondre à IPv4 uniquement, ou **any6** pour correspondre uniquement à IPv6. Vous pouvez spécifier une adresse d'hôte unique (comme 10.100.10.5 ou 2001:DB8::0DB8:800:200C:417A), ou un sous-réseau (au format 10.100.10.0/24 ou 10.100.10.0/255.255.255.0, ou pour IPv6, 2001:DB8:0:CD30::/60).
  - **Service** : une seule spécification de service TCP. La valeur par défaut est **tcp** sans port, mais vous pouvez spécifier un seul port (comme tcp/80 ou tcp/www) ou une plage de ports (comme tcp/1-100). Vous pouvez inclure des opérateurs; par exemple, !=tcp/80 exclut le port 80; <tcp/80 correspond à tous les ports inférieurs à 80; >tcp/80 correspond à tous les ports supérieurs à 80.

- **Enable Logging (Activer la journalisation)** ; **Logging Level (Niveau de journalisation)** ; **More Options (Autres options) > Logging Interval** (Intervalle de journalisation) : les options de journalisation définissent la façon dont les messages syslog seront générés pour les règles qui refusent réellement le trafic. Vous pouvez implémenter les options de journalisation suivantes :

- **Désélectionnez Enable Logging** (Activer la journalisation) : cela désactive la journalisation pour la règle. Aucun message de journal système d'aucun type ne sera émis pour le trafic refusé par cette règle.
- **Sélectionnez Enable Logging (Activer la journalisation) avec Logging Level (Niveau de journalisation) = Default** (Par défaut) : cela fournit la journalisation par défaut pour les règles. Le message de journal système 106103 est émis pour chaque paquet refusé. Si le périphérique est soumis à une attaque, la fréquence d'émission de ce message peut avoir une incidence sur les services.
- **Sélectionnez Enable Logging (Activer la journalisation) avec Non-Default Logging Level** (Niveau de journalisation autre que celui par défaut) : cela fournit un message syslog résumé, 106102, au lieu de 106103. Le message 106102 est émis lors de la première occurrence, puis à nouveau à chaque intervalle configuré dans **More Options (Autres options) > Logging Interval** (Intervalle de journalisation) (la valeur par défaut est toutes les 300 secondes, vous pouvez spécifier 1–600), en affichant le nombre d'occurrences pendant cet intervalle. Le niveau de journalisation recommandé est **Informational** (Informationnel).

- **More Options (Autres options) > Time Range (Plage de temps)** : nom de l'objet de plage temporelle qui définit les heures du jour et les jours de la semaine où la règle doit être active. Si vous ne spécifiez pas de plage temporelle, la règle est toujours active.

Exemples d'ACL de type Web

Voici quelques exemples de règles basées sur URL pour les listes de contrôle d'accès de type Web.

	Filtre	Incidence
Refuser	url http://*.yahoo.com/	Refuse l'accès à l'ensemble de Yahoo!
Refuser	url cifs://fileserver/share/directory	Refuse l'accès à tous les fichiers de l'emplacement spécifié.
Refuser	url https://www.example.com/ directory/file.html	Refuse l'accès au fichier précisé.
Autoriser	url https://www.example.com/directory	Permet l'accès à l'emplacement précisé.
Refuser	url http://*:8080/	Refuse l'accès HTTP de n'importe où via le port 8080.
Refuser	url http://10.10.10.10	Refuse l'accès HTTP à 10.10.10.10.
Autoriser	url any	Permet l'accès à n'importe quelle URL. Généralement utilisé après une liste de contrôle d'accès qui refuse l'accès à l'URL.

Surveillance des ACL

Les tableaux ACL Manager (Gestionnaire d'ACL), Standard ACL (ACL standard), Web ACL (ACL Web) et EtherType ACL (ACL EtherType) affichent une vue consolidée des listes de contrôle d'accès. Mais pour voir exactement ce qui est configuré sur le périphérique, vous pouvez utiliser les commandes suivantes. Saisissez les commandes dans **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**.

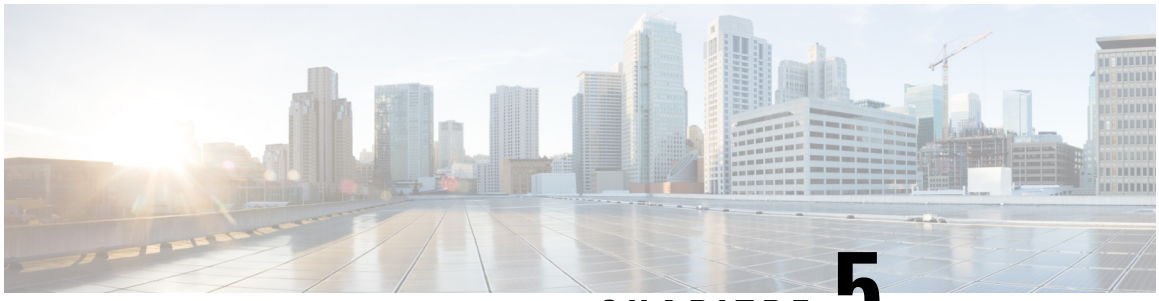
- **show access-list** [*name*] : affiche les listes d'accès, y compris le numéro de ligne pour chaque ACE et le nombre de résultats. Incluez un nom d'ACL ou vous verrez toutes les listes d'accès.
- **show running-config access-list** [*name*] : affiche la configuration actuelle de la liste d'accès en cours d'exécution. Incluez un nom d'ACL ou vous verrez toutes les listes d'accès.

Historique des ACL

Nom de la caractéristique	Versions	Description
ACL étendues, standard, de type Web	7.0(1)	Les listes de contrôle d'accès sont utilisées pour contrôler l'accès au réseau ou pour spécifier le trafic sur lequel de nombreuses fonctionnalités doivent agir. Une liste de contrôle d'accès étendue est utilisée pour le contrôle d'accès traversant le boîtier et plusieurs autres fonctionnalités. Les listes de contrôle d'accès standard sont utilisées dans les cartes de routage et les filtres VPN. Les listes de contrôle d'accès de type Web sont utilisées dans le filtrage VPN SSL sans client. Les listes de contrôle d'accès EtherType contrôlent le trafic de couche 2 non IP. Nous avons ajouté le gestionnaire d'ACL et d'autres pages pour configurer les listes de contrôle d'accès.
Adresses IP réelles dans les listes de contrôle d'accès étendues	8.3(1)	Lors de l'utilisation de la NAT ou de la PAT, les adresses et les ports mappés ne sont plus utilisés dans une liste de contrôle d'accès pour plusieurs fonctionnalités. Vous devez utiliser les adresses et les ports réels non traduits pour ces fonctionnalités. L'utilisation de l'adresse et du port réels signifie que si la configuration de la NAT change, vous n'avez pas besoin de modifier les listes de contrôle d'accès.
Prise en charge du pare-feu d'identité dans les listes de contrôle d'accès étendues	8.4(2)	Vous pouvez maintenant utiliser des utilisateurs et des groupes de pare-feu d'identité pour la source et la destination. Vous pouvez utiliser une liste de contrôle d'accès de pare-feu d'identité avec des règles d'accès, des règles AAA et pour l'authentification VPN.
Prise en charge d'EtherType ACL pour le trafic IS-IS	8.4(5), 9.1(2)	En mode de pare-feu transparent, l'ASA peut désormais contrôler le trafic IS-IS à l'aide d'une liste de contrôle d'accès EtherType. Nous avons modifié l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > EtherType Rules (Règles EtherType).
Prise en charge de Cisco TrustSec dans les listes de contrôle d'accès étendues	9.0(1)	Vous pouvez maintenant utiliser les groupes de sécurité Cisco TrustSec pour la source et la destination. Vous pouvez utiliser une liste de contrôle d'accès de pare-feu d'identité avec des règles d'accès.

Nom de la caractéristique	Versions	Description
ACL unifiées étendues et de type Web pour IPv4 et IPv6	9.0(1)	Les listes de contrôle d'accès étendues et de type Web prennent désormais en charge les adresses IPv4 et IPv6. Vous pouvez même spécifier une combinaison d'adresses IPv4 et IPv6 pour la source et la destination. Le mot-clé **any** a été modifié pour représenter le trafic IPv4 et IPv6. Les mots-clés **any4** et **any6** ont été ajoutés pour représenter le trafic IPv4 uniquement et IPv6 uniquement, respectivement. Les listes de contrôle d'accès propres à IPv6 sont obsolètes. Les listes de contrôle d'accès IPv6 existantes sont migrées vers des listes de contrôle d'accès étendues. Pour en savoir plus, consultez les notes de mise à jour. Nous avons modifié les écrans suivants : Configuration > Firewall (Pare-feu) > Access Rules (Critères d'accès) Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau [client]) > Group Policies (Stratégies de groupe) > General (Général) > More Options (Autres options)
Amélioration des ACL étendues et des objets pour filtrer le trafic ICMP par code ICMP	9.0(1)	Le trafic ICMP peut maintenant être autorisé ou refusé en fonction du code ICMP. Nous avons introduit ou modifié les écrans suivants : Configuration > Firewall (Pare-feu) > Objects (Objets) > Service Objects/Groups (Objets/groupes de services) Configuration > Firewall (Pare-feu) > Access Rules (Critères d'accès)
Session de configuration pour modifier les listes de contrôle d'accès et les objets. Référencement ultérieur des objets et des listes de contrôle d'accès dans les règles d'accès.	9.3(2)	Vous pouvez maintenant modifier les listes de contrôle d'accès et les objets dans une session de configuration isolée. Vous pouvez également référencer des objets et des ACL à l'avance, c'est-à-dire configurer des règles et des groupes d'accès pour des objets ou des ACL qui n'existent pas encore. Nous avons modifié les paramètres avancés pour les règles d'accès.
Prise en charge d'ACL pour le protocole SCTP (Stream Control Transmission Protocol)	9.5(2)	Vous pouvez maintenant créer des règles d'ACL à l'aide du protocole **sctp**, y compris les spécifications de port. Nous avons modifié les boîtes de dialogue d'ajout/modification pour les entrées de contrôle d'accès sur la page **Configuration** > **Firewall** > **Advanced** > **ACL Manager**.
Prise en charge de la règle Ethertype pour l'adresse du point d'accès au service de destination du paquet de contrôle de liaison logique IEEE 802.2.	9.6(2)	Vous pouvez maintenant écrire des règles de contrôle d'accès Ethertype pour l'adresse du point d'accès de service de destination du paquet de contrôle de liaison logique IEEE 802.2. En raison de cet ajout, le mot clé **bpdu** ne correspond plus au trafic prévu. Réécrivez les règles **bpdu** pour utiliser **dsap 0x42**. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **EtherType Rules (Règles EtherType)**.

Nom de la caractéristique	Versions	Description
Prise en charge en mode routé des règles Ethertype sur les interfaces membres de groupe de ponts et des règles d'accès étendues sur les interfaces virtuelles de groupe de ponts (BVI).	9.7(1)	Vous pouvez maintenant créer des listes de contrôle d'accès Ethertype et les appliquer aux interfaces membres de groupes de ponts en mode routé. Vous pouvez également appliquer des règles d'accès étendues à la BVI (Bridge Virtual Interface) en plus des interfaces membres. Nous avons modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Règles d'accès)**, **Configuration** > **Firewall (Pare-feu)** > **Ethertype Rules (Règles Ethertype)**.
Modifications de la liste de contrôle d'accès Ethertype.	9.9(1)	Les listes de contrôle d'accès EtherType prennent désormais en charge Ethernet II IPX (EII IPX). En outre, de nouveaux mots clés sont ajoutés au mot clé DSAP pour prendre en charge les valeurs DSAP courantes : BPDU (0x42), IPX (0xE0), IPX brut (0xFF) et ISIS (0xFE). Par conséquent, les entrées de contrôle d'accès EtherType existantes qui utilisent les mots-clés BPDU ou ISIS seront converties automatiquement pour utiliser la spécification DSAP, et les règles pour IPX seront converties en trois règles (DSAP IPX, DSAP brut IPX et EII IPX). De plus, la capture de paquets qui utilise IPX comme valeur EtherType est obsolète, car IPX correspond à trois EtherTypes distincts. Nous avons modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **EtherType Rules (Règles EtherType)**.
Prise en charge des groupes d'objets de service réseau dans les listes de contrôle d'accès étendues.	9.17(1)	Vous pouvez utiliser des objets de service réseau comme critères de source et de destination dans les listes de contrôle d'accès étendues et les règles de contrôle d'accès. Nous avons modifié l'écran suivant : Add/Edit extended ACE or access rule (Ajouter/Modifier une ACE étendue ou une règle d'accès) sur la page Firewall (Pare-feu).
Le référencement direct des ACL et des objets est toujours activé. De plus, la recherche de groupes d'objets pour le contrôle d'accès est désormais activée par défaut.	9.18(1)	Vous pouvez faire référence à des ACL ou à des objets réseau qui n'existent pas encore lors de la configuration de groupes d'accès ou de critères d'accès. De plus, la recherche de groupes d'objets est désormais activée par défaut pour le contrôle d'accès pour les *nouveaux* déploiements. Cette commande restera désactivée lors de la mise à niveau des périphériques. Si vous souhaitez l'activer (conseillé), vous devez le faire manuellement. Nous avons supprimé la commande **forward-reference enable** et modifié la valeur par défaut pour **object-group-search access-control** afin de l'activer.



CHAPITRE 5

ASA et Cisco TrustSec

Ce chapitre décrit comment mettre en œuvre Cisco TrustSec pour l'ASA.

- À propos de Cisco TrustSec, à la page 69
- Lignes directrices relatives à Cisco TrustSec, à la page 77
- Configurer l'ASA pour s'intégrer à Cisco TrustSec, à la page 80
- Prise en charge de Cisco TrustSec pour les VPN Secure Client (services client sécurisés), à la page 91
- Surveillance de Cisco TrustSec, à la page 92
- Historique de Cisco TrustSec, à la page 93

À propos de Cisco TrustSec

Traditionnellement, les fonctionnalités de sécurité telles que les pare-feu effectuent un contrôle d'accès en fonction d'adresses IP, de sous-réseaux et de protocoles prédéfinis. Cependant, avec la transition des entreprises vers des réseaux sans frontières, la technologie utilisée pour connecter les personnes et les entreprises ainsi que les exigences de sécurité pour la protection des données et des réseaux ont considérablement changé. Les terminaux sont de plus en plus mobiles et les utilisateurs utilisent souvent une variété de terminaux (par exemple, ordinateur portable ou ordinateur de bureau, téléphone intelligent ou tablette), ce qui signifie qu'une combinaison d'attributs d'utilisateur et d'attributs de terminal fournit les caractéristiques clés (en plus des règles basées sur des 6-tuples), que les périphériques d'application tels que les commutateurs et les routeurs avec fonctionnalités de pare-feu ou pare-feu dédiés peuvent utiliser de manière fiable pour prendre des décisions en matière de contrôle d'accès.

Par conséquent, la disponibilité et la propagation des attributs de terminal ou des attributs d'identité du client sont devenues des exigences de plus en plus importantes pour assurer la sécurité sur les réseaux des clients, aux couches d'accès, de distribution et de cœur du réseau, ainsi que dans le centre de données.

Cisco TrustSec fournit un contrôle d'accès qui s'appuie sur une infrastructure existante de prise en compte de l'identité pour assurer la confidentialité des données entre les périphériques réseau et intégrer les services d'accès de sécurité sur une seule plateforme. Dans la fonctionnalité Cisco TrustSec, les appareils d'application utilisent une combinaison d'attributs d'utilisateur et d'attributs de terminal pour prendre des décisions de contrôle d'accès basées sur les rôles et l'identité. La disponibilité et la propagation de ces informations permettent la sécurité sur les réseaux au niveau de l'accès, de la distribution et du cœur du réseau.

La mise en œuvre de Cisco TrustSec dans votre environnement présente les avantages suivants :

- Fournit à une main-d'œuvre mobile et complexe en pleine croissance un accès approprié et plus sécurisé à partir de n'importe quel périphérique

- Réduit les risques de sécurité en fournissant une visibilité complète sur qui et ce qui se connecte au réseau filaire ou sans fil
- Offre un contrôle exceptionnel sur l'activité des utilisateurs du réseau qui accèdent aux ressources informatiques physiques ou en nuage
- Réduit le coût total d'acquisition grâce à une gestion centralisée et hautement sécurisée des politiques d'accès et à des mécanismes d'application évolutifs
- Pour en savoir plus, consultez les URL suivantes :
  - Description du système Cisco TrustSec et de l'architecture pour l'entreprise.

    http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html
  - Des instructions pour le déploiement de la solution Cisco TrustSec dans l'entreprise, y compris des liens vers des guides de conception de composants.

    http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_DesignZone_TrustSec.html
  - Un aperçu de la solution Cisco TrustSec lorsqu'elle est utilisée avec l'ASA, les commutateurs, les contrôleurs de réseau local sans fil (WLAN) et les routeurs.

    http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/trustsec/solution_overview_c22-591771.pdf
  - La matrice de prise en charge de la plateforme Cisco TrustSec, qui répertorie les produits Cisco qui prennent en charge la solution Cisco TrustSec.

    http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html

À propos de la prise en charge de SGT et SXP dans Cisco TrustSec

Dans la fonctionnalité Cisco TrustSec, l'accès de groupe de sécurité modifie un réseau compatible avec la topologie en un réseau basé sur les rôles, ce qui permet l'application des politiques de bout en bout sur la base du contrôle d'accès basé sur les rôles (RBAC). Les informations d'authentification du périphérique et de l'utilisateur obtenues lors de l'authentification sont utilisées pour classer les paquets par groupe de sécurité. Chaque paquet entrant dans le nuage Cisco TrustSec est marqué par une balise de groupe de sécurité (SGT). Le balisage aide les intermédiaires de confiance à identifier l'identité de la source du paquet et à appliquer les politiques de sécurité tout au long du chemin de données. Une balise SGT peut indiquer un niveau de privilège dans le domaine lorsqu'elle est utilisée pour définir une liste de contrôle d'accès de groupe de sécurité.

Une balise SGT est attribuée à un périphérique par le biais de l'authentification IEEE 802.1X, de l'authentification Web ou du contournement de l'authentification MAC (MAB), qui se produit avec un attribut propre au fournisseur RADIUS. Une balise SGT peut être affectée de manière statique à une adresse IP particulière ou à une interface de commutation. Une balise SGT est transmise dynamiquement à un commutateur ou à un point d'accès après l'authentification réussie.

Le protocole SXP (Security-group eXchange Protocol) est un protocole mis au point pour Cisco TrustSec afin de propager la base de données de mappage IP-SGT des périphériques réseau qui ne prennent pas en charge le matériel compatible avec SGT vers le matériel qui prend en charge les SGT et les listes de contrôle d'accès de groupes de sécurité. SXP, un protocole de plan de contrôle, transmet le mappage IP-SGT des points d'authentification (comme les anciens commutateurs de couche d'accès) aux périphériques en amont du réseau.

Les connexions SXP sont point à point et utilisent TCP comme protocole de transport sous-jacent. SXP utilise le port TCP 64999 pour amorcer une connexion. En outre, une connexion SXP est identifiée de manière unique par les adresses IP source et de destination.

Rôles dans la fonctionnalité Cisco TrustSec

Pour fournir une application d'identité et d'accès basée sur les politiques, la fonctionnalité Cisco TrustSec comprend les rôles suivants :

- Demandeur d'accès (AR) : Les demandeurs d'accès sont des périphériques terminaux qui demandent l'accès aux ressources protégées dans le réseau. Ce sont des sujets principaux de l'architecture et leur privilège d'accès dépend de leurs informations d'authentification.

  Les demandeurs d'accès comprennent des périphériques de terminal tels que les PC, les ordinateurs portables, les téléphones portables, les imprimantes, les caméras et les téléphones IP compatibles avec le protocole MACsec.

- Point de décision des politiques (PDP) : un point de décision des politiques est responsable de prendre des décisions en matière de contrôle d'accès. Le PDP fournit des fonctionnalités telles que 802.1x, MAB et l'authentification Web. Le PDP prend en charge l'autorisation et l'application par le biais du VLAN, de la DACL et de l'accès au groupe de sécurité (SGACL/SXP/SGT).

  Dans la fonctionnalité Cisco TrustSec, le moteur de services de vérification des identités de Cisco (ISE) agit comme PDP. Cisco ISE fournit des fonctionnalités de politique de contrôle d'identité et d'accès.

- Point d'information sur les politiques (PIP) : un point d'information sur les politiques est une source qui fournit des informations externes (par exemple, réputation, emplacement et attributs LDAP) aux points de décision des politiques.

  Les points d'information sur les politiques comprennent des périphériques tels que le répertoire de session, le capteur IPS et le gestionnaire de communication.

- Point d'administration des politiques (PAP) : un point d'administration des politiques définit et insère les politiques dans le système d'autorisation. La PAP agit comme un référentiel d'identité en fournissant un mappage d'identité balise Cisco TrustSec-utilisateur et un mappage d'identité balise-serveur Cisco TrustSec.

  Dans la fonctionnalité Cisco TrustSec, le système de contrôle d'accès sécurisé Cisco (un serveur de politiques avec prise en charge intégrée de 802.1x et SGT) sert de PAP.

- Point d'application des politiques (PEP) : un point d'application des politiques est l'entité qui exécute les décisions (règles et actions de politique) prises par le PDP pour chaque AR. Les périphériques PEP obtiennent des informations d'identité par le biais du chemin de communication principal qui existe dans les réseaux. Les périphériques PEP connaissent les attributs d'identité de chaque AR de nombreuses sources, telles que les agents de terminal, les serveurs d'autorisation, les périphériques d'application homologues et les flux réseau. À leur tour, les périphériques PEP utilisent SXP pour propager le mappage IP-SGT vers des périphériques homologues de confiance mutuelle dans le réseau.

  Les points d'application des politiques comprennent des périphériques réseau tels que les commutateurs Catalyst, les routeurs, les pare-feu (en particulier l'ASA), les serveurs, les périphériques VPN et les périphériques SAN.

L'ASA sert le rôle de PEP dans l'architecture d'identité. À l'aide de SXP, l'ASA obtient les informations d'identité directement des points d'authentification et les utilise pour appliquer les politiques basées sur l'identité.

Application de la politique de groupe de sécurité

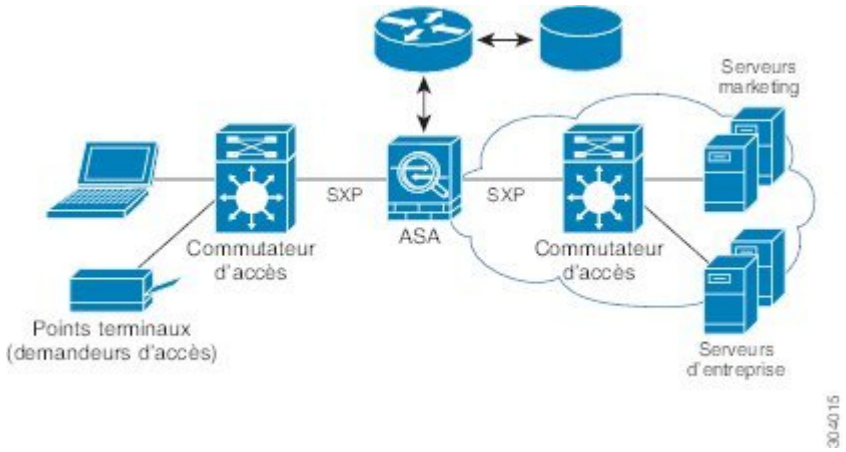
L'application de la politique de sécurité est basée sur le nom du groupe de sécurité. Un périphérique terminal tente d'accéder à une ressource dans le centre de données. Par rapport aux politiques traditionnelles basées sur IP configurées sur les pare-feu, les politiques basées sur l'identité sont configurées en fonction des identités d'utilisateur et de périphérique. Par exemple, mktg-contractor est autorisé à accéder à mktg-servers; mktg-corp-users sont autorisés à accéder à mktg-server et corp-servers.

Les avantages de ce type de déploiement sont les suivants :

- Le groupe d'utilisateurs et les ressources sont définis et appliqués à l'aide d'une gestion simplifiée des politiques d'objet unique (SGT).
- L'identité de l'utilisateur et l'identité de la ressource sont conservées dans toute l'infrastructure de commutation compatible avec Cisco TrustSec.

La figure suivante montre un déploiement pour l'application d'une politique basée sur le nom de groupe de sécurité.

Illustration 3 : Déploiement de l'application des politiques basées sur le nom de groupe de sécurité



La mise en œuvre de Cisco TrustSec vous permet de configurer des politiques de sécurité qui prennent en charge la segmentation des serveurs et comprend les fonctionnalités suivantes :

- Un ensemble de serveurs peut se voir attribuer une balise SGT pour simplifier la gestion des politiques.
- Les informations SGT sont conservées dans l'infrastructure des commutateurs compatibles avec Cisco TrustSec.
- L'ASA peut utiliser le mappage IP-SGT pour appliquer les politiques dans le domaine Cisco TrustSec.
- La simplification du déploiement est possible, car l'autorisation 802.1x pour les serveurs est obligatoire.

Comment l'ASA applique les politiques basées sur les groupes de sécurité

Remarque Les politiques de sécurité basées sur l'utilisateur et les politiques basées sur les groupes de sécurité peuvent coexister sur l'ASA. Toute combinaison d'attributs de réseau, d'utilisateurs et de groupes de sécurité peut être configurée dans une politique de sécurité.

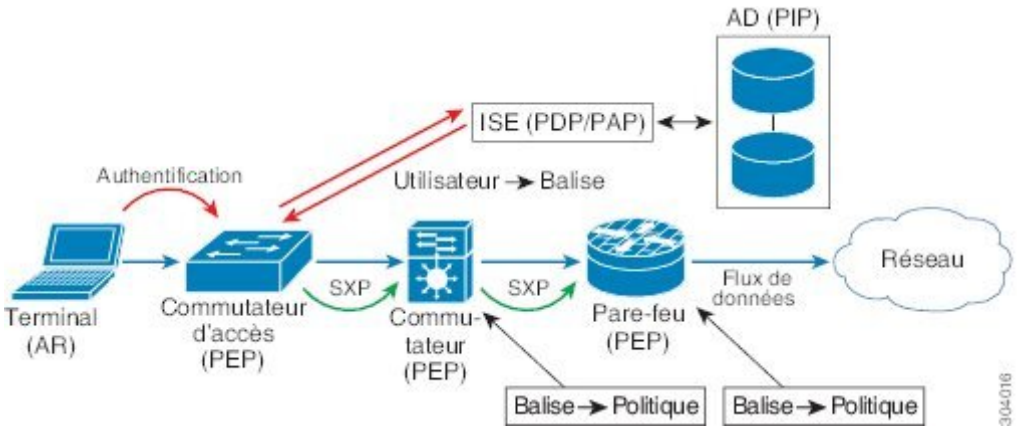
Pour configurer l'ASA pour qu'il fonctionne avec Cisco TrustSec, vous devez importer un fichier d'identifiant d'accès protégé (PAC) à partir de l'ISE.

L'importation du fichier PAC dans l'ASA établit un canal de communication sécurisé avec l'ISE. Une fois le canal établi, l'ASA amorce une transaction RADIUS sécurisée PAC avec l'ISE et télécharge les données d'environnement Cisco TrustSec (c'est-à-dire la table du groupe de sécurité). La table des groupes de sécurité mappe les balises SGT aux noms de groupes de sécurité. Les noms de groupes de sécurité sont créés sur l'ISE et fournissent des noms conviviaux pour les groupes de sécurité.

La première fois que l'ASA télécharge la table de groupes de sécurité, il parcourt toutes les entrées de la table et résout tous les noms de groupes de sécurité inclus dans les politiques de sécurité qui ont été configurées sur celui-ci; puis l'ASA active ces politiques de sécurité localement. Si l'ASA ne peut pas résoudre un nom de groupe de sécurité, il génère un message syslog pour le nom de groupe de sécurité inconnu.

La figure suivante montre comment une politique de sécurité est appliquée dans Cisco TrustSec.

Illustration 4 : Application de la politique de sécurité



1. Un terminal se connecte à un périphérique de couche d'accès directement ou par accès à distance et s'authentifie auprès de Cisco TrustSec.
2. Le périphérique de couche d'accès authentifie le terminal auprès de l'ISE en utilisant des méthodes d'authentification telles que 802.1X ou l'authentification Web. Le terminal transmet les informations de rôle et d'appartenance au groupe pour classer le périphérique dans le groupe de sécurité approprié.
3. Le périphérique de couche d'accès utilise SXP pour propager le mappage IP-SGT vers les périphériques en amont.
4. L'ASA reçoit le paquet et recherche les SGT des adresses IP source et de destination à l'aide du mappage IP-SGT transmis par SXP.

Si le mappage est nouveau, l'ASA l'enregistre dans sa base de données IP-SGT Manager locale. La base de données IP-SGT Manager, qui s'exécute dans le plan de commande, suit le mappage IP-SGT pour chaque adresse IPv4 ou IPv6. La base de données enregistre la source à partir de laquelle le mappage a été appris. L'adresse IP homologue de la connexion SXP est utilisée comme source du mappage. Plusieurs sources peuvent exister pour chaque entrée mappée IP-SGT.

Si l'ASA est configuré en tant que Speaker, l'ASA transmet toutes les entrées de mappage IP-SGT à ses homologues SXP.

5. Si une politique de sécurité est configurée sur l'ASA avec ce SGT ou ce nom de groupe de sécurité, l'ASA applique la politique. (Vous pouvez créer des politiques de sécurité sur l'ASA qui incluent des SGT ou des noms de groupes de sécurité. Pour appliquer les politiques en fonction des noms de groupe de sécurité, l'ASA a besoin de la table de groupe de sécurité pour mapper les noms de groupe de sécurité aux SGT.)

   Si l'ASA ne peut pas trouver de nom de groupe de sécurité dans la table des groupes de sécurité et qu'il est inclus dans une politique de sécurité, l'ASA considère le nom du groupe de sécurité comme inconnu et génère un message syslog. Après que l'ASA a actualisé la table des groupes de sécurité à partir de l'ISE et a appris le nom du groupe de sécurité, l'ASA génère un message syslog indiquant que le nom du groupe de sécurité est connu.

Effets des modifications des groupes de sécurité sur l'ISE

L'ASA actualise périodiquement la table du groupe de sécurité en téléchargeant une table mise à jour à partir de l'ISE. Les groupes de sécurité peuvent changer sur l'ISE entre les téléchargements. Ces modifications ne sont pas répercutées sur l'ASA tant qu'il n'a pas actualisé la table des groupes de sécurité.

Astuces Nous vous recommandons de planifier les modifications de configuration des politiques sur l'ISE pendant une fenêtre de maintenance, puis d'actualiser manuellement la table des groupes de sécurité sur l'ASA pour vous assurer que les modifications des groupes de sécurité ont été intégrées.

Le traitement des modifications de configuration des politiques de cette manière optimise les possibilités de résolution du nom de groupe de sécurité et d'activation immédiate des politiques de sécurité.

La table du groupe de sécurité est automatiquement actualisée à l'expiration de la minuterie des données d'environnement. Vous pouvez également déclencher une actualisation du tableau de groupe de sécurité sur demande.

Si un groupe de sécurité change sur l'ISE, les événements suivants se produisent lorsque l'ASA actualise la table du groupe de sécurité :

- Seules les politiques de groupes de sécurité qui ont été configurées à l'aide de noms de groupes de sécurité doivent être résolues avec la table de groupes de sécurité. Les politiques qui comprennent des balises de groupe de sécurité sont toujours actives.
- Lorsque la table des groupes de sécurité est disponible pour la première fois, toutes les politiques utilisant des noms de groupes de sécurité sont parcourues, les noms de groupes de sécurité sont résolus et les politiques sont activées. Toutes les politiques utilisant des balises sont parcourues et des messages syslog sont générés pour les balises inconnues.
- Si la table de groupe de sécurité a expiré, les politiques continuent d'être appliquées en fonction de la dernière table de groupe de sécurité téléchargée jusqu'à ce que vous l'effaciez ou qu'une nouvelle table soit disponible.

- Lorsqu'un nom de groupe de sécurité résolu devient inconnu sur l'ASA, la politique de sécurité est désactivée; toutefois, elle demeure dans la configuration en cours d'exécution de l'ASA.
- Si un groupe de sécurité existant est supprimé sur le PAP, une balise de groupe de sécurité connue précédemment peut devenir inconnue, mais aucun changement dans l'état de la politique ne se produit sur l'ASA. Un nom de groupe de sécurité connu précédemment peut ne pas être résolu, et la politique est alors inactivée. Si le nom du groupe de sécurité est réutilisé, la politique est recompilée à l'aide de la nouvelle balise.
- Si un nouveau groupe de sécurité est ajouté sur le PAP, une balise de groupe de sécurité inconnue précédemment peut être connue, un message syslog est généré, mais aucun changement dans l'état de la politique ne se produit. Un nom de groupe de sécurité inconnu précédemment peut être résolu, et les politiques associées sont ensuite activées.
- Si une balise a été renommée sur le PAP, les politiques qui ont été configurées à l'aide de balises affichent le nouveau nom, et aucun changement dans l'état des politiques ne se produit. Les politiques qui ont été configurées avec des noms de groupes de sécurité sont recompilées à l'aide de la nouvelle valeur de balise.

Rôles de speaker et de listener sur l'ASA

L'ASA prend en charge SXP pour envoyer et recevoir des entrées de mappage IP-SGT à destination et en provenance d'autres périphériques réseau. L'utilisation de SXP permet aux périphériques de sécurité et aux pare-feu d'obtenir les informations d'identité des commutateurs d'accès sans qu'il soit nécessaire de procéder à des mises à niveau ou à des modifications du matériel. SXP peut également être utilisé pour transmettre les entrées de mappage IP-SGT des périphériques en amont (comme les périphériques de centre de données) vers les périphériques en aval. L'ASA peut recevoir des informations des directions en amont et en aval.

Lors de la configuration d'une connexion SXP sur l'ASA avec un homologue SXP, vous devez désigner l'ASA comme Speaker ou Listener pour cette connexion afin qu'il puisse échanger des informations d'identité :

- Mode Speaker : configure l'ASA afin qu'il puisse transférer toutes les entrées de mappage IP-SGT actives collectées sur l'ASA vers des périphériques en amont pour l'application des politiques.
- Mode Listener : configure l'ASA afin qu'il puisse recevoir des entrées de mappage IP-SGT des périphériques en aval (commutateurs compatibles avec SGT) et utiliser ces informations pour créer des définitions de politique.

Si une extrémité d'une connexion SXP est configurée en tant que Speaker, l'autre extrémité doit être configurée en tant que Listener, et vice versa. Si les deux périphériques à chaque extrémité d'une connexion SXP sont configurés avec le même rôle (soit les deux comme Speakers, soit les deux comme Listeners), la connexion SXP échoue et l'ASA génère un message syslog.

Plusieurs connexions SXP peuvent apprendre les entrées de mappage IP-SGT qui ont été téléchargées à partir de la base de données de mappage IP-SGT. Après l'établissement d'une connexion SXP avec un homologue SXP sur l'ASA, le Listener télécharge l'ensemble de la base de données de mappage IP-SGT à partir du Speaker. Toutes les modifications apportées après cela ne sont envoyées que lorsqu'un nouveau périphérique apparaît sur le réseau. Par conséquent, le débit du flux d'informations SXP est conditionnel au débit auquel les hôtes terminaux s'authentifient auprès du réseau.

Les entrées de mappage IP-SGT qui ont été apprises des connexions SXP sont conservées dans la base de données de mappage SXP IP-SGT. Les mêmes entrées de mappage peuvent être apprises de différentes connexions SXP. La base de données de mappage conserve une copie pour chaque entrée de mappage apprise. Plusieurs entrées de mappage de la même valeur de mappage IP-SGT sont identifiées par l'adresse IP homologue

de la connexion à partir de laquelle le mappage a été appris. SXP demande au gestionnaire IP-SGT d'ajouter une entrée de mappage lorsqu'un nouveau mappage est appris pour la première fois et de supprimer une entrée de mappage lorsque la dernière copie dans la base de données SXP est supprimée.

Chaque fois qu'une connexion SXP est configurée en tant que Speaker, SXP demande au gestionnaire IP-SGT de transférer toutes les entrées de mappage collectées sur le périphérique vers l'homologue. Lorsqu'un nouveau mappage est appris localement, le gestionnaire IP-SGT demande à SXP de le transmettre par des connexions configurées comme Speakers.

La configuration de l'ASA pour qu'il soit à la fois Speaker et Listener pour une connexion SXP peut entraîner une boucle SXP, ce qui signifie que les données SXP peuvent être reçues par un homologue SXP qui les a transmises à l'origine.

Enregistrer l'ASA auprès de l'ISE

L'ASA doit être configurée comme un appareil réseau Cisco TrustSec reconnu dans l'ISE avant que l'ASA puisse importer avec succès un fichier PAC. Pour enregistrer l'ASA auprès de l'ISE, procédez comme suit :

Procédure

Étape 1 Connectez-vous à l'ISE.

Étape 2 Choisissez **Administration** > **Network Devices (Périphériques réseau)** > **Network Devices (Périphériques réseau)**.

Étape 3 Cliquez sur **Add** (ajouter).

Étape 4 Saisissez l'adresse IP de l'ASA.

Étape 5 Lorsque l'ISE est utilisé pour l'authentification des utilisateurs, saisissez un secret partagé dans la zone Authentication Settings (paramètres d'authentification).

Lorsque vous configurez le serveur AAA sur l'ASA, fournissez le secret partagé que vous créez ici sur l'ISE. Le serveur AAA sur l'ASA utilise ce secret partagé pour communiquer avec l'ISE.

Étape 6 Précisez un nom de périphérique, un ID de périphérique, un mot de passe et un intervalle de téléchargement pour l'ASA. Consultez la documentation d'ISE pour savoir comment effectuer ces tâches.

Créer un groupe de sécurité sur l'ISE

Lors de la configuration de l'ASA pour communiquer avec l'ISE, vous spécifiez un serveur AAA. Lors de la configuration du serveur AAA sur l'ASA, vous devez spécifier un groupe de serveurs. Le groupe de serveurs doit être configuré pour utiliser le protocole RADIUS. Pour créer un groupe de sécurité sur l'ISE, procédez comme suit :

Procédure

Étape 1 Connectez-vous à l'ISE.

Étape 2 Choisissez **Policy (Politique)** > **Policy Elements (Éléments de politique)** > **Results (Résultats)** > **Security Group Access (Accès au groupe de sécurité)** > **Security Group (Groupe de sécurité)**.

Étape 3 Ajoutez un groupe de sécurité pour l'ASA. (Les groupes de sécurité sont globaux et non spécifiques à l'ASA.)

L'ISE crée une entrée sous Security Groups (Groupes de sécurité) avec une balise.

Étape 4 Dans la zone Security Group Access (Accès au groupe de sécurité), configurez les informations d'authentification d'ID de périphérique et un mot de passe pour l'ASA.

Générer le fichier PAC

Pour générer le fichier PAC, procédez comme suit.



Remarque Le fichier PAC comprend une clé partagée qui permet à l'ASA et à l'ISE de sécuriser les transactions RADIUS qui se produisent entre eux. Pour cette raison, assurez-vous de le stocker en toute sécurité sur l'ASA.

Procédure

Étape 1 Connectez-vous à l'ISE.

Étape 2 Choisissez **Administration** > **Network Resources (Ressources réseau)** > **Network Devices (Périphériques réseau)**.

Étape 3 Dans la liste des périphériques, choisissez l'ASA.

Étape 4 Sous Security Group Access (SGA) (Accès aux groupes de sécurité), cliquez sur **Generate PAC** (Générer le PAC).

Étape 5 Pour chiffrer le fichier PAC, saisissez un mot de passe.

Le mot de passe (ou la clé de chiffrement) que vous saisissez pour chiffrer le fichier PAC est indépendant du mot de passe qui a été configuré sur l'ISE dans le cadre des informations d'authentification du périphérique.

L'ISE génère le fichier PAC. L'ASA peut importer le fichier PAC à partir de la mémoire flash ou d'un serveur distant via TFTP, FTP, HTTP, HTTPS ou SMB. (Le fichier PAC ne doit pas résider sur la mémoire flash de l'ASA avant que vous puissiez l'importer.)

Lignes directrices relatives à Cisco TrustSec

Cette section comprend les lignes directrices et les limites que vous devez consulter avant de configurer Cisco TrustSec.

Basculement

- Vous pouvez configurer des politiques basées sur des groupes de sécurité sur l'ASA dans les configurations actif/actif et actif/veille.

- Lorsque l'ASA fait partie d'une configuration de basculement, vous devez importer le fichier PAC sur le périphérique ASA principal. Vous devez également actualiser les données d'environnement sur le périphérique principal.
- L'ASA peut communiquer avec l'ISE configuré pour la haute disponibilité (HA).
- Vous pouvez configurer plusieurs serveurs ISE sur l'ASA et si le premier serveur est inaccessible, il continue vers le serveur suivant, etc. Toutefois, si la liste de serveurs est téléchargée dans le cadre des données d'environnement Cisco TrustSec, elle est ignorée.
- Si le fichier PAC téléchargé depuis l'ISE expire sur l'ASA et que celui-ci ne parvient pas à télécharger une table de groupes de sécurité mise à jour, l'ASA continue d'appliquer les politiques de sécurité selon la dernière table de groupes de sécurité téléchargée, jusqu'au téléchargement d'une table mise à jour.

Mise en grappes

- Lorsque l'ASA fait partie d'une configuration de mise en grappe, vous devez importer le fichier PAC dans l'unité de contrôle.
- Lorsque l'ASA fait partie d'une configuration de mise en grappe, vous devez actualiser les données d'environnement sur l'unité de contrôle.

IPv6

L'ASA prend en charge SXP pour IPv6 et les périphériques réseau compatibles avec IPv6. Le serveur AAA doit utiliser une adresse IPv4.

Imposition SGT de couche 2

- Pris en charge uniquement sur les interfaces physiques, les sous-interfaces et les interfaces EtherChannel.
- Non pris en charge sur les interfaces logiques ou les interfaces virtuelles, comme les BVI.
- Ne prend pas en charge le chiffrement de liaison à l'aide de la négociation SAP et de MACsec.
- Aucune prise en charge sur les liaisons de basculement.
- Aucune prise en charge sur les liaisons de commande de grappe.
- L'ASA ne reclasse pas les flux existants si la balise SGT est modifiée. Toutes les décisions de politique prises en fonction de la balise SGT précédente restent en vigueur pendant la durée du flux. Cependant, l'ASA peut refléter immédiatement les modifications de SGT sur les paquets de sortie, même si les paquets appartiennent à un flux dont la classification était basée sur une SGT précédente.
- Les ports de commutation Firepower 1010 et les interfaces VLAN ne prennent pas en charge l'application du balisage de groupe de sécurité de couche 2.

Directives supplémentaires

- L'ASA prend en charge la version 3 de SXP. L'ASA négocie les versions de SXP avec différents périphériques réseau compatibles avec SXP.
- L'ASA ne prend pas en charge la modification d'autorisation (CoA) pour les données d'environnement Cisco TrustSec (CTS).

- Vous pouvez configurer l'ASA pour actualiser la table de groupe de sécurité à l'expiration de la minuterie de réconciliation SXP et vous pouvez télécharger la table de groupe de sécurité à la demande. Lorsque la table de groupe de sécurité sur l'ASA est mise à jour à partir d'ISE, les modifications sont répercutées dans les politiques de sécurité appropriées.
- Cisco TrustSec prend en charge la fonctionnalité Smart Call Home en mode contexte unique et multi-contexte, mais pas dans le contexte du système.
- L'ASA ne peut être configurée que pour l'interopérabilité dans un seul domaine Cisco TrustSec.
- L'ASA ne prend pas en charge la configuration statique du mappage de nom SGT sur le périphérique.
- La NAT n'est pas prise en charge dans les messages SXP.
- SXP achemine le mappage IP-SGT vers les points d'application dans le réseau. Si un commutateur de couche d'accès appartient à un domaine NAT différent de celui du point d'application, le mappage IP-SGT qu'il charge n'est pas valide et une recherche de base de données de mappage IP-SGT sur le périphérique d'application ne donne pas de résultats valides. Par conséquent, l'ASA ne peut pas appliquer la politique de sécurité compatible avec les groupes de sécurité sur le périphérique d'application.
- Vous pouvez configurer un mot de passe par défaut que l'ASA utilise pour les connexions SXP, ou vous pouvez choisir de ne pas utiliser de mot de passe; cependant, les mots de passe spécifiques à la connexion ne sont pas pris en charge pour les homologues SXP. Le mot de passe SXP par défaut configuré doit être cohérent sur le réseau de déploiement. Si vous configurez un mot de passe de connexion spécifique, les connexions peuvent échouer et un message d'avertissement s'affiche. Si vous configurez la connexion avec le mot de passe par défaut, mais qu'il n'est pas configuré, le résultat est le même que lorsque vous avez configuré la connexion sans mot de passe.
- L'ASA peut être configuré comme un Speaker ou un Listener SXP, ou les deux. Cependant, des boucles de connexion SXP peuvent se former lorsqu'un périphérique a des connexions bidirectionnelles avec un homologue ou fait partie d'une chaîne de périphériques connectés de manière unidirectionnelle. (L'ASA peut apprendre le mappage IP-SGT pour les ressources de la couche d'accès dans le centre de données. L'ASA pourrait avoir besoin de propager ces balises vers les périphériques en aval.) Les boucles de connexion SXP peuvent entraîner un comportement inattendu du transport des messages SXP. Dans les cas où l'ASA est configuré pour être un Speaker et un Listener, une boucle de connexion SXP peut se produire, ce qui fait que les données SXP sont reçues par l'homologue qui les a transmises à l'origine.
- Lors de la modification de l'adresse IP locale de l'ASA, vous devez vous assurer que tous les homologues SXP ont mis à jour leur liste d'homologues. En outre, si les homologues SXP modifient leurs adresses IP, vous devez vous assurer que ces modifications sont répercutées sur l'ASA.
- Le provisionnement automatique du fichier PAC n'est pas pris en charge. L'administrateur de l'ASA doit demander le fichier PAC à l'interface d'administration ISE et l'importer dans l'ASA.
- Les fichiers PAC ont des dates d'expiration. Vous devez importer le fichier PAC mis à jour avant que le fichier PAC actuel n'expire; sinon, l'ASA ne peut pas récupérer les mises à jour des données d'environnement. Si le fichier PAC téléchargé depuis l'ISE expire sur l'ASA et que celui-ci ne parvient pas à télécharger une table de groupes de sécurité mise à jour, l'ASA continue d'appliquer les politiques de sécurité selon la dernière table de groupes de sécurité téléchargée, jusqu'au téléchargement d'une table mise à jour.
- Lorsqu'un groupe de sécurité change sur ISE (par exemple, il est renommé ou supprimé), l'ASA ne modifie pas l'état des politiques de sécurité ASA qui contiennent une balise SGT ou un nom de groupe de sécurité associé au groupe de sécurité modifié ; cependant, l'ASA génère un message syslog pour indiquer que ces politiques de sécurité ont été modifiées.

- Les types de multidiffusion ne sont pas pris en charge dans ISE 1.0.
- Une connexion SXP reste dans l'état d'initialisation entre deux homologues SXP interconnectés par l'ASA; comme le montre l'exemple suivant :

```
(SXP peer A) - - - - (ASA) - - - (SXP peer B)
```

Par conséquent, lors de la configuration de l'ASA pour l'intégration à Cisco TrustSec, vous devez activer les options TCP no-NAT, no-SEQ-RAND et MD5-AUTHENTICATION sur l'ASA pour configurer les connexions SXP. Créez une politique de contournement d'état TCP pour le trafic destiné au port SXP TCP 64999 entre les homologues SXP. Appliquez ensuite la politique sur les interfaces appropriées.

Par exemple, l'ensemble de commandes suivant montre comment configurer l'ASA pour une politique de contournement de l'état TCP :

```
access-list SXP-MD5-ACL extended permit tcp host peerA host peerB eq 64999
access-list SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
 tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
 match access-list SXP-MD5-ACL

policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
class SXP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options SXP-MD5-OPTION-ALLOW
  set connection advanced-options tcp-state-bypass
service-policy global_policy global
```

Configurer l'ASA pour s'intégrer à Cisco TrustSec

Pour configurer l'ASA afin qu'il s'intègre à Cisco TrustSec, effectuez les tâches suivantes.

Avant de commencer

Avant de configurer l'ASA pour qu'il s'intègre à Cisco TrustSec, vous devez effectuer les tâches suivantes dans ISE :

- Enregistrer l'ASA auprès de l'ISE, à la page 76
- Créer un groupe de sécurité sur l'ISE, à la page 76
- Générer le fichier PAC, à la page 77

Procédure

Étape 1 Configurer le serveur AAA pour l'intégration de Cisco TrustSec, à la page 81

Étape 2 Importer un fichier PAC, à la page 82

Étape 3 Configurer le protocole d'échange de sécurité, à la page 83

Cette tâche active et définit les valeurs par défaut pour SXP.

Étape 4 Ajouter un homologue de connexion SXP, à la page 85

Étape 5 Actualiser les données d'environnement, à la page 86

Effectuez cette opération selon les besoins.

Étape 6 Configurer la politique de sécurité, à la page 86

Étape 7 Configurer l'imposition du balisage de groupe de sécurité de couche 2, à la page 87

Configurer le serveur AAA pour l'intégration de Cisco TrustSec

Cette section décrit comment intégrer le serveur AAA pour Cisco TrustSec. Pour configurer le groupe de serveurs AAA afin de communiquer avec l'ISE sur l'ASA, procédez comme suit.

Avant de commencer

- Le groupe de serveurs référencé doit être configuré pour utiliser le protocole RADIUS. Si vous ajoutez un groupe de serveurs non RADIUS à l'ASA, la configuration échoue.
- Si ISE est également utilisé pour l'authentification des utilisateurs, obtenez le secret partagé qui a été saisi sur ISE lorsque vous avez enregistré l'ASA auprès de ISE. Communiquez avec votre administrateur ISE pour obtenir ces informations.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall** (Pare-feu) > **Identity By TrustSec (Identité par TrustSec**).

Étape 2 Cliquez sur **Manage** (Gérer) pour ajouter un groupe de serveurs à l'ASA.

La boîte de dialogue **Configure AAA Server Group** (Configurer un groupe de serveurs AAA) apparaît.

Étape 3 Saisissez le nom du groupe de sécurité qui a été créé sur ISE pour l'ASA.

Le nom du groupe de serveurs que vous spécifiez ici doit correspondre au nom du groupe de sécurité qui a été créé sur ISE pour l'ASA. Si ces deux noms de groupe ne correspondent pas, l'ASA ne peut pas communiquer avec l'ISE. Communiquez avec votre administrateur ISE pour obtenir ces informations.

Étape 4 Dans la liste déroulante **Protocol** (Protocole), choisissez le type de serveur **RADIUS**.

Pour remplir les champs restants dans la boîte de dialogue **AAA Server Group** (Groupe de serveurs AAA), consultez le chapitre RADIUS dans le guide de configuration des opérations générales.

Étape 5 Cliquez sur **OK**.

Étape 6 Sélectionnez le groupe de serveurs AAA que vous venez de créer et cliquez sur **Add** (Ajouter) dans la zone **Servers in the Selected Group** (Serveurs du groupe sélectionné) pour ajouter un serveur à un groupe.

La boîte de dialogue **Add AAA Server** (Ajouter un serveur AAA) apparaît.

Étape 7 Sélectionnez l'interface réseau où réside le serveur ISE.

Étape 8 Entrez l'adresse IP du serveur ISE.

Pour remplir les champs restants dans la boîte de dialogue AAA Server (Serveur AAA), consultez le chapitre RADIUS dans le guide de configuration des opérations générales.

Étape 9 Cliquez sur **OK**.

Étape 10 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.

Importer un fichier PAC

Cette section décrit comment importer un fichier PAC.

Avant de commencer

- L'ASA doit être configurée comme périphérique réseau Cisco TrustSec reconnu dans l'ISE avant que l'ASA puisse générer un fichier PAC.
- Obtenez le mot de passe utilisé pour chiffrer le fichier PAC lors de sa génération sur l'ISE. L'ASA nécessite ce mot de passe pour importer et déchiffrer le fichier PAC.
- Lors de l'importation, le fichier PAC réside dans la NVRAM. Lors du fonctionnement en mode haute disponibilité, si vous configurez correctement les liens de basculement et les liaisons avec état, l'importation du fichier PAC dans l'unité active entraînera la réplication sur l'unité secondaire. Comme le fichier importé réside dans la NVRAM, vous devez importer le fichier à nouveau chaque fois que le périphérique redémarre, par exemple, après une mise à niveau logicielle.
- Le périphérique utilise un seul fichier PAC. Si vous en importez plusieurs, chaque fichier PAC importé remplace le fichier importé précédemment.
- L'ASA nécessite d'accéder au fichier PAC généré par l'ISE. L'ASA peut importer le fichier PAC à partir de la mémoire flash ou d'un serveur distant via TFTP, FTP, HTTP, HTTPS ou SMB. (Le fichier PAC n'a pas besoin de résider sur la mémoire flash ASA avant que vous puissiez l'importer.)
- Le groupe de serveurs a été configuré pour l'ASA.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall** (Pare-feu) > **Identity By TrustSec (Identité par TrustSec**).

Étape 2 Cochez la case **Enable Security Exchange Protocol** (Activer Security Exchange Protocol) pour activer SXP.

Étape 3 Cliquez sur **Import PAC (Importer le PAC**) pour afficher la boîte de dialogue **Import PAC** (Importer le PAC).

Étape 4 Saisissez le chemin d'accès et le nom de fichier du fichier PAC en utilisant l'un des formats suivants :

- **disk0** : chemin d'accès et nom de fichier sur disk0
- **disk1** : chemin d'accès et nom de fichier sur disk1
- **flash** : chemin d'accès et nom de fichier en mémoire flash
- **ftp** : chemin d'accès et nom de fichier sur FTP
- **http** : chemin d'accès et nom de fichier sur HTTP
- **https** : chemin d'accès et nom de fichier sur HTTPS
- **smb** : chemin d'accès et nom de fichier sur SMB
- **tftp** : chemin d'accès et nom de fichier sur TFTP

Mode-multiple

- **http** : chemin d'accès et nom de fichier sur HTTP
- **https** : chemin d'accès et nom de fichier sur HTTPS
- **smb** : chemin d'accès et nom de fichier sur SMB
- **tftp** : chemin d'accès et nom de fichier sur TFTP

Étape 5 Saisissez le mot de passe utilisé pour chiffrer le fichier PAC. Le mot de passe est indépendant du mot de passe qui a été configuré sur l'ISE dans le cadre des informations d'authentification du périphérique.

Étape 6 Entrez le mot de passe de nouveau pour le confirmer.

Étape 7 Cliquez sur **Import (Importer)**.

Étape 8 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.

Lorsque vous importez le fichier PAC, le fichier est converti au format ASCII HEX et envoyé à l'ASA en mode non interactif.

Configurer le protocole d'échange de sécurité

Vous devez activer et configurer le protocole SXP (Security Exchange Protocol) pour utiliser Cisco Trustsec.

Avant de commencer

Au moins une interface doit être à l'état UP/UP. Si vous activez SXP avec toutes les interfaces en panne, l'ASA n'affiche pas de message indiquant que SXP ne fonctionne pas ou qu'il n'a pas pu être activé. Si vous vérifiez la configuration en saisissant la commande **show running-config**, la sortie affiche le message suivant :

```
"WARNING: SXP configuration in process, please wait for a few moments and try again."
```

Procédure

Étape 1 Choisissez **Configuration** > **Firewall** > **Identity By TrustSec (Configuration > Pare-feu > Identity By TrustSec**).

Étape 2 Cochez la case **Enable Security Exchange Protocol** (Activer Security Exchange Protocol) pour activer SXP. Par défaut, SXP est désactivé.

Étape 3 (Facultatif ; non recommandé.) Saisissez l'adresse IP locale par défaut pour les connexions SXP. L'adresse IP peut être une adresse IPv4 ou IPv6.

Remarque
L'ASA détermine l'adresse IP locale pour une connexion SXP comme adresse IP de l'interface sortante accessible par l'adresse IP homologue. Si l'adresse locale configurée est différente de l'adresse IP de l'interface sortante, l'ASA ne peut pas se connecter à l'homologue SXP et génère un message syslog. Nous vous recommandons de ne pas configurer d'adresse IP source par défaut pour les connexions SXP et de permettre à l'ASA d'effectuer une recherche de routage/ARP pour déterminer l'adresse IP source d'une connexion SXP.

Étape 4 (Facultatif) Saisissez le mot de passe par défaut pour l'authentification TCP MD5 avec les homologues SXP. Par défaut, les connexions SXP n'ont pas de mot de passe défini.

Configurez un mot de passe par défaut si et seulement si vous configurez les homologues de connexion SXP pour utiliser le mot de passe par défaut. Le mot de passe peut comporter jusqu'à 80 caractères. Il n'est pas chiffré.

Étape 5 (Facultatif) Modifiez l'intervalle de temps entre les tentatives de l'ASA pour configurer de nouvelles connexions SXP entre les homologues SXP dans le champ **Retry Timer** (Minuterie de nouvelle tentative).

L'ASA continue de faire des tentatives de connexion jusqu'à ce qu'une connexion réussisse, en attendant l'intervalle de nouvelle tentative avant de réessayer après un échec de tentative. Vous pouvez spécifier une période de nouvelle tentative comprise entre 0 et 64 000 secondes. La valeur par défaut est de 120 secondes. Si vous spécifiez 0 seconde, l'ASA ne tente pas de se connecter aux homologues SXP.

Nous vous recommandons de configurer la minuterie de nouvelle tentative à une valeur différente de celle des périphériques homologues SXP.

Étape 6 (Facultatif) Modifiez la valeur de la minuterie de rapprochement.

Une fois qu'un homologue a mis fin à une connexion SXP, une minuterie de maintien démarre. Si un homologue SXP se connecte pendant l'exécution de la minuterie de maintien, l'ASA démarre la minuterie de rapprochement ; puis, l'ASA met à jour la base de données de mappage SXP pour connaître les derniers mappages.

À l'expiration de la minuterie de rapprochement, l'ASA analyse la base de données de mappage SXP pour identifier les entrées de mappage périmées (qui ont été apprises lors d'une session de connexion précédente). L'ASA marque ces connexions comme obsolètes. À l'expiration de la minuterie de rapprochement, l'ASA supprime les entrées obsolètes de la base de données de mappage SXP.

Vous pouvez spécifier une période de rapprochement comprise entre 1 et 64 000 secondes. La valeur par défaut est de 120 secondes.

Étape 7 (Facultatif) Dans **Network Map** (Mappage réseau), configurez la profondeur de l'expansion du sous-réseau IPv4 lorsque l'ASA agit en tant que locuteur pour les homologues qui utilisent SXPv2 ou une version antérieure.

Si un homologue utilise SXPv2 ou une version antérieure, il ne peut pas comprendre les liaisons entre SGT et sous-réseaux. L'ASA peut étendre les liaisons de sous-réseau IPv4 aux liaisons d'hôtes individuels (les liaisons IPv6 ne sont pas étendues). Cette commande spécifie le nombre maximal de liaisons d'hôte qui peuvent être générées à partir d'une liaison de sous-réseau.

Vous pouvez spécifier que le nombre maximal est compris entre 0 et 65 535. La valeur par défaut est 0, ce qui signifie que les liaisons de sous-réseau ne sont pas développées en liaisons d'hôte.

Étape 8 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.

Ajouter un homologue de connexion SXP

Pour ajouter un homologue de connexion SXP, procédez comme suit :

Procédure

Étape 1 Choisissez **ConfigurationFirewall** (Pare-feu) > **Identity By TrustSec (Identité par TrustSec** >).

Étape 2 Cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add Connection** (Ajouter une connexion).

Étape 3 Saisissez l'adresse IPv4 ou IPv6 de l'homologue SXP. L'adresse IP de l'homologue doit être accessible à partir de l'interface sortante de l'ASA.

Étape 4 Indiquez s'il faut utiliser ou non la clé d'authentification pour la connexion SXP en choisissant l'une des valeurs suivantes :

- **Default** (Par défaut) : utilisez le mot de passe par défaut configuré pour les connexions SXP.
- **None** (Aucun) : n'utilisez pas de mot de passe pour la connexion SXP.

Étape 5 (Facultatif) Précisez le mode de connexion SXP en choisissant l'une des valeurs suivantes :

- **Local** : utilisez le périphérique SXP local.
- **Peer (Homologue)** : utilisez le périphérique SXP homologue.

Étape 6 Précisez si l'ASA fonctionne comme Speaker ou Listener pour la connexion SXP :

- **Speaker** : l'ASA peut transférer le mappage IP-SGT vers des périphériques en amont.
- **Listener** : l'ASA peut recevoir le mappage IP-SGT de la part de périphériques en aval.

Étape 7 (Facultatif) Cliquez sur **Advanced** (Avancé) et saisissez l'adresse IPv4 ou IPv6 locale de la connexion SXP.

L'ASA utilise toujours une recherche de routage pour déterminer l'interface correcte. Si vous spécifiez une adresse, elle doit correspondre à l'adresse de l'interface trouvée par la recherche de routage sur l'interface sortante. Nous vous recommandons de ne pas configurer d'adresse IP source pour une connexion SXP et de permettre à l'ASA d'effectuer une recherche de routage/ARP pour déterminer l'adresse IP source de la connexion SXP.

Étape 8 Cliquez sur **OK**.

Étape 9 Cliquez sur **Apply** (Appliquer) pour enregistrer vos paramètres dans la configuration d'exécution.

Actualiser les données d'environnement

L'ASA télécharge les données d'environnement à partir de l'ISE, qui comprend la table de noms de balise de groupe de sécurité (SGT). L'ASA actualise automatiquement ses données d'environnement obtenues auprès de l'ISE lorsque vous effectuez les tâches suivantes sur l'ASA :

- Configurez un serveur AAA pour communiquer avec l'ISE.
- Importez un fichier PAC à partir de l'ISE.
- Déterminez le groupe de serveurs AAA que l'ASA utilisera pour récupérer les données d'environnement Cisco TrustSec.

Normalement, vous n'avez pas besoin d'actualiser manuellement les données d'environnement à partir de l'ISE; cependant, les groupes de sécurité peuvent changer sur l'ISE. Ces modifications ne sont pas répercutées sur l'ASA tant que vous n'avez pas actualisé les données dans la table des groupes de sécurité de l'ASA. Actualisez donc les données sur l'ASA pour vous assurer que toutes les modifications de groupe de sécurité apportées sur l'ISE sont répercutées sur l'ASA.

Remarque Nous vous recommandons de planifier les modifications de configuration des politiques sur l'ISE et l'actualisation manuelle des données sur l'ASA pendant une fenêtre de maintenance. Le traitement des modifications de configuration des politiques de cette manière maximise les possibilités de résolution des noms de groupes de sécurité et l'activation immédiate des politiques de sécurité sur l'ASA.

Pour actualiser les données d'environnement, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Firewall** (Pare-feu) > **Identity By TrustSec (Identité par TrustSec**).

Étape 2 Cliquez sur **Refresh Environment Data** (Actualiser les données d'environnement) dans la zone **Server Group Setup** (Configuration du groupe de serveurs).

L'ASA actualise les données d'environnement Cisco TrustSec à partir de l'ISE et réinitialise la minuterie de réconciliation à la valeur par défaut configurée.

Configurer la politique de sécurité

Vous pouvez intégrer la politique Cisco TrustSec dans de nombreuses fonctionnalités ASA. Toute fonctionnalité qui utilise des listes de contrôle d'accès étendues (sauf si elle est répertoriée dans ce chapitre comme non prise en charge) peut tirer parti de Cisco TrustSec. Vous pouvez ajouter des arguments de groupe de sécurité aux listes de contrôle d'accès étendues, ainsi qu'aux paramètres basés sur le réseau traditionnel.

- Pour configurer les règles d'accès, consultez Configurer les règles d'accès, à la page 19. Pour d'autres listes de contrôle d'accès étendues, consultez Configurer les ACL étendues, à la page 56.
- Pour configurer les groupes d'objets de groupe de sécurité qui peuvent être utilisés dans l'ACL, consultez Configurer les groupes d'objets de groupe de sécurité, à la page 43.

Par exemple, une règle d'accès autorise ou refuse le trafic sur une interface en utilisant les informations réseau. Grâce à Cisco TrustSec, vous pouvez contrôler l'accès en fonction du groupe de sécurité. Par exemple, vous pouvez créer une règle d'accès pour sample_securitygroup1 10.0.0.0 255.0.0.0, ce qui signifie que le groupe de sécurité peut avoir n'importe quelle adresse IP sur le sous-réseau 10.0.0.0/8.

Vous pouvez configurer des politiques de sécurité en fonction de combinaisons de noms de groupes de sécurité (serveurs, utilisateurs, périphériques non gérés, etc.), d'attributs basés sur l'utilisateur et d'objets basés sur l'adresse IP traditionnelle (adresse IP, objet Active Directory et nom de domaine complet FQDN). L'appartenance au groupe de sécurité peut s'étendre au-delà des rôles pour inclure les attributs de périphérique et d'emplacement et est indépendante de l'appartenance au groupe d'utilisateurs.

Configurer l'imposition du balisage de groupe de sécurité de couche 2

Cisco TrustSec identifie et authentifie chaque utilisateur et ressource du réseau et attribue un numéro de 16 bits appelé balise de groupe de sécurité (SGT). Cet identifiant est à son tour propagé entre les sauts de réseau, ce qui permet à tous les périphériques intermédiaires tels que les ASA, les commutateurs et les routeurs d'appliquer des politiques en fonction de cette balise d'identité.

SGT plus Ethernet Tagging, également appelé Imposition SGT de couche 2, permet à l'ASA d'envoyer et de recevoir des balises de groupe de sécurité sur les interfaces Ethernet à l'aide du cadrage Ethernet propriétaire de Cisco (EtherType 0x8909), qui permet l'insertion de balises de groupe de sécurité source dans des trames Ethernet en texte brut. L'ASA insère des balises de groupe de sécurité sur le paquet sortant et traite les balises de groupe de sécurité sur le paquet entrant, en fonction d'une configuration manuelle par interface. Cette fonctionnalité permet la propagation en ligne, saut par saut, de l'identité des terminaux sur les périphériques réseau et fournit une imposition SGT de couche 2 transparente entre chaque saut.

La figure suivante montre un exemple typique d'imposition SGT de couche 2.

Illustration 5 : Imposition SGT de couche 2



Scénarios d'utilisation

Le tableau suivant décrit le comportement attendu pour le trafic d'entrée lors de la configuration de cette fonctionnalité.

Tableau 3 : Trafic d'entrée

Configuration de l'interface	Paquet étiqueté reçu	Paquet non étiqueté reçu
Aucune commande n'est envoyée.	Paquet abandonné.	La valeur SGT provient du gestionnaire IP-SGT.
La commande **cts manual** est émise.	La valeur SGT provient du gestionnaire IP-SGT.	La valeur SGT provient du gestionnaire IP-SGT.
La commande **cts manual** et la commande **policy static sgt** *sgt_number* sont toutes deux émises.	La valeur SGT provient de la commande **policy static sgt** *sgt_number* .	La valeur SGT provient de la commande **policy static sgt** *sgt_number* .
La commande **cts manual** et la commande **policy static sgt** *sgt_number* **trusted** sont toutes deux émises.	La valeur SGT provient de la SGT en ligne dans le paquet.	La valeur SGT provient de la commande **policy static sgt** *sgt_number* .

Remarque S'il n'y a pas de mappage IP-SGT correspondant à partir du gestionnaire IP-SGT, une valeur SGT réservée de « 0x0 » pour « Inconnu » est utilisée.

Le tableau suivant décrit le comportement attendu pour le trafic de sortie lors de la configuration de cette fonctionnalité.

Tableau 4 : Trafic de sortie

Configuration de l'interface	Paquet étiqueté ou non étiqueté envoyé
Aucune commande n'est envoyée.	Non balisé
La commande **cts manual** est émise.	Balisé
La commande **cts manual** et la commande **propagate sgt** sont toutes deux émises.	Balisé
La commande **cts manual** et la commande **no propagate sgt** sont toutes deux émises.	Non balisé

Le tableau suivant décrit le comportement attendu du trafic vers le boîtier et à partir du boîtier lors de la configuration de cette fonctionnalité.

Tableau 5 : Trafic entrant et sortant

Configuration de l'interface	Paquet étiqueté ou non étiqueté reçu
Aucune commande n'est émise sur l'interface d'entrée pour le trafic vers le boîtier.	Paquet abandonné.
La commande **cts manual** est émise sur l'interface d'entrée pour le trafic vers le boîtier.	Le paquet est accepté, mais il n'y a pas d'application de politique ni de propagation de SGT.
La commande **cts manual** n'est pas émise ou la commande **cts manual** et **no propagate sgt** sont toutes deux émises sur l'interface de sortie pour le trafic à partir du boîtier.	Un paquet non étiqueté est envoyé, mais il n'y a pas d'application de la politique. Le numéro SGT provient du gestionnaire IP-SGT.
La commande **cts manual** est émise ou la commande **cts manual** et la commande **propagate sgt** sont toutes deux émises sur l'interface de sortie pour le trafic à partir du boîtier.	Le paquet étiqueté est envoyé. Le numéro SGT provient du gestionnaire IP-SGT.



Remarque S'il n'y a pas de mappage IP-SGT correspondant à partir du gestionnaire IP-SGT, une valeur SGT réservée de « 0x0 » pour « Inconnu » est utilisée.

Configurer une balise de groupe de sécurité sur une interface

Pour configurer une balise de groupe de sécurité sur une interface, procédez comme suit :

Procédure

Étape 1 Choisissez une des options suivantes :

- **Configuration** > **Device Setup (Configuration du périphérique)** > **Interfaces (Interfaces) > Add Interface (Ajouter une interface**) > **Advanced (Avancé)**
- **Configuration > Device Setup (Configuration du périphérique)** > **Interfaces > Add Redundant Interface (Ajouter une interface redondante)** > **Advanced (Avancé)**
- **Configuration > Device Setup (Configuration du périphérique)** > **Interfaces (Interfaces) > Add Ethernet Interface (Ajouter une interface Ethernet**) > **Advanced (Avancé)**

Étape 2 Cochez la case **Enable secure group tagging for Cisco TrustSec** (Activer le balisage de groupe sécurisé pour Cisco TrustSec).

Étape 3 Cochez la case **Tag egress packets with security group tags** (Marquer les paquets de sortie avec des balises de groupe de sécurité).

Étape 4 Cochez la case **Add a static secure group tag to all ingress packets** (Ajouter une balise de groupe sécurisé statique à tous les paquets d'entrée).

Étape 5 Saisissez un numéro de balise de groupe sécurisé. Les valeurs valides sont comprises entre 2 et 65 519.

Étape 6 Cochez la case **This is a trusted interface. Do not override existing security group tags** (Il s'agit d'une interface de confiance. Ne pas remplacer les balises de groupe de sécurité existantes.)

Étape 7 Cliquez sur**OK** pour sauvegarder vos paramètres.

Configurer manuellement les liaisons IP-SGT

Pour configurer manuellement les liaisons IP-SGT, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Firewall Identity by TrustSec (Identité par TrustSec du pare-feu)**.

Étape 2 Cliquez sur **Add** (Ajouter) dans la zone **SGT Map Setup** (Configuration du mappage SGT), ou sélectionnez un mappage SGT et cliquez sur **Edit** (Modifier).

Étape 3 Dans la boîte de dialogue SGT Map (Mappage SGT), saisissez l'adresse IP et la valeur SGT dans les champs appropriés.

Les numéros SGT peuvent être compris entre 2 et 65 519.

Pour mapper un réseau à une balise SGT, cochez la case **Prefix** (Préfixe) et saisissez le préfixe du sous-réseau ou IPv6. Par exemple, saisissez 24 pour mapper 10.100.10.0/24.

Étape 4 Cliquez sur **OK**, puis cliquez sur **Apply** (Appliquer) pour enregistrer vos paramètres.

Prise en charge de Cisco TrustSec pour les VPN Secure Client (services client sécurisés)

L'ASA prend en charge le balisage de groupe de sécurité des sessions VPN. Vous pouvez attribuer une balise de groupe de sécurité (SGT) à une session VPN en utilisant un serveur AAA externe, ou en configurant une balise de groupe de sécurité pour un utilisateur local ou pour une politique de groupe VPN. Cette balise peut ensuite être propagée par l'intermédiaire du système Cisco TrustSec sur Ethernet de couche 2. Les balises de groupe de sécurité sont utiles sur les politiques de groupe et pour les utilisateurs locaux lorsque le serveur AAA ne peut pas fournir de SGT.

Voici le processus typique d'attribution d'une balise SGT à un utilisateur de VPN :

1. Un utilisateur se connecte à un VPN d'accès à distance qui utilise un groupe de serveurs AAA contenant des serveurs ISE.
2. L'ASA demande des informations AAA à ISE, qui peuvent inclure une balise SGT. L'ASA attribue également une adresse IP au trafic tunnelisé de l'utilisateur.
3. L'ASA utilise les informations AAA pour authentifier l'utilisateur et crée un tunnel.
4. L'ASA utilise la balise SGT à partir des informations AAA et l'adresse IP attribuée pour ajouter une balise SGT dans l'en-tête de la couche 2.
5. Les paquets qui comprennent la balise SGT sont transmis au périphérique homologue suivant dans le réseau Cisco TrustSec.

S'il n'y a pas de SGT dans les attributs du serveur AAA pour l'affecter à un utilisateur VPN, l'ASA utilise la balise dans la politique de groupe. S'il n'y a pas de balise SGT dans la politique de groupe, la balise 0x0 est attribuée.

Remarque Vous pouvez également utiliser ISE pour appliquer les politiques à l'aide de la modification d'autorisation (CoA) ISE. Pour en savoir plus sur la configuration de l'application des politiques, consultez le guide de configuration VPN.

Ajouter une balise SGT aux politiques de groupe du VPN d'accès à distance et aux utilisateurs locaux

Pour configurer un attribut SGT sur les politiques de groupe VPN d'accès à distance ou sur la politique VPN pour un utilisateur défini dans la base de données d'utilisateurs LOCAL, procédez comme suit.

Il n'y a pas de balise SGT par défaut pour les politiques de groupe ou les utilisateurs locaux.

Procédure

Étape 1 Pour configurer une SGT sur une politique de groupe VPN d'accès à distance :

a) Choisissez **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** > **(Configuration VPN d'accès à distance Accès réseau (client) Politiques de groupe)**.
b) Cliquez sur l'onglet **General** (Général), puis sur **More Options** (Plus d'options).
c) Saisissez une valeur comprise entre 2 et 65 519 dans le champ **Security Group Tag (SGT)** (Balise de groupe de sécurité (SGT)).

   Vous pouvez également sélectionner None (Aucun) pour ne définir aucune balise SGT.

d) Cliquez sur **OK**.

Étape 2 Pour configurer une SGT pour un utilisateur dans la base de données LOCAL :

a) Choisissez **Configuration** > **Remote Access VPN** > **AAA/Local Users** > **Local Users** > **(Configuration VPN d'accès à distance AAA/Utilisateurs locaux Utilisateurs locaux).**
b) Sélectionnez un utilisateur, puis cliquez sur **Edit** (Modifier).
c) Cliquez sur **VPN Policy** (Politique VPN).
d) Saisissez une valeur comprise entre 2 et 65 519 dans le champ **Security Group Tag (SGT)** (Balise de groupe de sécurité (SGT)).

   Vous pouvez également sélectionner None (Aucun) pour ne définir aucune balise SGT.

e) Cliquez sur **OK**.

Surveillance de Cisco TrustSec

Consultez les écrans suivants pour superviser Cisco TrustSec :

- **Monitoring (Surveillance)** > **Properties (Propriétés)** > **Identity By TrustSec (Identité par TrustSec)** > **SXP Connections (Connexions SXP)**

  Affiche les valeurs par défaut configurées pour l'infrastructure Cisco TrustSec et les commandes SXP.

- **Monitoring (Surveillance)** > **Properties (Propriétés)** > **Connections (Connexions)**

  Filtre les entrées de mappage de l'adresse IP et de la table de groupe de sécurité afin que vous puissiez afficher les données par valeur de table de groupe de sécurité, nom de groupe de sécurité ou adresse IP.

- **Monitoring (Surveillance)** > **Properties (Propriétés)** > **Identity By TrustSec (Identité par TrustSec)** > **Environment Data (Données d'environnement)**

  Affiche les informations sur l'environnement Cisco TrustSec contenues dans la table des groupes de sécurité sur l'ASA.

- **Monitoring (Surveillance)** > **Properties (Propriétés)** > **Identity By TrustSec (Identité par TrustSec)** > **IP Mapping (Mappage IP)**

  Filtre les entrées de mappage de l'adresse IP et de la table de groupe de sécurité afin que vous puissiez afficher les données par valeur de table de groupe de sécurité, nom de groupe de sécurité ou adresse IP. Cliquez sur **Where Used** (Emplacement d'utilisation) pour afficher l'endroit où l'objet de groupe de sécurité sélectionné est utilisé dans une ACL ou imbriqué dans un autre objet de groupe de sécurité.

- **Monitoring (Surveillance)** > **Properties (Propriétés)** > **Identity By TrustSec (Identité par TrustSec)** > **PAC**

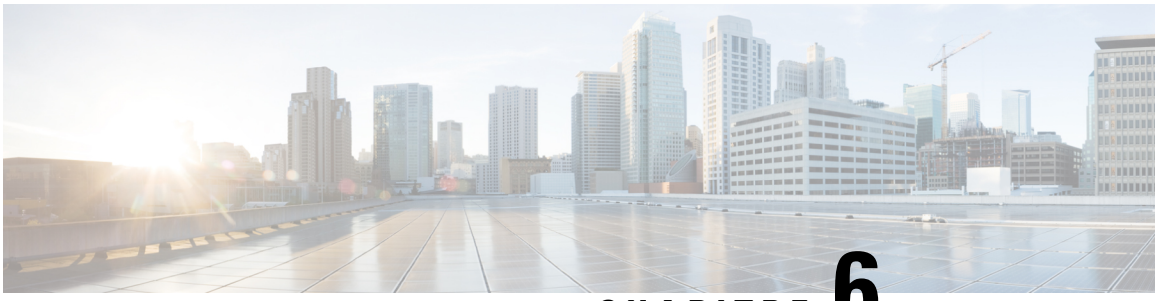
Affiche les informations sur le fichier PAC importé dans l'ASA à partir de l'ISE et comprend un message d'avertissement lorsque le fichier PAC a expiré ou se trouve dans les 30 jours de son expiration.

Historique de Cisco TrustSec

Tableau 6 : Historique de Cisco TrustSec

Nom de la caractéristique	Versions de plateforme	Description
TrustSec de Cisco	9.0(1)	Cisco TrustSec fournit un contrôle d'accès qui s'appuie sur une infrastructure existante de prise en compte de l'identité pour assurer la confidentialité des données entre les périphériques réseau et intégrer les services d'accès de sécurité sur une seule plateforme. Dans la fonctionnalité Cisco TrustSec, les appareils d'application utilisent une combinaison d'attributs d'utilisateur et d'attributs de terminal pour prendre des décisions de contrôle d'accès basées sur les rôles et l'identité. Dans cette version, l'ASA s'intègre à Cisco TrustSec pour fournir une application des politiques basées sur des groupes de sécurité. Les politiques d'accès au sein du domaine Cisco TrustSec sont indépendantes de la topologie, en fonction des rôles des périphériques source et de destination plutôt que des adresses IP du réseau. L'ASA peut utiliser Cisco TrustSec pour d'autres types de politiques basées sur des groupes de sécurité, telles que l'inspection des applications; par exemple, vous pouvez configurer une carte de trafic qui comprend une politique d'accès basée sur un groupe de sécurité. Nous avons introduit ou modifié les écrans suivants : Configuration > Firewall (Pare-feu) > Identity By TrustSec (Identité par TrustSec) Configuration > Firewall (Pare-feu) > Objects (Objets) > Security Groups Object Groups (Groupes d'objets de groupes de sécurité) Configuration > Firewall (Pare-feu) > Access Rules (Règles d'accès) > Add Access Rules (Ajouter des règles d'accès) Monitoring (Surveillance) > Properties (Propriétés) > Identity By Tag (Identité par balise).

Nom de la caractéristique	Versions de plateforme	Description
Imposition de balises de groupe de sécurité de couche 2	9.3(1)	Vous pouvez désormais utiliser le balisage de groupe de sécurité combiné au balisage Ethernet pour appliquer les politiques. SGT plus Ethernet Tagging, également appelé Layer 2 SGT Imposition, permet à l'ASA d'envoyer et de recevoir des balises de groupe de sécurité sur les interfaces Ethernet à l'aide du cadrage Ethernet propriétaire de Cisco (EtherType 0x8909), qui permet l'insertion de balises de groupe de sécurité source dans des trames Ethernet en texte clair. Nous avons modifié les écrans suivants : Configuration > Device Setup (Configuration du périphérique) > Interfaces > Add Interface (Ajouter une interface) > Advanced (Avancé) Configuration > Device Setup (Configuration du périphérique) > Interfaces > Add Redundant Interface (Ajouter une interface redondante) > Advanced (Avancé) Configuration > Device Setup (Configuration du périphérique) > Add Ethernet Interface (Ajouter une interface Ethernet) > Advanced (Avancé).
Prise en charge par Cisco Trustsec du protocole SXP (Security Exchange Protocol) version 3.	9.6(1)	Cisco Trustsec sur l'ASA implémente désormais SXPv3, qui permet des liaisons SGT-sous-réseau, plus efficaces que les liaisons hôte. Nous avons modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Identity By TrustSec (Identité par TrustSec)** et les boîtes de dialogue **SGT Map Setup (Configuration de la carte SGT)**.
Minuterie de maintien de suppression configurable de la connexion Trustsec SXP	9.8(3)	La minuterie de maintien de la connexion SXP par défaut est de 120 secondes. Vous pouvez maintenant configurer cette minuterie, entre 120 et 64 000 secondes. Commandes nouvelles/modifiées : **cts sxp delete-hold-down period**, **show cts sxp connection brief**, **show cts sxp connections** ASDM n'est pas pris en charge.



CHAPITRE 6

Cisco Umbrella

Vous pouvez configurer le périphérique pour rediriger les requêtes DNS vers Cisco Umbrella, afin que votre politique FQDN définie dans Cisco Umbrella puisse être appliquée aux connexions des utilisateurs. Les rubriques suivantes expliquent comment configurer Cisco Umbrella Connector pour intégrer l'appareil à Cisco Umbrella.

- À propos de Cisco Umbrella Connector, à la page 95
- Exigences de licence pour Cisco Umbrella Connector, à la page 96
- Lignes directrices et limites relatives à Cisco Umbrella, à la page 97
- Configurer Cisco Umbrella Connector, à la page 99
- Surveillance du connecteur Cisco Umbrella , à la page 104
- Historique du connecteur Cisco Umbrella, à la page 107

À propos de Cisco Umbrella Connector

Si vous utilisez Cisco Umbrella, vous pouvez configurer Cisco Umbrella Connector pour rediriger les requêtes DNS vers Cisco Umbrella. Cela permet à Cisco Umbrella d'identifier les demandes adressées à des noms de domaine non autorisés ou douteux et d'appliquer votre politique de sécurité basée sur DNS.

Le connecteur Cisco Umbrella fait partie de l'inspection DNS du système. Si votre liste de politiques d'inspection DNS existante décide de bloquer ou d'abandonner une demande en fonction de vos paramètres d'inspection DNS, la demande n'est pas transmise à Cisco Umbrella. Ainsi, vous avez deux lignes de protection : votre politique d'inspection DNS locale et votre politique basée sur le nuage Cisco Umbrella.

Lors de la redirection des demandes de recherche DNS vers Cisco Umbrella, le connecteur Cisco Umbrella ajoute un enregistrement EDNS (Extension mécanismes for DNS). Un enregistrement EDNS comprend les renseignements sur l'identifiant du périphérique , l'ID de l'organisation et l'adresse IP du client. Votre politique en nuage peut utiliser ces critères pour contrôler l'accès en plus de la réputation du nom de domaine complet. Vous pouvez également choisir de chiffrer la requête DNS à l'aide de DNSCrypt pour assurer la confidentialité des noms d'utilisateurs et des adresses IP internes.

Politique de sécurité entreprise Cisco Umbrella

Dans votre politique Cisco Umbrella Enterprise Security basée sur le nuage, vous pouvez contrôler l'accès en fonction de la réputation du nom de domaine complet (FQDN) dans la demande de recherche DNS. Votre politique de sécurité d'entreprise peut appliquer l'une des actions suivantes :

- Autoriser : si vous n'avez aucune règle de blocage pour un nom de domaine complet et que Cisco Umbrella détermine qu'il appartient à un site non malveillant, l'adresse IP réelle du site est renvoyée. Ce comportement est tout à fait normal.
- Proxy : si vous n'avez aucune règle de blocage pour un nom de domaine complet et que Cisco Umbrella détermine qu'il appartient à un site suspect, la réponse DNS renvoie l'adresse IP du serveur proxy intelligent Cisco Umbrella. Le serveur proxy peut ensuite inspecter la connexion HTTP et appliquer le filtrage d'URL. Vous devez vous assurer que le proxy intelligent est activé à partir du tableau de bord Cisco Umbrella (**Security Setting (Paramètre de sécurité)** > **Enable Intelligent Proxy (Activer le proxy intelligent)**).
- Blocage : si vous bloquez explicitement un nom de domaine complet ou si Cisco Umbrella détermine qu'il appartient à un site malveillant, la réponse DNS renvoie l'adresse IP de la page de destination du nuage Cisco Umbrella pour les connexions bloquées.

Enregistrement de Cisco Umbrella

Lorsque vous configurez Cisco Umbrella Connector sur un périphérique, il s'enregistre auprès de Cisco Umbrella dans le nuage. Le processus d'enregistrement attribue un ID de périphérique unique, qui identifie l'un des éléments suivants :

- Un périphérique autonome en mode contexte unique.
- Une paire à haute disponibilité en mode contexte unique.
- Une grappe en mode contexte unique.
- Un contexte de sécurité dans un périphérique autonome multi-contexte.
- Un contexte de sécurité d'une paire à haute disponibilité
- Un contexte de sécurité d'une grappe.

Une fois enregistrés, les détails du périphérique s'affichent dans le tableau de bord de Cisco Umbrella. Vous pouvez ensuite modifier la politique associée à un périphérique. Lors de l'enregistrement, la politique que vous spécifiez dans la configuration est utilisée ou la politique par défaut est attribuée. Vous pouvez affecter la même politique Cisco Umbrella à plusieurs périphériques. Si vous spécifiez la politique, l'ID de périphérique que vous recevez est différent de ce que vous obtiendriez si vous ne spécifiez pas de politique.

Exigences de licence pour Cisco Umbrella Connector

Pour utiliser le Cisco Umbrella Connector, vous devez avoir une licence 3DES. Si vous utilisez Smart Licensing, votre compte doit être activé pour la fonctionnalité soumise au contrôle des exportations.

Le portail Cisco Umbrella comporte des exigences de licence distinctes.

Lignes directrices et limites relatives à Cisco Umbrella

Mode contextuel

- En mode contexte multiple, vous configurez Cisco Umbrella Connector dans chaque contexte. Chaque contexte possède un ID de périphérique distinct et est représenté comme un périphérique distinct dans le tableau de bord de Cisco Umbrella Connector. Le nom du périphérique est le nom d'hôte configuré dans le contexte, plus le modèle matériel, plus le nom du contexte. Par exemple, CiscoASA-ASA5515-Context1.

Basculement

- L'unité active dans la paire à haute disponibilité enregistre la paire en tant qu'unité unique auprès de Cisco Umbrella. Les deux homologues utilisent le même ID de périphérique, qui est composé de leurs numéros de série : *numéro de série principal_numéro de série secondaire*. Pour le mode de contexte multiple, chaque paire de contextes de sécurité est considérée comme une unité unique. Vous devez configurer la haute disponibilité, et les unités doivent avoir formé avec succès un groupe de haute disponibilité (même si le périphérique de secours est actuellement en état d'échec) avant d'activer Cisco Umbrella, sinon l'enregistrement échouera.

Grappe

- L'unité de contrôle de grappe enregistre la grappe en tant qu'unité unique auprès de Cisco Umbrella. Tous les homologues utilisent le même ID de périphérique. Pour le mode de contexte multiple, un contexte de sécurité dans la grappe est considéré comme une unité unique pour tous les homologues.

Directives supplémentaires

- La redirection vers Cisco Umbrella est effectuée pour les demandes DNS dans le trafic de transit uniquement. Les requêtes DNS que le système lui-même lance ne sont jamais redirigées vers Cisco Umbrella. Par exemple, les règles de contrôle d'accès basées sur le nom de domaine complet ne sont jamais résolues en fonction de la politique Cisco Umbrella, ni les noms de domaine complets utilisés dans d'autres commandes ou paramètres de configuration.
- Cisco Umbrella Connector fonctionne sur toute demande DNS dans le trafic de transit. Cependant, les actions de blocage et de serveur proxy ne sont effectives que si la réponse DNS est ensuite utilisée pour les connexions HTTP/HTTPS, car l'adresse IP renvoyée concerne un site Web. Toutes les adresses bloquées ou relayées par proxy pour les connexions non HTTP/HTTPS échoueront ou se termineront de manière erronée. Par exemple, envoyer une requête ping à un nom de domaine complet bloqué entraînerait l'envoi d'une requête ping au serveur qui héberge la page de blocage Cisco Umbrella.



Remarque Cisco Umbrella tente d'identifier intelligemment les noms de domaine complets qui pourraient être non HTTP/HTTPS et ne renvoie pas l'adresse IP au proxy intelligent pour ces noms de domaine complets dans le cas des noms de domaine relayés par proxy.

- Le système envoie le trafic DNS/UDP uniquement à Cisco Umbrella. Si vous activez l'inspection DNS/TCP, le système n'envoie aucune demande DNS/TCP à Cisco Umbrella. Cependant, les requêtes DNS/TCP n'incrémentent pas le compteur de contournement Cisco Umbrella.
- Si vous activez DNScrypt pour l'inspection Cisco Umbrella, le système utilise UDP/443 pour la session chiffrée. Vous devez inclure UDP/443 avec UDP/53 dans la carte de trafic qui applique l'inspection DNS pour Cisco Umbrella pour que DNScrypt fonctionne correctement. UDP/443 et UDP/53 sont inclus dans la carte de trafic d'inspection par défaut pour DNS, mais si vous créez une carte personnalisée, veillez à définir une liste de contrôle d'accès qui inclut les deux ports pour la carte de correspondance.
- DNScrypt utilise IPv4 uniquement pour l'établissement de liaison de mise à jour de certificat. Cependant, DNScrypt chiffre le trafic IPv4 et IPv6.
- Il doit y avoir une route IPv4 vers Internet qui puisse atteindre api.umbrella.com et api.opendns.com (l'enregistrement utilise IPv4 uniquement). Vous devez également avoir des routes vers les résolveurs DNS suivants, et vos règles d'accès doivent autoriser le trafic DNS vers ces hôtes. Ces routes peuvent passer par les interfaces de données ou l'interface de gestion; toute route valide fonctionnera à la fois pour l'enregistrement et la résolution DNS. Les serveurs par défaut utilisés par le système sont indiqués; vous pouvez utiliser les autres serveurs en configurant le résolveur dans les paramètres globaux de Cisco Umbrella.
  - 208.67.220.220 (par défaut du système pour IPv4)
  - 208.67.222.222
  - 2620:119:53::53 (par défaut du système pour IPv6)
  - 2620:119:35::35
- Le système ne prend pas en charge le service Cisco Umbrella FamilyShield. Si vous configurez les résolveurs FamilyShield, vous pourriez obtenir des résultats inattendus.
- Lors de l'évaluation du mode ouvert en cas d'échec, le système détermine si le résolveur Cisco Umbrella est en panne ou si un périphérique intermédiaire abandonne la demande ou la réponse DNS en fonction du temps écoulé depuis l'envoi de la demande en attente de la réponse. D'autres facteurs, tels que l'absence de voie de routage vers le résolveur Cisco Umbrella, ne sont pas pris en compte.
- Pour annuler l'enregistrement d'un appareil, supprimez d'abord la configuration Cisco Umbrella, puis supprimez l'appareil du tableau de bord Cisco Umbrella.
- Toute demande Web qui utilise des adresses IP au lieu de FQDN contournera Cisco Umbrella. En outre, si un client itinérant obtient une résolution DNS à partir d'une connexion WAN différente de celle qui passe par un périphérique compatible avec Cisco Umbrella, les connexions qui utilisent ces résolutions contournent Cisco Umbrella.
- Si un utilisateur dispose d'un serveur proxy HTTP, le serveur proxy peut effectuer une résolution DNS, et les résolutions ne passeront pas par Cisco Umbrella.
- Les NAT DNS46 et DNS64 ne sont pas prises en charge. Vous ne pouvez pas traduire les demandes DNS entre l'adressage IPv4 et IPv6.
- L'enregistrement EDNS comprendra les adresses d'hôte IPv4 et IPv6.
- Si le client utilise DNS sur HTTPS, le service de sécurité en nuage n'inspectera pas le trafic DNS et HTTP/HTTPS.

Configurer Cisco Umbrella Connector

Vous pouvez configurer l'appareil pour interagir avec Cisco Umbrella dans le cloud. Le système redirige les demandes de recherche DNS vers Cisco Umbrella, qui applique ensuite votre politique de nom de domaine complet (FQDN) Enterprise Security en nuage. Pour le trafic malveillant ou suspect, les utilisateurs peuvent être bloqués d'un site ou redirigés vers un proxy intelligent qui peut effectuer le filtrage d'URL en fonction de votre politique en nuage.

La procédure suivante explique le processus de bout en bout pour configurer Cisco Umbrella Connector.

Avant de commencer

En mode de contexte multiple, effectuez cette procédure dans chaque contexte de sécurité qui doit utiliser Cisco Umbrella.

Procédure

Étape 1 Créez un compte sur Cisco Umbrella, https://umbrella.cisco.com.

Étape 2 Installer le certificat d'autorité de certification à partir du serveur d'enregistrement Cisco Umbrella, à la page 99.

L'enregistrement du périphérique utilise HTTPS, ce qui nécessite l'installation du certificat racine.

Étape 3 Si ce n'est pas déjà fait, configurez les serveurs DNS et activez la recherche DNS sur les interfaces.

Configurez les paramètres sur la page **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **DNS Client (Client DNS)**.

Vous pouvez utiliser vos propres serveurs ou configurer les serveurs Cisco Umbrella. L'inspection DNS redirige automatiquement vers les résolveurs Cisco Umbrella, même si vous configurez des serveurs différents.

- 208.67.220.220
- 208.67.222.222
- 2620:119:53::53
- 2620:119:35::35

Étape 4 Configurer les paramètres globaux du connecteur Cisco Umbrella, à la page 100.

Étape 5 Activer Cisco Umbrella dans la liste des politiques d'inspection DNS, à la page 102.

Étape 6 Vérifier l'enregistrement de Cisco Umbrella, à la page 103.

Installer le certificat d'autorité de certification à partir du serveur d'enregistrement Cisco Umbrella

Vous devez importer le certificat racine pour établir la connexion HTTPS avec le serveur d'enregistrement de Cisco Umbrella. Le système utilise la connexion HTTPS lors de l'enregistrement du périphérique. Dans

Cisco Umbrella, choisissez **Deployments (Déploiements) > Configuration (Configuration) > Root Certificate (Certificat racine)** et téléchargez le certificat.

Avant de commencer

Lorsque Cisco Umbrella met à jour son certificat, vous devez télécharger le nouveau certificat. Le certificat racine peut également changer. Assurez-vous d'avoir téléchargé le bon certificat racine.

Lorsque vous mettez à jour le certificat, vous devez désactiver Cisco Umbrella, puis le réactiver, pour que le système prenne en compte le nouveau certificat et s'enregistre correctement auprès de Cisco Umbrella.

Procédure

Étape 1 Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats d'autorité de certification)**.

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Saisissez un **Trustpoint Name** (Nom du point de confiance), tel que ctx1 ou umbrella_server.

Étape 4 Sélectionnez **Paste Certificate in PEM Format** (Coller le certificat au format PEM), puis collez le certificat dans la boîte.

Peu importe si vous incluez les lignes BEGIN CERTIFICATE et END CERTIFICATE.

Étape 5 Cliquez sur **Install Certificate** (Installer le certificat).

Le certificat est créé sur le périphérique. Vous devrez actualiser votre affichage pour voir le point de confiance répertorié.

Configurer les paramètres globaux du connecteur Cisco Umbrella

Les paramètres globaux d'Umbrella définissent principalement le jeton API nécessaire pour enregistrer le périphérique auprès de Cisco Umbrella.

Les paramètres globaux ne sont pas suffisants pour activer Cisco Umbrella. Vous devez également activer Cisco Umbrella dans votre liste des politiques d'inspection DNS, comme décrit dans Activer Cisco Umbrella dans la liste des politiques d'inspection DNS, à la page 102.

Avant de commencer

- Connectez-vous au tableau de bord des périphériques réseau Cisco Umbrella (https://login.umbrella.com/) et obtenez un jeton API de périphérique réseau hérité pour votre organisation. Un jeton sera une chaîne hexadécimale, par exemple, AABBA59A0BDE1485C912AF. Générez une clé API pour les appareils réseau hérités à partir du tableau de bord Cisco Umbrella.
- Installez le certificat pour le serveur d'enregistrement Cisco Umbrella.

Procédure

Étape 1 Choisissez Configuration (**Configuration)** > **Firewall** > **(Pare-feu)** > **Objects** > **(Objets)** > **Umbrella** (Cisco Umbrella).

Étape 2 Sélectionnez **Enable Umbrella** (Activer Cisco Umbrella).

Étape 3 Saisissez le jeton API dans le champ **Token** (Jeton).

Étape 4 (Facultatif) Si vous avez l'intention d'activer DNScrypt dans la carte de stratégie d'inspection DNS, vous pouvez éventuellement configurer la clé **Public Key** (Clé publique) du fournisseur DNScrypt pour la vérification des certificats. Si vous ne configurez pas la clé, la clé publique par défaut actuellement distribuée est utilisée pour la validation.

La clé est une valeur hexadécimale de 32 octets. Saisissez la valeur hexadécimale en ASCII avec un séparateur de deux points tous les 2 octets. La clé fait 79 octets. Obtenez cette clé auprès de Cisco Umbrella.

La clé par défaut est :
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

Pour revenir à l'utilisation de la clé publique par défaut, supprimez la clé dans le champ **Public Key** (Clé publique).

Étape 5 (Facultatif) Sélectionnez **EDNS Timeout** (Délai d'expiration EDNS) et modifiez le délai d'inactivité après lequel une connexion d'un client au serveur Cisco Umbrella sera supprimée s'il n'y a pas de réponse du serveur.

Le délai d'expiration est au format heures:minutes:secondes et peut être compris entre 0:0:0 et 1193:0:0. La valeur par défaut est 0:02:00 (2 minutes).

Étape 6 (Facultatif) Dans **Resolver IPv4** (Résolveur IPv4) et **Resolver IPv6** (Résolveur IPv6), configurez les adresses des serveurs DNS Cisco Umbrella autres que les serveurs par défaut, qui résolvent les demandes DNS, que vous souhaitez utiliser.

Si vous ne configurez pas ces options, le système utilise les serveurs par défaut.

Étape 7 (Facultatif) Configurez les noms de domaine locaux pour lesquels Cisco Umbrella doit être contourné.

Vous pouvez identifier les domaines locaux pour lesquels les demandes DNS doivent contourner Cisco Umbrella et aller directement aux serveurs DNS configurés. Par exemple, vous pouvez demander à votre serveur DNS interne de résoudre tous les noms pour le nom de domaine de l'organisation en supposant que toutes les connexions internes sont autorisées.

Vous pouvez spécifier une seule classe d'expressions régulières qui inclut les objets d'expression régulière définissant les domaines locaux, ou saisir les noms directement en tant qu'objets d'expression régulière. Vous pouvez également les combiner, bien que vous ne puissiez avoir au plus qu'une seule classe.

Cliquez sur le bouton **Manage** (Gérer) à côté de l'option **Local Domain Bypass Regex Class** (Classe d'expressions régulières de contournement de domaine local) pour créer la classe. Vous pouvez également cliquer sur le bouton **Manage** (Gérer) dans la boîte de dialogue Add/Edit (Ajouter/Modifier) pour les expressions régulières afin de créer ces objets.

Activer Cisco Umbrella dans la liste des politiques d'inspection DNS

La configuration des paramètres globaux de Cisco Umbrella n'est pas suffisante pour enregistrer le périphérique et activer la redirection de recherche DNS. Vous devez ajouter Cisco Umbrella dans le cadre de votre inspection DNS active.

Vous pouvez activer Cisco Umbrella globalement en l'ajoutant à la liste des politiques d'inspection DNS preset_dns_map.

Toutefois, si vous avez personnalisé l'inspection DNS et appliqué différentes listes des politiques d'inspection à différentes classes de trafic, vous devez activer Cisco Umbrella sur chaque clesse pour laquelle vous souhaitez le service.

La procédure suivante explique comment mettre en œuvre Cisco Umbrella globalement. Si vous avez des listes des politiques DNS personnalisées, consultez Configurer la liste des politiques d'inspection DNS, à la page 309.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **DNS** .

Étape 2 Double-cliquez sur la liste d'inspection **preset_dns_map** pour la modifier.

Étape 3 Cliquez sur l'onglet **Cisco Umbrella Connections (connexions Cisco Umbrella)** et activez la connexion à Cisco Umbrella dans le nuage.

- **Cisco Umbrella** : active Cisco Umbrella. Vous pouvez éventuellement spécifier le nom de la politique Cisco Umbrella à appliquer au périphérique dans le champ **Umbrella Tag** (Balise Cisco Umbrella). Si vous ne spécifiez pas de politique, la politique par défaut est appliquée. Après l'enregistrement, l'ID de l'appareil Cisco Umbrella s'affiche à côté de la balise.
- **Enable DNScrypt** (Activer DNScrypt) : active DNScrypt pour chiffrer les connexions entre le périphérique et Cisco Umbrella. L'activation de DNScrypt démarre le fil d'échange de clés avec le résolveur Umbrella. Le fil d'échange de clés effectue l'établissement de liaison avec le résolveur toutes les heures et met à jour le périphérique avec une nouvelle clé secrète. Comme DNScrypt utilise UDP/443, vous devez vous assurer que la carte de trafic utilisée pour l'inspection DNS comprend ce port. Notez que la classe d'inspection par défaut comprend déjà UDP/443 pour l'inspection DNS.
- **Fail Open** (Autoriser en cas de défaillance) : activez cette option si vous souhaitez que la résolution DNS continue de fonctionner lorsque le serveur DNS Cisco Umbrella est indisponible. En cas d'échec de l'ouverture, si le serveur DNS Cisco Umbrella n'est pas disponible, Cisco Umbrella se désactive dans cette liste des politiques et permet aux demandes DNS d'accéder aux autres serveurs DNS configurés sur le système, le cas échéant. Lorsque les serveurs DNS Cisco Umbrella sont de nouveau disponibles, la liste des politiques reprend leur utilisation. Si vous ne sélectionnez pas cette option, les requêtes DNS continuent d'être acheminées vers le résolveur Cisco Umbrella inaccessible, de sorte qu'elles ne recevront pas de réponse

Étape 4 Cliquez sur **OK** .

Vérifier l'enregistrement de Cisco Umbrella

Après avoir configuré les paramètres globaux de Cisco Umbrella et avoir activé Cisco Umbrella dans l'inspection DNS, l'appareil doit communiquer avec Cisco Umbrella et s'enregistrer. Vous pouvez vérifier la réussite de l'enregistrement en vérifiant si Cisco Umbrella a fourni un identifiant d'appareil.

Utilisez **Tools (Outils)** > **Command Line Interface** (Interface de ligne de commande) ou une session SSH pour entrer ces commandes.

Tout d'abord, vérifiez les statistiques de la politique de service et recherchez la ligne d'enregistrement Cisco Umbrella. Il doit indiquer la politique appliquée par Cisco Umbrella (la balise), l'état HTTP de la connexion et l'ID de l'appareil.

L'état devrait être 200 Success (Réussite). Les codes d'erreur indiquent les éléments suivants : 401 indique que le jeton API était incorrect, et 409 indique que le périphérique existe déjà dans Cisco Umbrella.

Notez que les lignes du résolveur Cisco Umbrella ne doivent pas indiquer que les résolveurs ne répondent pas. Si tel est le cas, vérifiez que vous avez ouvert la communication DNS avec ces adresses IP dans votre politique de contrôle d'accès. Il peut s'agir d'une situation temporaire ou peut indiquer un problème de routage.

```
asa(config)# show service-policy inspect dns
Interface inside:
  Service-policy: global_policy
    Class-map: inspection_default
     Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate
 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
       umbrella registration: mode: fail-open tag: default, status: 200 success, device-id:
 010a13b8fbdfc9aa
          Umbrella ipv4 resolver: 208.67.220.220
          Umbrella ipv6 resolver: 2620:119:53::53
       Umbrella: bypass 0, req inject 0 - sent 0, res recv 0 - inject 0 local-domain-bypass
 10
        DNScrypt egress: rcvd 402, encrypt 402, bypass 0, inject 402
        DNScrypt ingress: rcvd 804, decrypt 402, bypass 402, inject 402
        DNScrypt: Certificate Update: completion 10, failure 1
```

Vous pouvez également vérifier la configuration en cours (filtre sur policy-map). La commande umbrella dans la liste des politiques est mise à jour pour afficher l'ID du périphérique. Vous ne pouvez pas configurer directement l'ID de l'appareil lorsque vous activez cette commande. L'exemple suivant modifie la sortie pour afficher les informations pertinentes. Vous pouvez également voir l'ID de l'appareil dans ASDM en modifiant la liste d'inspection DNS utilisée pour Cisco Umbrella ; l'ID est affiché sous l'onglet **Umbrella Connections** (Connexions Umbrella).

```
ciscoasa(config)# show running-config policy-map
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
  dnscrypt
  umbrella device-id 010a3e5760fdd6d3
  no tcp-inspection
policy-map global_policy
```

```
class inspection_default
  inspect dns preset_dns_map
```

Surveillance du connecteur Cisco Umbrella

Les rubriques suivantes expliquent comment surveiller Cisco Umbrella Connector.

Surveillance des statistiques de politique de service Cisco Umbrella

Vous pouvez afficher les statistiques récapitulées et détaillées pour l'inspection DNS avec Cisco Umbrella activé.

Utilisez **Tools (Outils)** > **Command Line Interface** (Interface de ligne de commande) ou une session SSH pour entrer ces commandes.

show service-policy inspect dns [**detail**]

Sans le mot-clé **detail**, vous voyez tous les compteurs d'inspection DNS de base ainsi que les informations de configuration Cisco Umbrella. Le champ d'état fournit le code d'état HTTP pour la tentative du système de s'enregistrer auprès de Cisco Umbrella.

Les lignes Resolver (résolveur) indiquent quels serveurs Cisco Umbrella sont utilisés. Ces lignes indiqueront si le serveur **ne répond pas**, ou si le système **sonde** actuellement le serveur pour déterminer s'il est devenu disponible. Si le mode est fail-open, le système permet aux demandes DNS d'être acheminées vers d'autres serveurs DNS (le cas échéant); sinon, les requêtes DNS ne recevront pas de réponse tant que les serveurs Cisco Umbrella ne répondront pas.

```
asa(config)# show service-policy inspect dns
Interface inside:
  Service-policy: global_policy
    Class-map: inspection_default
     Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate
 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
       umbrella registration: mode: fail-open tag: default, status: 200 success, device-id:
 010a13b8fbdfc9aa
          Umbrella ipv4 resolver: 208.67.220.220
          Umbrella ipv6 resolver: 2620:119:53::53
       Umbrella: bypass 0, req inject 0 - sent 0, res recv 0 - inject 0 local-domain-bypass
 10
        DNScrypt egress: rcvd 402, encrypt 402, bypass 0, inject 402
        DNScrypt ingress: rcvd 804, decrypt 402, bypass 402, inject 402
        DNScrypt: Certificate Update: completion 10, failure 1
```

La sortie détaillée affiche les statistiques DNScrypt et les clés utilisées.

```
asa(config)# show service-policy inspect dns detail
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
    Class-map: dnscrypt30000
```

```
     Inspect: dns dns_umbrella, packet 12, lock fail 0, drop 0, reset-drop 0,
              5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
       message-length maximum client auto, drop 0
       message-length maximum 1500, drop 0
       dns-guard, count 3
       protocol-enforcement, drop 0
       nat-rewrite, count 0
      Umbrella registration: mode: fail-open tag: default, status: 200 SUCCESS, device-id:
010af97abf89abc3, retry 0
         Umbrella ipv4 resolver: 208.67.220.220
         Umbrella ipv6 resolver: 2620:119:53::53
      Umbrella: bypass 0, req inject 6 - sent 6, res recv 6 - inject 6 local-domain-bypass
10
         Umbrella app-id fail, count 0
         Umbrella flow alloc fail, count 0
         Umbrella block alloc fail, count 0
         Umbrella client flow expired, count 0
         Umbrella server flow expired, count 0
         Umbrella request drop, count 0
         Umbrella response drop, count 0
       DNScrypt egress: rcvd 6, encrypt 6, bypass 0, inject 6
       DNScrypt ingress: rcvd 18, decrypt 6, bypass 12, inject 6
         DNScrypt length error, count 0
         DNScrypt add padding error, count 0
         DNScrypt encryption error, count 0
         DNScrypt magic_mismatch error, count 0
         DNScrypt disabled, count 0
         DNScrypt flow error, count 0
         DNScrypt nonce error, count 0
       DNScrypt: Certificate Update: completion 1, failure 1
         DNScrypt Receive internal drop count 0
         DNScrypt Receive on wrong channel drop count 0
         DNScrypt Receive cannot queue drop count 0
         DNScrypt No memory to create channel count 0
         DNScrypt Send no output interface count 1
         DNScrypt Send open channel failed count 0
         DNScrypt Send no handle count 0
         DNScrypt Send dupb failure count 0
         DNScrypt Create cert update no memory count 0
         DNScrypt Store cert no memory count 0
         DNScrypt Certificate invalid length count 0
         DNScrypt Certificate invalid magic count 0
         DNScrypt Certificate invalid major version count 0
         DNScrypt Certificate invalid minor version count 0
         DNScrypt Certificate invalid signature count 0
         Last Successful: 01:42:29 UTC May 2 2018, Last Failed: None
         Magic DNSC, Major Version 0x0001, Minor Version 0x0000,
         Query Magic 0x714e7a696d657555, Serial Number 1517943461,
         Start Time 1517943461 (18:57:41 UTC Feb 6 2018)
         End Time 1549479461 (18:57:41 UTC Feb 6 2019)
         Server Public Key
240B:11B7:AD02:FAC0:6285:1E88:6EAA:44E7:AE5B:AD2F:921F:9577:514D:E226:D552:6836
         Client Secret Key Hash
48DD:E6D3:C058:D063:1098:C6B4:BA6F:D8A7:F0F8:0754:40B0:AFB3:CB31:2B22:A7A4:9CEE
         Client Public key
6CB9:FA4B:4273:E10A:8A67:BA66:76A3:BFF5:2FB9:5004:CD3B:B3F2:86C1:A7EC:A0B6:1A58
         NM key Hash
9182:9F42:6C01:003C:9939:7741:1734:D199:22DF:511E:E8C9:206B:D0A3:8181:CE57:8020
```

Surveillance des messages Syslog Cisco Umbrella

Vous pouvez surveiller les messages de journal système liés à Cisco Umbrella suivants :

- %ASA-3-339001 : Échec de la mise à jour du certificat DNSCRYPT après *nombre* tentatives.

  Vérifiez qu'il y a une route vers le serveur Cisco Umbrella et que l'interface de sortie est opérationnelle et fonctionne correctement. Vérifiez aussi que la clé publique configurée pour DNScrypt est correcte. Vous devrez peut-être obtenir une nouvelle clé de Cisco Umbrella.

- %ASA-3-339002 : L'enregistrement de l'appareil Cisco Umbrella a échoué avec le code d'erreur *error_code*.

  Les codes d'erreur ont les significations suivantes :

  - 400 : il y a un problème de format ou de contenu de la demande. Le jeton est probablement trop court ou corrompu. Vérifiez que le jeton correspond à celui sur le tableau de bord Cisco Umbrella.
  - 401 : le jeton API n'est pas autorisé. Essayez de reconfigurer le jeton. Si vous avez actualisé le jeton dans le tableau de bord Cisco Umbrella, vous devez vous assurer d'utiliser le nouveau jeton.
  - 409 : l'ID de l'appareil est en conflit avec une autre organisation. Veuillez vérifier auprès de l'Administrateur Cisco Umbrella pour voir quel est le problème.
  - 500 : il y a une erreur de serveur interne. Vérifiez auprès de l'Administrateur Cisco Umbrella pour voir quel est le problème.

- %ASA-6-339003 : L'enregistrement de l'appareil Cisco Umbrella a réussi.

- %ASA-3-339004 : L'enregistrement de l'appareil Cisco Umbrella a échoué en raison d'un jeton manquant.

  Vous devez obtenir un jeton API de Cisco Umbrella et le configurer dans les paramètres globaux de Cisco Umbrella.

- %ASA-3-339005 : L'enregistrement de l'appareil Cisco Umbrella a échoué après *plusieurs* tentatives.

  Consultez les messages du journal système 339002 pour identifier les erreurs que vous devez corriger.

- %ASA-3-339006 : l'*IP_address* du résolveur Cisco Umbrella est accessible, ce qui reprend la redirection Umbrella.

  Ce message indique que le système fonctionne normalement. Aucune autre mesure n'est nécessaire.

- %ASA-3-339007 : l'*IP_address* du résolveur Cisco Umbrella ne répond pas et le mode de fermeture en cas de non-conformité est utilisé, démarrant la sonde pour le résolveur.

  Comme vous utilisez le mode de fermeture en cas de non-conformité, les utilisateurs ne recevront pas de réponses à leurs demandes DNS tant que le serveur DNS Cisco Umbrella ne sera pas de nouveau en ligne. Si le problème persiste, vérifiez qu'il existe une voie de routage entre le système et les serveurs Cisco Umbrella, et que vous autorisez le trafic DNS vers les serveurs dans votre politique de contrôle d'accès.

Historique du connecteur Cisco Umbrella

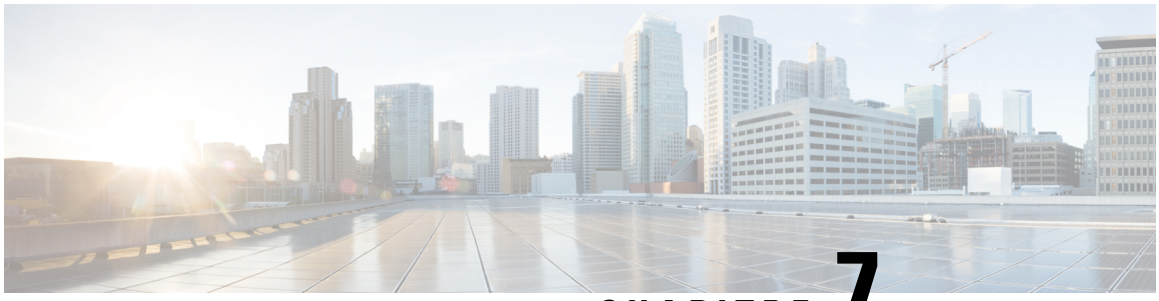
Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de Cisco Umbrella	9.10(1)	Vous pouvez configurer le périphérique pour rediriger les requêtes DNS vers Cisco Umbrella, afin que votre politique de sécurité d'entreprise définie dans Cisco Umbrella puisse être appliquée aux connexions des utilisateurs. Vous pouvez autoriser ou bloquer les connexions en fonction du FQDN ou, pour les FQDN suspects, vous pouvez rediriger l'utilisateur vers le mandataire intelligent Cisco Umbrella, qui peut effectuer le filtrage d'URL. La configuration de Cisco Umbrella fait partie de la politique d'inspection DNS. Écrans nouveaux ou modifiés : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Cisco Umbrella**, **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **DNS**.
Améliorations de Cisco Umbrella.	9.12(1)	Vous pouvez maintenant identifier les noms de domaine locaux qui doivent contourner Cisco Umbrella. Les demandes DNS pour ces domaines sont directement transmises aux serveurs DNS sans passer par Cisco Umbrella. Vous pouvez également identifier les serveurs Cisco Umbrella à utiliser pour la résolution des demandes DNS. Enfin, vous pouvez définir la politique d'inspection de Cisco Umbrella pour qu'elle s'ouvre même en cas de non-conformité, afin que les demandes DNS ne soient pas bloquées si le serveur Cisco Umbrella n'est pas disponible. Nous avons modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Cisco Umbrella**, **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **DNS**.



PARTIE II

Services de pare-feu pour les environnements virtuels

• Contrôle d’accès basé sur les attributs, à la page 111



CHAPITRE 7

Contrôle d'accès basé sur les attributs

Les attributs sont des objets réseau personnalisés à utiliser dans votre configuration. Vous pouvez les définir et les utiliser dans les configurations ASA pour filtrer le trafic associé à une ou plusieurs machines virtuelles dans un environnement VMware ESXi géré par VMware vCenter. Vous pouvez définir des listes de contrôle d'accès (ACL) pour affecter des politiques au trafic provenant de groupes de VM partageant un ou plusieurs attributs. Vous attribuez des attributs aux machines virtuelles dans l'environnement ESXi et configurez un agent d'attribut, qui se connecte à vCenter ou à un seul hôte ESXi à l'aide du protocole HTTPS. L'agent demande et récupère ensuite une ou plusieurs liaisons qui mettent en corrélation des attributs spécifiques avec l'adresse IP principale d'une machine virtuelle.

Le contrôle d'accès basé sur les attributs est pris en charge sur toutes les plateformes matérielles et sur toutes les plateformes ASA virtuelles fonctionnant sur les hyperviseurs ESXi, KVM ou HyperV. Les attributs ne peuvent être récupérés qu'à partir de machines virtuelles fonctionnant sur un hyperviseur ESXi.

- Lignes directrices relatives aux objets réseau basés sur les attributs, à la page 111
- Configurer le contrôle d'accès basé sur les attributs, à la page 112
- Surveillance des objets réseau basés sur les attributs , à la page 117
- Historique du contrôle d'accès basé sur les attributs, à la page 117

Lignes directrices relatives aux objets réseau basés sur les attributs

Directives IPv6

- Adresses IPv6 non prises en charge par vCenter pour les informations d'authentification de l'hôte.
- IPv6 est pris en charge pour les liaisons de machine virtuelle où l'adresse IP principale de la machine virtuelle est une adresse IPv6.

Directives et limites additionnelles

- Le mode multi-contexte n'est pas pris en charge. Les objets réseau basés sur les attributs sont pris en charge pour le contexte en mode unique uniquement.
- Les objets réseau basés sur les attributs prennent en charge uniquement la liaison à l'adresse principale de la machine virtuelle. La liaison à plusieurs vNIC sur une seule machine virtuelle n'est pas prise en charge.

- Les objets réseau basés sur les attributs ne peuvent être configurés que pour les objets utilisés pour les groupes d'accès. Les objets réseau pour d'autres fonctionnalités (NAT, etc.) ne sont pas pris en charge.
- Les machines virtuelles doivent exécuter les outils VMware afin de signaler les adresses IP principales à vCenter. L'ASA n'est pas informé des modifications d'attributs, sauf si vCenter sait l'adresse IP de la machine virtuelle. Il s'agit d'une restriction vCenter.
- Les objets réseau basés sur les attributs ne sont pas pris en charge dans les environnements Amazon Web Services (AWS) ou Microsoft Azure.

Configurer le contrôle d'accès basé sur les attributs

La procédure suivante fournit une séquence générale pour la mise en œuvre du contrôle d'accès basé sur les attributs sur les machines virtuelles gérées dans un environnement VMware ESXi.

Procédure

Étape 1 Attribuez des types d'attributs et des valeurs personnalisés à vos machines virtuelles gérées. Consultez Configurer les attributs des machines virtuelles vCenter, à la page 112.

Étape 2 Configurez un agent d'attributs pour une connexion à votre serveur vCenter ou à votre hôte ESXi. Consultez Configurer un agent d'attribut de VM, à la page 114.

Étape 3 Configurez les objets réseau basés sur les attributs nécessaires pour votre schéma de déploiement. Consultez Configurer les objets réseau basés sur les attributs, à la page 115.

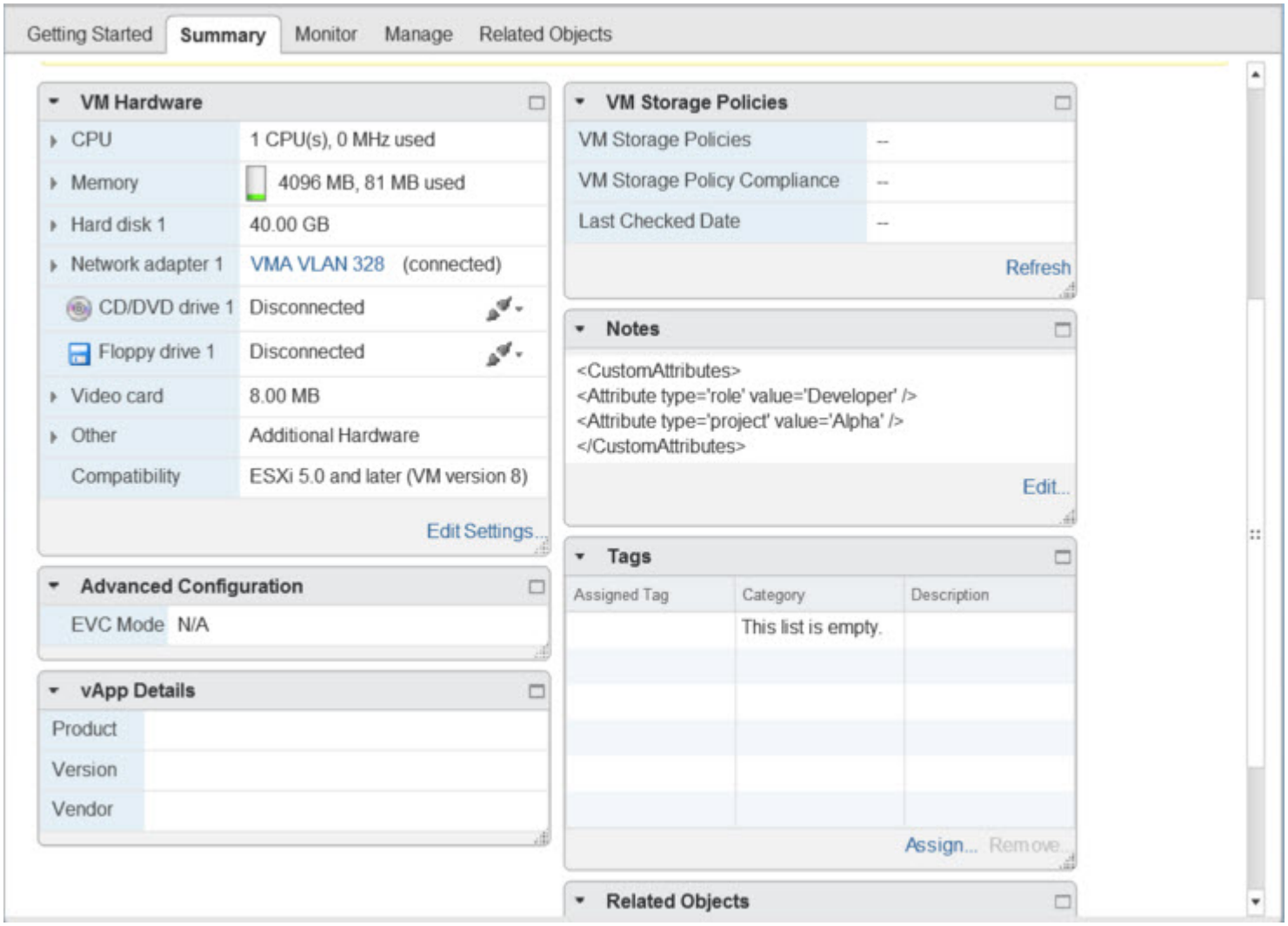
Étape 4 Configurez les listes de contrôle d'accès et les règles. Voir Configurer les règles d'accès à l'aide d'objets réseau basés sur les attributs, à la page 116 .

Configurer les attributs des machines virtuelles vCenter

Vous attribuez des types d'attributs et des valeurs personnalisés aux machines virtuelles et associez ces attributs aux objets réseau. Vous pouvez ensuite utiliser ces objets réseau basés sur des attributs pour appliquer des listes de contrôle d'accès à un ensemble de machines virtuelles ayant des caractéristiques communes définies par l'utilisateur. Par exemple, vous pouvez isoler les machines de version de développeur des machines de test, ou regrouper les machines virtuelles par projet et/ou emplacement. Pour que l'ASA surveille les machines virtuelles à l'aide des attributs, vous devez mettre les attributs à la disposition de vCenter à partir des machines virtuelles gérées. Vous le faites en insérant un fichier texte formaté dans le champ Notes, qui se trouve sur la page Summary (Résumé) des machines virtuelles dans vCenter.

Vous pouvez voir le champ Notes dans la figure suivante.

Illustration 6 : Onglet Summary (Résumé) d'une machine virtuelle dans vCenter



Pour spécifier des attributs personnalisés, vous copiez un fichier XML correctement formaté dans le champ Notes de la machine virtuelle. Le format du fichier est :

```
<CustomAttributes>
<Attribute type='attribute-type' value='attribute-value'/>
...
</CustomAttributes>
```

Une seule machine virtuelle peut avoir plusieurs attributs définis par la répétition de la deuxième ligne ci-dessus. Notez que chaque ligne doit identifier un type d'attribut unique. Si le même type d'attribut est défini avec plusieurs valeurs d'attribut, chaque mise à jour de liaison pour ce type d'attribut remplacera la précédente.

Pour les valeurs d'attribut de chaîne, la valeur associée à la définition d'objet doit correspondre exactement à la valeur signalée à vCenter par la machine virtuelle. Par exemple, une valeur d'attribut *Build Machine* ne correspond pas à la valeur d'inscription *build machine* sur la machine virtuelle. Aucune liaison ne sera ajoutée à la liste d'hôte pour cet attribut.

Vous pouvez définir plusieurs types d'attributs uniques dans un seul fichier.

Procédure

Étape 1 Sélectionnez la machine virtuelle dans votre inventaire vCenter.

Étape 2 Cliquez sur l'onglet **Summary** (Résumé) de la machine virtuelle.

Étape 3 Dans le champ **Notes**, cliquez sur le lien **de modification**.

Étape 4 Collez le fichier texte des attributs personnalisés dans la zone **Modifier les notes**. Le fichier texte doit suivre le format du modèle XML :

Exemple :

```
<CustomAttributes>
<Attribute type='attribute-type' value='attribute-value'/>
...
</CustomAttributes>
```

Étape 5 Cliquez sur **OK**.

Configurer un agent d'attribut de VM

Vous configurez un agent d'attribut de VM pour communiquer avec vCenter ou un seul hôte ESXi. Lorsque vous attribuez des attributs aux machines virtuelles dans l'environnement VMware, l'agent d'attributs envoie un message à vCenter pour indiquer quels attributs ont été configurés, et vCenter répond par une mise à jour de liaison pour chaque machine virtuelle pour laquelle un type d'attribut correspondant est configuré.

L'agent d'attributs de VM et vCenter échangent des mises à jour de liaison comme suit :

- Si l'agent émet une demande contenant un nouveau type d'attribut, vCenter répond avec une mise à jour de liaison pour chaque machine virtuelle où le type d'attribut est configuré. Passé ce point, vCenter n'émet une nouvelle liaison que lorsqu'une valeur d'attribut est ajoutée ou modifiée.
- Si un attribut surveillé change pour une ou plusieurs machines virtuelles, un message de mise à jour de liaison est reçu. Chaque message de liaison est identifié par l'adresse IP de la machine virtuelle qui signale la valeur de l'attribut.
- Si plusieurs attributs sont surveillés par un seul agent, une seule mise à jour de liaison contient la valeur actuelle de tous les attributs surveillés pour chaque machine virtuelle.
- Si un attribut spécifique surveillé par l'agent n'est pas configuré sur une machine virtuelle, la liaison contiendra une valeur d'attribut vide pour cette machine virtuelle.
- Si une machine virtuelle n'a pas été configurée avec des attributs surveillés, vCenter n'envoie pas de mise à jour de liaison.

Chaque agent d'attribut communique avec exactement un hôte vCenter ou ESXi. Un seul ASA peut avoir plusieurs agents d'attributs définis, chacun communiquant avec un vCenter différent, ou un ou plusieurs communiquant avec le même vCenter.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **VM Attribute Agent (Agent d'attribut de VM)**.

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Dans la zone Informations sur l'hôte :

a) Choisissez d'activer l'adresse IP et les informations d'authentification.
b) Saisissez le nom d'hôte ou l'adresse IP.
c) Saisir un nom d'utilisateur.
d) Sélectionnez le type de mot de passe : **Clear Text** (Texte en clair), **UnEncrypted** (Non chiffré) ou **Encrypted** (Chiffré).
e) Saisissez le mot de passe

Étape 4 Dans la zone d'informations Keepalive Information (Informations keepalive) :

a) Saisissez l' **intervalle de nouvelle tentative**. Saisissez une valeur entre 1 et 65 535. La valeur par défaut est 30.
b) Saisissez le **nombre de tentatives**. Saisissez une valeur entre 1 et 32. La valeur par défaut est de 3.

Étape 5 Cliquez sur **OK**.

Configurer les objets réseau basés sur les attributs

Les objets réseau basés sur les attributs filtrent le trafic en fonction des attributs associés à une ou plusieurs machines virtuelles dans un environnement VMware ESXi. Vous pouvez définir des listes de contrôle d'accès (ACL) pour affecter des politiques au trafic provenant de groupes de machines virtuelles partageant un ou plusieurs attributs.

Par exemple, vous pouvez configurer des règles d'accès qui permettent aux machines ayant un attribut *engineering* d'accéder aux machines avec un attribut *eng_lab*. Un administrateur réseau peut ajouter ou supprimer des machines d'ingénierie et des serveurs de laboratoire pendant que la politique de sécurité gérée par l'administrateur de sécurité continue de fonctionner automatiquement sans mises à jour manuelles des règles d'accès.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Règles d'accès)** > **Advanced Options (Options avancées)**.

Étape 2 Cochez la case **Enable Object Group Search Algorithm** (Activer l'algorithme de recherche de groupe d'objets).

Vous devez activer la recherche de groupe d'objets pour configurer les attributs de VM.

Étape 3 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Objects/Groups (Objets/groupes de services réseau)**.

Étape 4 Effectuez l'une des opérations suivantes :

- Choisissez **Add (Ajouter) > Network Object Attributes (Attributs d'objet réseau)** pour ajouter un nouvel objet réseau basé sur les attributs. Saisissez un nom et, éventuellement, une description.
- Choisissez un objet réseau existant basé sur les attributs et cliquez sur **Edit** (Modifier).

Étape 5 Pour un nouvel objet réseau basé sur les attributs, saisissez des valeurs dans les champs suivants :

a) **Agent Name** (Nom de l'agent) : cliquez sur le bouton de navigation et sélectionnez un agent d'attribut de VM (ou définissez-en un nouveau).

Si vous configurez un objet réseau basé sur les attributs pour utiliser un agent d'attribut qui n'a pas été configuré, un agent d'espace réservé est automatiquement créé sans informations d'authentification et avec des valeurs keepalive par défaut. Cet agent reste dans l'état « No credentials available » (Aucun identifiant disponible) jusqu'à ce que les informations d'authentification de l'hôte soient fournies.

b) **Attribute Type** (Type d'attribut) : cette entrée de chaîne définit le type d'attribut et doit inclure le préfixe **custom**. Par exemple, custom.role.

c) **Attribute Value** (Valeur d'attribut) : cette entrée de chaîne associe une valeur au type d'attribut.

Ensemble, la paire *Attribute Type (Type d'attribut)* et *Attribute Value (Valeur d'attribut)* définit un attribut unique. Cela vous permet de définir plusieurs attributs qui correspondent à votre schéma de déploiement particulier. Si vous définissez le même type d'attribut plus d'une fois avec plusieurs valeurs d'attribut, la dernière valeur définie remplace la précédente.

Étape 6 Cliquez sur **OK**.

Configurer les règles d'accès à l'aide d'objets réseau basés sur les attributs

Pour appliquer une règle d'accès à l'aide d'objets réseau basés sur des attributs, procédez comme suit.

Procédure

Étape 1 Choose **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Règles d'accès)**.

Les règles sont classées par interface et direction, avec un groupe distinct pour les règles globales. Si vous configurez des règles d'accès de gestion, elles sont répétées sur cette page. Ces groupes sont équivalents à la liste de contrôle d'accès étendue qui est créée et affectée à l'interface ou globalement en tant que groupe d'accès. Ces ACL apparaissent également sur la page ACL Manager (Gestionnaire d'ACL).

Étape 2 Effectuez l'une des actions suivantes :

- Pour ajouter une nouvelle règle, choisissez Add (Ajouter) **> Add Access Rule** (Ajouter une règle d'accès).
- Pour insérer une règle à un emplacement spécifique dans un conteneur, sélectionnez une règle existante et choisissez **Add (Ajouter) > Insert (Insérer)** pour ajouter la règle au-dessus, ou choisissez **Add (Ajouter) > Insert After (Insérer après)**.
- Pour modifier une règle, sélectionnez-la et cliquez sur **Edit** (Modifier).

Étape 3 Renseignez les propriétés de la règle. Les principales options à sélectionner sont les suivantes :

- **Interface** : l'interface à laquelle la règle s'applique. Sélectionnez Any (Tous) pour créer une règle globale. Pour les groupes de ponts en mode routé, vous pouvez créer des règles d'accès pour l'interface virtuelle de pont (BVI) et chaque interface de membre de groupe de ponts.
- **Action : Permit/Deny (Autoriser/Refuser)** : précisez si vous autorisez le trafic décrit ou si vous le bloquez.
- **Source/Destination criteria** (Critères source/destination) : sélectionnez l'objet réseau basé sur l'attribut source (objet d'origine) et l'objet réseau basé sur l'attribut de destination (objet cible du flux de trafic). Vous pouvez également préciser un nom d'utilisateur ou de groupe d'utilisateurs pour la source. En outre, vous pouvez utiliser le champ Service pour identifier le type spécifique de trafic si vous souhaitez cibler la règle de manière plus étroite que tout le trafic IP. Si vous mettez en œuvre Cisco TrustSec, vous pouvez utiliser des groupes de sécurité pour définir la source et la destination.

Pour des informations détaillées sur les options, consultez Propriétés de la règle d'accès, à la page 20.

Lorsque vous avez terminé de définir la règle, cliquez sur **OK** pour l'ajouter au tableau.

Étape 4 Cliquez sur **Apply** (Appliquer) pour enregistrer la règle d'accès dans votre configuration.

Surveillance des objets réseau basés sur les attributs

Pour les objets réseau basés sur des attributs, vous pouvez analyser l'utilisation d'un objet individuel. À partir de leur page dans le dossier **Configuration > Firewall (Pare-feu) > Objects (Objets) > Network Objects/Groups (Objets/groupes réseau)**, cliquez sur le bouton **Where Used** (Où utilisé).

Pour les objets réseau basés sur des attributs, vous pouvez également cliquer sur le bouton Not Used (Non utilisé) pour rechercher les objets qui ne sont utilisés dans aucune règle. Cet affichage vous donne un raccourci pour supprimer ces objets inutilisés.

Historique du contrôle d'accès basé sur les attributs

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge des objets réseau basés sur les attributs	9.7(1)	Vous pouvez désormais contrôler l'accès réseau à l'aide des attributs de la machine virtuelle en plus des caractéristiques du réseau traditionnelles telles que les adresses IP, les protocoles et les ports. Les machines virtuelles doivent se trouver dans un environnement VMware ESXi. Nous avons introduit ou modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Object Attributes (Attributs d'objet réseau)**. Nous avons introduit l'écran suivant : **Configuration** > **Firewall** (Pare-feu) > VM **Attribute Agent (Agent d'attributs de VM)** .

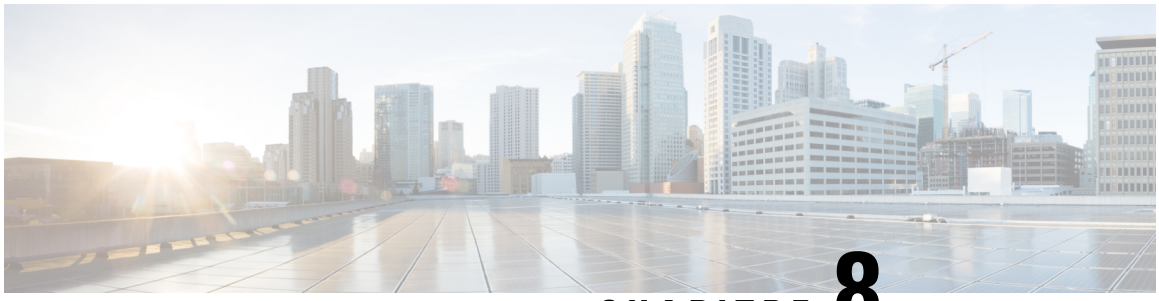
Nom de la caractéristique	Versions de plateforme	Description
Suppression de la prise en charge des objets réseau basés sur les attributs de VM de l'ASA 5506-X (tous les modèles), 5508-X, 5512-X, 5516-X.	9.10(1)	Vous ne pouvez plus utiliser d'objets réseau basés sur des attributs de VM sur les plateformes suivantes : ASA 5506-X (tous les modèles), 5508-X, 5512-X, 5516-X.



PARTIE III

NAT (Network Address Translation; Translation d'adresses de réseau)

- Traduction d’adresses réseau (NAT), à la page 121
- Exemples et références de NAT, à la page 195
- Mappage de l’adresse et du port (MAP), à la page 259



CHAPITRE 8

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 121
- Principes de base de la NAT, à la page 122
- Directives pour la NAT, à la page 127
- Traduction d'adresses réseau dynamique, à la page 135
- PAT dynamique, à la page 144
- NAT statique, à la page 166
- NAT d'identité, à la page 178
- Surveillance de la NAT, à la page 186
- Historique de la NAT, à la page 186

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 routé 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 (adresse/hôte/réseau/interface réelle) : 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 135.
- 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 144.
- 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 166.
- 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 178.

NAT objet de réseau et Twice NAT (NAT en double)

Vous pouvez mettre en œuvre la traduction d'adresses de deux manières : *network object NAT (NAT objet de réseau)* et *twice NAT (NAT en double)*.

Nous vous recommandons d'utiliser la network object NAT (NAT objet de réseau), sauf si vous avez besoin des fonctionnalités supplémentaires offertes par twice NAT (NAT en double). Il est plus facile de configurer network object NAT (NAT objet de réseau) 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 objet de réseau

Toutes les règles NAT configurées comme paramètre d'un objet réseau sont considérées comme des règles *network object NAT (NAT objet de réseau)*. 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.

Après avoir configuré l'objet réseau, vous pouvez identifier l'adresse mappée de cet objet, soit en tant qu'adresse en ligne, soit en tant qu'autre objet de réseau ou groupe d'objets réseau.

Lorsqu'un paquet entre dans une interface, les adresses IP de source et de destination sont vérifiées par rapport aux règles network object NAT (NAT objet de réseau). 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 twice NAT (NAT en double) pour ce type de fonctionnalité, où vous pouvez identifier l'adresse de source et de destination dans une seule règle.

Twice NAT (NAT en double)

Twice NAT (NAT en double) 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 NAT objet de réseau et Twice NAT (NAT en double)

Les principales différences entre ces deux types de NAT sont les suivantes :

- Votre définition de l'adresse réelle.
  - NAT d'objet réseau : vous définissez la NAT comme paramètre pour un objet réseau. Un objet réseau nomme un hôte, une plage ou un sous-réseau IP afin que vous puissiez ensuite utiliser l'objet dans la configuration NAT au lieu des adresses IP réelles. L'adresse IP de l'objet réseau sert d'adresse réelle. Cette méthode vous permet d'ajouter facilement une NAT à des objets réseau qui peuvent déjà être utilisés dans d'autres parties de votre configuration.
  - Twice NAT (NAT en double) : 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 twice NAT (NAT en double) est plus évolutif.
- Mise en œuvre de la NAT de source et de destination.
  - NAT objet de réseau : 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.
  - Twice NAT (NAT en double) : 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 twice NAT (NAT en double). 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 objet de réseau : classés automatiquement dans la table NAT.
  - Twice NAT (NAT en double) : classés manuellement dans la table NAT (avant ou après les règles network object NAT (NAT objet de réseau)).

Ordre des règles NAT

Les règles NAT objet de réseau et twice NAT (NAT en double) 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 7 : Tableau des règles NAT.

Section de tableau	Type de règle	Ordre des règles dans la section
Section 1	Twice NAT (NAT en double)	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 twice NAT (NAT en double) 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 de tableau	Type de règle	Ordre des règles dans la section
Section 2	NAT objet de réseau	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	Twice NAT (NAT en double)	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)

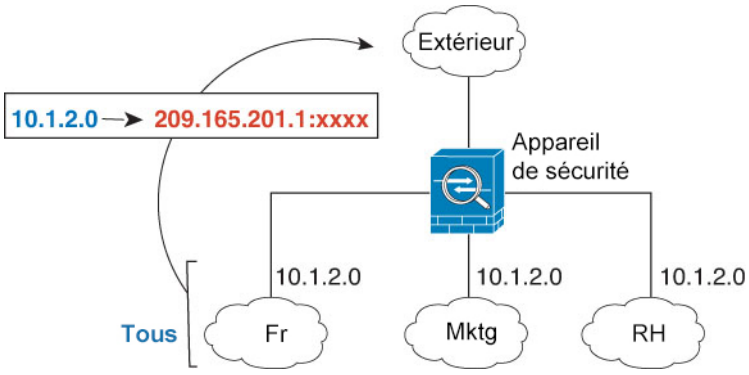
- 172.16.1.0/24 (dynamique) (définition de l'objet)
- 192.168.1.0/24 (dynamique)

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 Internet.

Illustration 7 : 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.

Directives pour la NAT

Les rubriques suivantes fournissent des instructions détaillées pour la mise en œuvre de la NAT.

Lignes directrices sur le mode pare-feu pour la NAT

La NAT est prise en charge en mode de pare-feu routé et transparent.

Cependant, la configuration de la NAT sur les interfaces membres de groupes de ponts (les interfaces qui font partie d'une interface virtuelle de groupe de ponts, ou BVI) a les 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 une NAT entre des interfaces de membres de groupes de ponts, vous devez préciser les adresses réelles et mappées. Vous ne pouvez pas définir « any » comme interface.
- Vous ne pouvez pas configurer l'interface PAT lorsque l'adresse mappée est une interface de membre d'un groupe de ponts, 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 dynamique44/66 et le PAT44 dynamique sont les seules méthodes autorisées; Le PAT66 dynamique n'est pas pris en charge. Cependant, vous pouvez effectuer une NAT64/46 entre les membres de différents groupes de ponts ou entre un membre d'un groupe de ponts (source) et l'interface de routage standard (destination).

Lignes directrices relatives à la NAT 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 (twice NAT (NAT en double) 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 (twice NAT (NAT en double) 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. Vous pouvez également traduire les adresses réseau à réseau, où la première adresse IPv4 est mappée à la première adresse IPv6, la deuxième à la seconde, et ainsi de suite.

- 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.

Lignes directrices 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 objet de réseau 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 le 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 tentative de rétablissement de la connexion devrait atteindre la règle NAT et la connexion devrait être NATée 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.

- Lors de la traduction du trafic SCTP, utilisez uniquement la NAT de l'objet réseau statique. La NAT ou la PAT dynamique ne sont pas autorisées. Bien que vous puissiez configurer deux règles de NAT statique, cela n'est pas recommandé, car la topologie de la partie destination de l'association SCTP est inconnue.
- Les objets et les groupes d'objets utilisés dans la NAT ne peuvent pas être non définis; ils doivent inclure des adresses IP.
- 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.
- (Twice NAT (NAT en double) seulement.) Lorsque vous utilisez **any** (n'importe laquelle) comme adresse source dans une règle NAT, la définition du trafic « any » (IPv4 ou IPv6) dépend de la règle. Avant que ASA effectue la NAT sur un paquet, le paquet doit être IPv6-vers-IPv6 ou IPv4-vers-IPv4; avec cette condition préalable, ASA 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
  - (Mode transparent.) L'adresse IP de gestion.
  - (NAT dynamique.) L'adresse IP de l'interface de secours lorsque le VPN est activé.
  - Ensemble d'adresses de VPN existantes
- 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.
- Pour les limites de l'inspection des applications avec NAT ou PAT, consultez Inspections par défaut et limites de la NAT, à la page 289.
- 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. Consultez Routage des paquets NAT, à la page 223 pour de plus amples renseignements.
- Si vous activez la commande **arp permit-nonconnected**, le système ne répond pas aux requêtes ARP si l'adresse mappée ne fait partie d'aucun sous-réseau connecté et vous ne spécifiez pas non plus l'interface mappée dans la règle NAT (c'est-à-dire si vous spécifiez « any »). Pour résoudre ce problème, spécifiez l'interface mappée.
- 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.

- Si vous utilisez PAT sur le trafic RPC de Sun, qui est utilisé pour la connexion aux serveurs NFS, sachez que le serveur NFS peut rejeter des connexions si le port PAT est supérieur à 1024. La configuration par défaut des serveurs NFS est de rejeter les connexions des ports d'une valeur supérieure à 1024. L'erreur est généralement « Autorisation refusée ». Le mappage des ports supérieurs à 1024 peut se produire si vous utilisez l'option « flat range » pour utiliser les numéros de port les plus élevés si un port de la plage inférieure n'est pas disponible, en particulier si vous ne sélectionnez pas l'option d'inclusion de la plage inférieure dans la plage fixe. Le mappage des ports supérieurs à 1024 se produit si vous ne sélectionnez pas l'option d'inclusion des ports réservés (1 à 1023) dans la plage de ports d'un ensemble PAT. Vous pouvez éviter ce problème en modifiant la configuration du serveur NFS pour autoriser tous les numéros de port.
- La NAT s'applique uniquement au trafic de transit. Le trafic généré par le système n'est pas soumis à la NAT.
- Vous pouvez améliorer les performances et la fiabilité du système en utilisant le modèle de validation transactionnelle pour la NAT. Pour plus d'informations, consultez le chapitre sur les paramètres de base dans le guide de configuration des opérations générales. L'option se trouve sous **Configurations (Configurations) > Device Management (gestion des périphériques) > Advanced (Avancé) > Rule Engine (moteur de règles)**.
- N'utilisez pas de combinaisons de lettres majuscules ou minuscules avant de nommer un objet réseau ou un ensemble TAP.
- L'option unidirectionnelle est surtout utile dans l'exécution de tests et peut ne pas fonctionner avec tous les protocoles. Par exemple, SIP nécessite une inspection de protocole pour traduire les en-têtes SIP à l'aide de la NAT, des processus impossibles si vous sélectionnez la traduction unidirectionnelle.
- Vous ne pouvez pas utiliser la NAT sur la charge utile interne des registres PIM (Protocol Independent Multicast).
- (Twice NAT (NAT en double)) 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 politique de contrôle d'accès correspondante.

Lignes directrices de NAT d'objets réseau pour les objets d'adresses mappées

Pour la NAT dynamique, vous devez utiliser un objet ou un groupe pour les adresses mappées. Pour les autres types de NAT, vous pouvez utiliser un objet ou un groupe, ou vous avez la possibilité d'utiliser des adresses en ligne. Les groupes d'objets réseau sont particulièrement utiles pour créer un ensemble d'adresses mappées avec des plages d'adresses IP discontinues ou plusieurs hôtes ou sous-réseaux.

Tenez compte des Lignes directrices suivantes lors de la création d'objets pour les adresses mappées.

- Un groupe d'objets réseau peut contenir des objets ou des adresses en ligne des adresses IPv4 ou IPv6. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses.
- Consultez Lignes directrices supplémentaires pour la NAT, à la page 129 pour en savoir plus sur les adresses IP mappées non autorisées.
- N'utilisez pas de combinaisons de lettres majuscules ou minuscules pour nommer un objet réseau ou un ensemble PAT.
- NAT dynamique :
  - Vous ne pouvez pas utiliser une adresse en ligne; vous devez configurer un objet ou un groupe réseau.
  - L'objet ou le groupe ne peut pas contenir de sous-réseau; l'objet doit définir une plage ; le groupe peut inclure des hôtes et des plages.
  - Si un objet réseau mappé contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP d'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 (masquer) :
  - Au lieu d'utiliser un objet, vous pouvez éventuellement configurer une adresse d'hôte en ligne ou préciser l'adresse de l'interface.
  - Si vous utilisez un objet, l'objet ou le groupe ne peut pas contenir de sous-réseau. L'objet doit définir un hôte ou, pour un pool PAT, une plage. Le groupe (pour un ensemble PAT) peut inclure des hôtes et des plages.
- NAT statique ou NAT statique avec traduction de port
  - Au lieu d'utiliser un objet, vous pouvez configurer une adresse en ligne ou préciser l'adresse de l'interface (pour la NAT statique avec traduction de port).
  - Si vous utilisez un objet, l'objet ou le groupe peut contenir un hôte, une plage ou un sous-réseau.
- NAT d'identité
  - Au lieu d'utiliser un objet, vous pouvez configurer une adresse en ligne.

- Si vous utilisez un objet, celui-ci doit correspondre aux adresses réelles que vous souhaitez traduire.

Lignes directrices pour le NAT Twice concernant les objets d'adresses réelles et mappées

Pour chaque règle NAT, configurez jusqu'à quatre objets ou groupes réseau pour :

- Adresse réelle de la source
- Adresse mappée de la source
- Adresse réelle de destination
- Adresse mappée de destination

Les objets sont requis, sauf si vous spécifiez le mot-clé **any** en ligne pour représenter tout le trafic ou, pour certains types de NAT, le mot-clé **interface** pour représenter l'adresse de l'interface. Les groupes d'objets réseau sont particulièrement utiles pour créer un ensemble d'adresses mappées avec des plages d'adresses IP discontinues ou plusieurs hôtes ou sous-réseaux.

Tenez compte des lignes directrices suivantes lors de la création d'objets pour la NAT Twice.

- Un groupe d'objets réseau peut contenir des objets ou des adresses en ligne IPv4 ou IPv6. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses.
- Consultez Lignes directrices supplémentaires pour la NAT, à la page 129 pour en savoir plus sur les adresses IP mappées non autorisées.
- N'utilisez pas de combinaisons de lettres majuscules ou minuscules pour nommer un objet réseau ou un ensemble PAT.
- NAT dynamique source :
  - Vous configurez généralement un groupe plus important d'adresses réelles à mapper à un groupe plus restreint.
  - L'objet ou le groupe mappé ne peut pas contenir de sous-réseau; l'objet doit définir une plage; le groupe peut inclure des hôtes et des plages.
  - Si l'objet réseau mappé contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP d'hôte sont utilisées comme PAT de secours. Si l'objet ne contient qu'une seule adresse d'hôte, il est utilisé pour la PAT.
- NAT dynamique source PAT (masquer) :
  - Si vous utilisez un objet, l'objet ou le groupe ne peut pas contenir de sous-réseau. L'objet doit définir un hôte ou, pour un ensemble PAT, une plage. Le groupe (pour un ensemble PAT) peut inclure des hôtes et des plages.
- Source NAT statique ou NAT statique avec traduction de port :
  - L'objet ou le groupe peut contenir des hôtes, des plages ou des sous-réseaux.

- Le mappage statique est généralement de type un à un, de sorte que les adresses réelles sont en nombre égal aux adresses mappées. Vous pouvez, cependant, avoir des quantités différentes si vous le souhaitez.

- Source NAT d'identité :
  - Les objets réels et mappés doivent correspondre. Vous pouvez utiliser le même objet pour les deux ou créer des objets distincts qui contiennent les mêmes adresses IP.

- NAT statique de destination ou NAT statique avec traduction de port (la traduction de destination est toujours statique) :
  - Bien que la fonctionnalité principale de la NAT Twice soit l'inclusion de l'adresse IP de destination, l'adresse IP de destination est facultative. 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 configurer la NAT Twice sans adresse de destination pour profiter de certaines des autres qualités de la NAT Twice, y compris l'utilisation de groupes d'objets réseau pour les adresses réelles ou le tri manuel des règles. Pour en savoir plus, consultez Comparaison de NAT objet de réseau et Twice NAT (NAT en double), à la page 124.
  - Pour la NAT d'identité, les objets réels et mappés doivent correspondre. Vous pouvez utiliser le même objet pour les deux ou créer des objets distincts qui contiennent les mêmes adresses IP.
  - Le mappage statique est généralement de type un à un, de sorte que les adresses réelles sont en nombre égal aux adresses mappées. Vous pouvez, cependant, avoir des quantités différentes si vous le souhaitez.
  - Pour la NAT d'interface statique avec traduction de port (mode routé uniquement), vous pouvez spécifier le mot-clé **interface** au lieu d'un objet ou d'un groupe de réseau pour l'adresse mappée.
  - Vous pouvez utiliser un nom de domaine complet, tel que www.exemple.com, comme destination traduite (mappée). Pour de plus amples renseignements, consultez la section Lignes directrices relatives aux destinations FQDN, à la page 134.

Lignes directrices relatives aux destinations FQDN

Vous pouvez spécifier la destination traduite (mappée) dans une règle twice NAT (NAT en double) en utilisant un objet réseau de nom de domaine complet (FQDN) au lieu d'une adresse IP. Par exemple, vous pouvez créer une règle basée sur le trafic destiné au serveur Web www.exemple.com.

Lorsque vous utilisez un nom de domaine complet, le système obtient la résolution DNS et écrit la règle NAT en fonction de l'adresse renvoyée. Si vous utilisez plusieurs groupes de serveurs DNS, les domaines de filtre sont respectés et l'adresse est demandée au groupe approprié en fonction des filtres. Si plusieurs adresses sont obtenues à partir du serveur DNS, l'adresse utilisée est basée sur les éléments suivants :

- S'il existe une adresse sur le même sous-réseau que l'interface spécifiée, cette adresse est utilisée. S'il n'y en a pas sur le même sous-réseau, la première adresse renvoyée est utilisée.
- Le type d'adresse IP de la source traduite et celui de la destination traduite doivent correspondre. Par exemple, si l'adresse source traduite est au format IPv6, l'objet FQDN doit spécifier IPv6 comme type d'adresse. Si la source traduite est au format IPv4, l'objet FQDN doit spécifier IPv4 comme type d'adresse.

Vous ne pouvez pas inclure un objet FQDN dans un groupe de réseaux utilisé pour la destination NAT manuelle. Dans la NAT, un objet FQDN doit être utilisé seul, car un seul hôte de destination est logique pour ce type de règle NAT.

Si le nom de domaine complet ne peut pas être résolu en adresse IP, la règle n'est pas fonctionnelle tant qu'une résolution DNS n'est pas obtenue.

Lignes directrices NAT Twice pour les objets de service pour les ports réels et mappés

Vous pouvez éventuellement configurer des objets de service pour :

- **Port réel source (statique uniquement)** *ou* **port réel de destination**
- **Port mappé source (statique uniquement)** *ou* **port mappé de destination**

Tenez compte des lignes directrices suivantes lors de la création d'objets pour la NAT Twice.

- La NAT prend en charge uniquement les protocoles TCP, UDP et SCTP. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (soit TCP, soit UDP). Bien que vous puissiez configurer des règles de NAT Twice statiques avec des spécifications de port SCTP, cela n'est pas recommandé, car la topologie de la partie destination de l'association SCTP est inconnue. Utilisez plutôt la NAT d'objet statique pour SCTP.
- L'opérateur « non égal » (**neq**) n'est pas pris en charge.
- Pour la traduction de port d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.
- NAT dynamique source : la NAT dynamique source ne prend pas en charge la traduction de port.
- PAT dynamique source (Masquer) : la PAT dynamique source ne prend pas en charge la traduction de port.
- NAT statique source, NAT statique avec traduction de port ou NAT d'identité : un objet de service peut contenir à la fois un port source et un port de destination; toutefois, vous devez préciser *soit* le port source, *soit* le port de destination pour les deux objets de service. Vous ne devez spécifier *les deux*, ports source et de destination, que si votre application utilise un port source fixe (comme certains serveurs DNS) ; mais les ports sources fixes sont rares. Par exemple, si vous souhaitez traduire le port pour l'hôte source, configurez le service source.
- NAT statique de destination ou NAT statique avec traduction de port (la traduction de destination est toujours statique) : pour la NAT source non statique, vous pouvez effectuer une traduction de port uniquement sur la destination. Un objet de service peut contenir à la fois un port source et un port de destination, mais seul le port de destination est utilisé dans ce cas. Si vous spécifiez le port source, il sera ignoré.

Traduction d'adresses réseau dynamique

Les rubriques suivantes expliquent la NAT dynamique et comment la configurer.

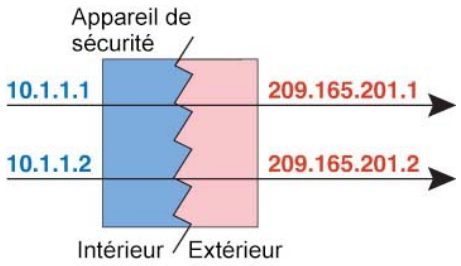
À propos de la NAT dynamique

La NAT dynamique traduit un groupe d'adresses réelles en un ensemble d'adresses mappées qui sont routables sur le réseau de destination. Le 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.

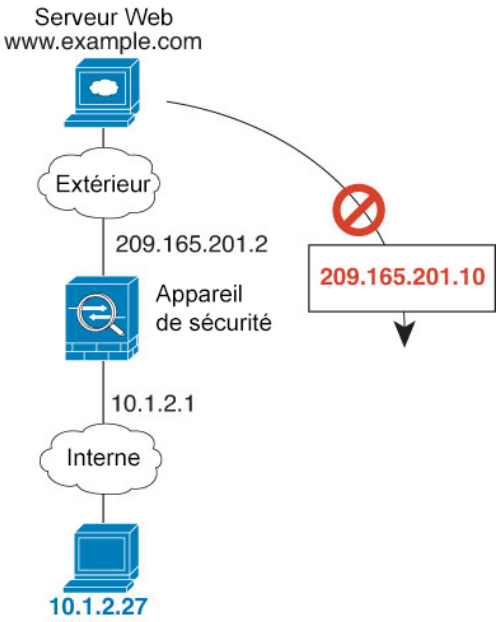
La figure suivante montre un scénario de NAT dynamique typique. Seuls les hôtes réels peuvent créer une session NAT, et le trafic qui répond est autorisé à revenir.

Illustration 8 : 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 9 : 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 sucrharger, 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 dynamique

Cette section décrit comment configurer la NAT d'objet réseau pour la NAT dynamique.

Procédure

Étape 1 Ajouter la NAT à un objet réseau nouveau ou existant :

- Pour ajouter un nouvel objet réseau, choisissez **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)**, puis cliquez sur **Add (Ajouter) > Add Network Object NAT Rule (Ajouter une règle NAT d'objet réseau)**.
- Pour ajouter la NAT à un objet réseau existant, choisissez **Configuration > Firewall (Pare-feu) > Objects (Objets) > Network Objects/Groups (Objets/groupes réseau)**, puis modifiez un objet réseau.

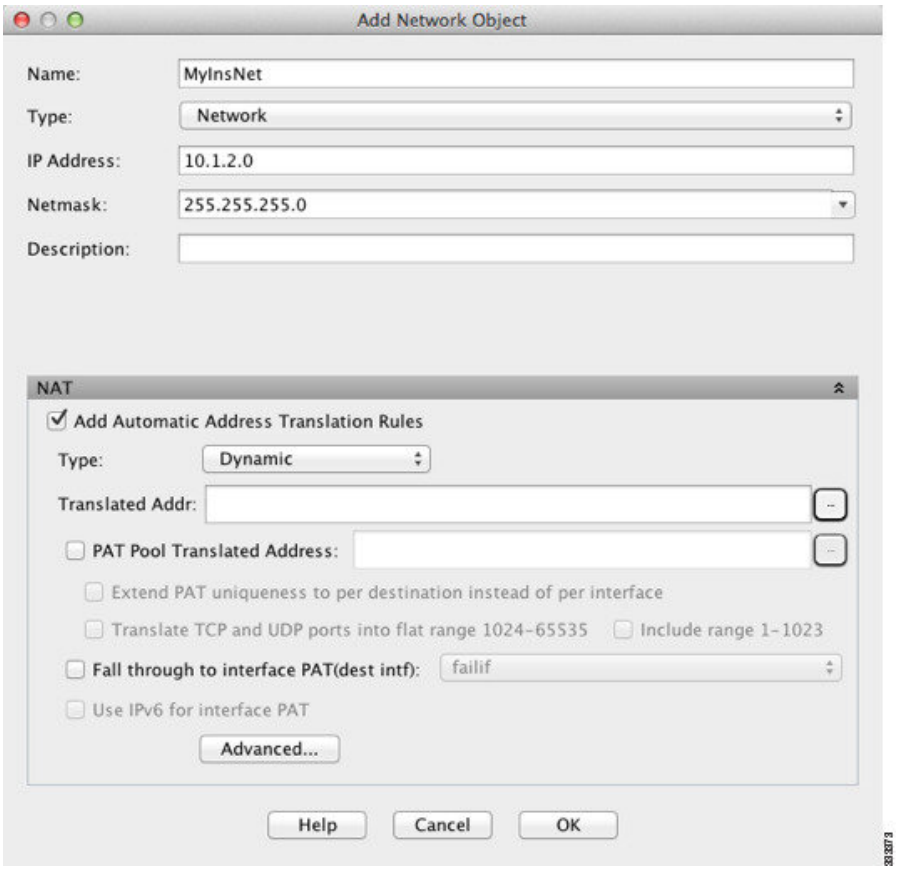
Étape 2 Renseignez les champs suivants :

a) **Name** : nom de l'objet. Utilisez les caractères a à z, A à Z, 0 à 9, un point, un tiret, une virgule ou un trait de soulignement. Le nom doit comporter au maximum 64 caractères.

b) **Type** : hôte, réseau ou plage.

c) **IP Addresses** (Adresses IP) : adresses IPv4 ou IPv6, une adresse unique pour un hôte, une adresse de début et de fin pour une plage et, pour le sous-réseau, soit une adresse réseau IPv4 et un masque (par exemple, 10.100.10.0 255.255.255.0), soit une adresse IPv6 et une longueur de préfixe (par exemple, 2001:DB8:0:CD30::/60).

Étape 3 Si la section NAT est masquée, cliquez sur **NAT** pour développer la section.



Étape 4 Cochez la case **Add Automatic Translation Rules** (Ajouter des règles de traduction automatique).

Étape 5 Dans la liste déroulante Type, choisissez **Dynamic** (Dynamique).

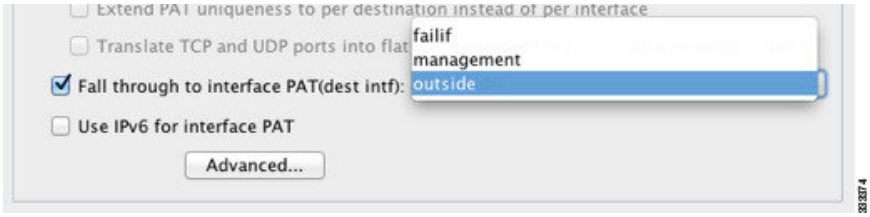
Étape 6 À droite du champ Translated Addr (Adresse traduite), cliquez sur le bouton de navigation et choisissez l'objet réseau ou le groupe d'objets réseau qui contient les adresses mappées.

Vous pouvez créer un nouvel objet si nécessaire.

L'objet ou le groupe ne peut pas contenir 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 objet réseau mappé contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP d'hôte sont utilisées comme PAT de secours. Si l'objet ne contient qu'une seule adresse d'hôte, il est utilisé pour la PAT.

Étape 7 (Facultatif, lorsque l'interface mappée n'est pas membre d'un groupe de ponts uniquement.) Pour utiliser l'adresse IP de l'interface comme méthode de sauvegarde lorsque les autres adresses mappées sont déjà allouées, cochez la case **Fall through to interface PAT (dest intf)** (Basculer vers la PAT d'interface [dest intf]) et choisissez l'interface dans la liste déroulante. Pour utiliser l'adresse IPv6 de l'interface, cochez également la case **Use IPv6 for interface PAT** (Utiliser IPv6 pour la PAT d'interface).



Étape 8 (Facultatif) Cliquez sur **Advanced** (Avancé), configurez les options suivantes dans la boîte de dialogue Advanced NAT Settings (Paramètres NAT avancés), puis cliquez sur **OK**.

- **Translate DNS replies for rule** (Traduire les réponses DNS pour la règle) : traduit l'adresse IP dans les réponses DNS. Assurez-vous que l'inspection DNS est activée (elle est activée par défaut). Consultez Réécriture des requêtes et des réponses DNS à l'aide de la NAT, à la page 244 pour de plus amples renseignements.
- (Requis pour les interfaces membres d'un groupe de ponts.) **Interface** : spécifie l'interface réelle (**Source**) et l'interface mappée (**Destination**) auxquelles cette règle NAT s'applique. Par défaut, la règle s'applique à toutes les interfaces, à l'exception des interfaces membres des groupes de ponts.

Étape 9 Cliquez sur **OK**, puis sur **Apply**(appliquer).

Configurer la NAT Twice dynamique

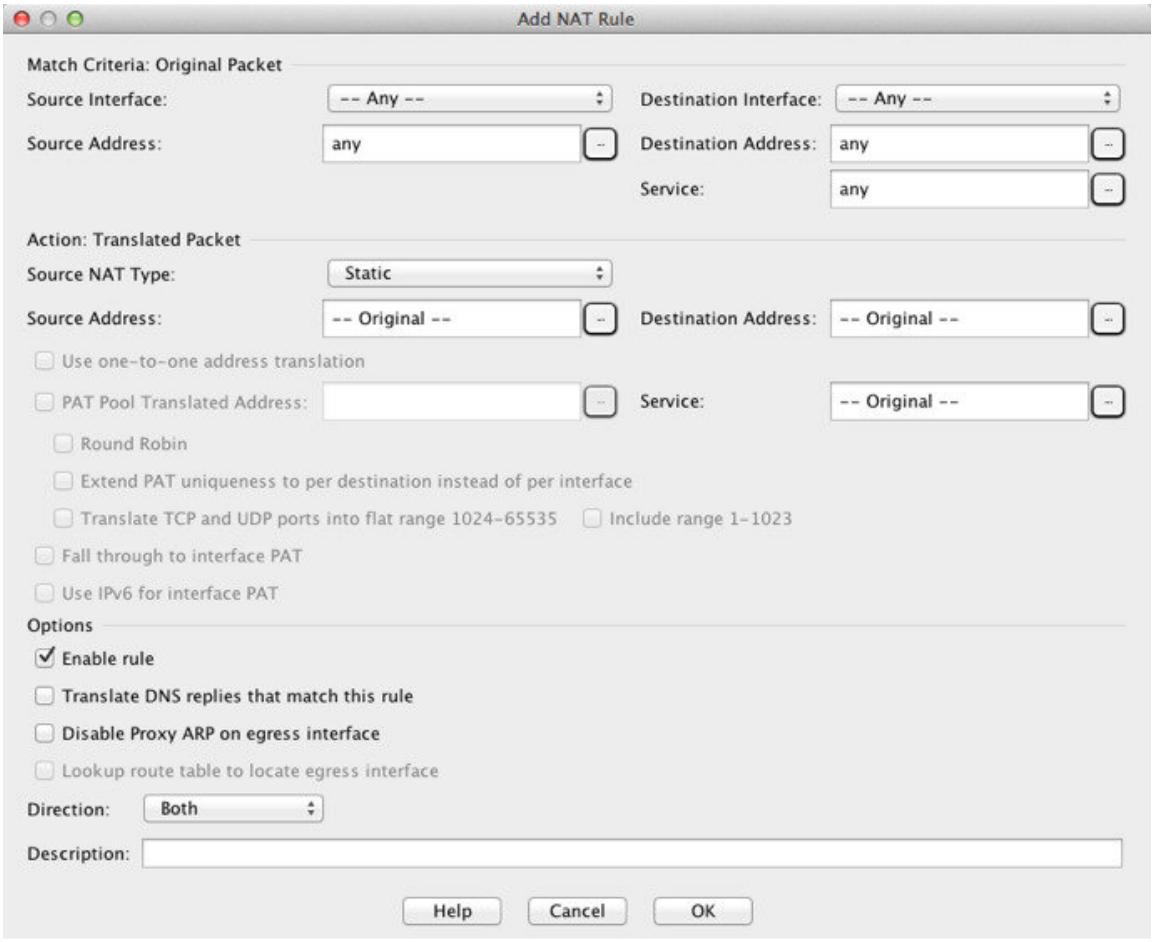
Cette section décrit comment configurer la NAT Twice pour la NAT dynamique.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall** > **NAT Rules** (Configuration > Pare-feu > Règles NAT), puis effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter), ou **Add > Add NAT Rule Before Network Object NAT Rules** (Ajouter > Ajouter une règle NAT avant les règles NAT de l'objet réseau).
- Cliquez sur **Add > Add NAT Rule After Network Object NAT Rules** (Ajouter > Ajouter une règle NAT après les règles NAT de l'objet réseau).
- Sélectionnez une règle de NAT Twice et cliquez sur **Edit** (Modifier).

La boîte de dialogue Add NAT Rule (ajouter une règle NAT) apparaît.

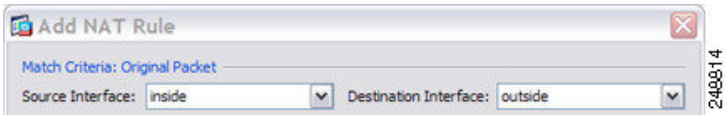


Étape 2 (Requis pour les interfaces membres d'un groupe de ponts.) Définissez les interfaces source et destination.

En mode routé, la valeur par défaut est toute interface pour la source et la destination. Vous pouvez sélectionner des interfaces spécifiques pour l'une des options ou les deux. Cependant, vous devez sélectionner l'interface lors de l'écriture d'une règle pour les interfaces des membres du groupe de ponts ; « any » n'inclut pas ces interfaces.

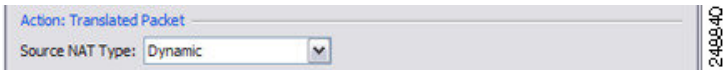
a) Dans la liste déroulante **Match Criteria: Original Packet (Critères de correspondance : paquet d'origine) > Source Interface** (Interface source) , choisissez l'interface source.

b) Dans la liste déroulante **Match Criteria: Original Packet > Destination Interface (Critères de correspondance : paquet d'origine > Interface de destination)**, choisissez l'interface de destination.

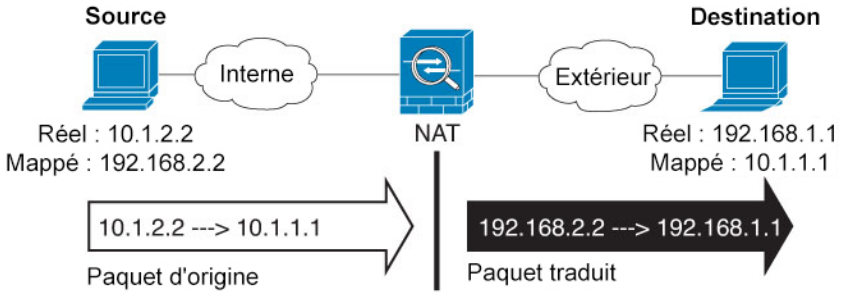


Étape 3 Choisissez **Dynamic** (Dynamique) dans la liste déroulante **Action: Translated Packet** > **Source NAT Type** (Action : paquet traduit > Type de NAT source).

Ce paramètre s'applique uniquement à l'adresse source; la traduction de destination est toujours statique.



Étape 4 Identifiez les adresses de paquets d'origine, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface source (*l'adresse source réelle* et *l'adresse de destination mappée*). Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.



a) Pour **les critères de correspondance : le paquet d'origine > l'adresse source**, cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse source d'origine. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. La valeur par défaut est **any**.

b) (Facultatif) Pour **les critères de correspondance : le paquet d'origine > l'adresse de destination**, cliquez sur le bouton de navigation et choisissez un objet réseau, un groupe ou une interface réseau existant, ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse de destination d'origine. Un groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type.

Bien que la fonctionnalité principale de la NAT Twice soit l'inclusion de l'adresse IP de destination, l'adresse IP de destination est facultative. 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 configurer la NAT Twice sans adresse de destination pour profiter de certaines des autres qualités de la NAT Twice, y compris l'utilisation de groupes d'objets réseau pour les adresses réelles ou le tri manuel des règles. Pour en savoir plus, consultez Comparaison de NAT objet de réseau et Twice NAT (NAT en double), à la page 124.

Pour la NAT d'interface statique avec traduction de port uniquement, choisissez une interface dans la boîte de dialogue Browse (Parcourir). Assurez-vous de également configurer une traduction de service. Pour cette option, vous devez configurer une interface spécifique pour l'interface source. Consultez NAT statique avec traduction de port, à la page 167 pour de plus amples renseignements.

Étape 5 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 (l'*adresse source mappée* et l'*adresse de destination réelle*). Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

a) Pour **Action : Paquet traduit > Adresse source**, cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse source traduite.

Pour la NAT dynamique, vous configurez généralement un groupe plus important d'adresses source à mapper à un groupe plus restreint.

Si un objet réseau mappé contient à la fois des plages et des adresses IP d'hôte, les plages sont utilisées pour la NAT dynamique, puis les adresses IP d'hôte sont utilisées comme repli PAT. Si l'objet ne contient qu'une seule adresse d'hôte, il est utilisé pour la PAT.

Remarque

L'objet ou le groupe ne peut pas contenir de sous-réseau.

b) Pour **l'action : Paquet traduit > Adresse de destination**, cliquez sur le bouton de navigation et choisissez un objet ou un groupe de réseau existant, ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse de destination traduite. Vous pouvez également utiliser un objet réseau FQDN pour l'adresse mappée de destination.

Pour la NAT d'identité pour l'adresse de destination, utilisez simplement le même objet ou groupe pour les adresses réelles et mappées.

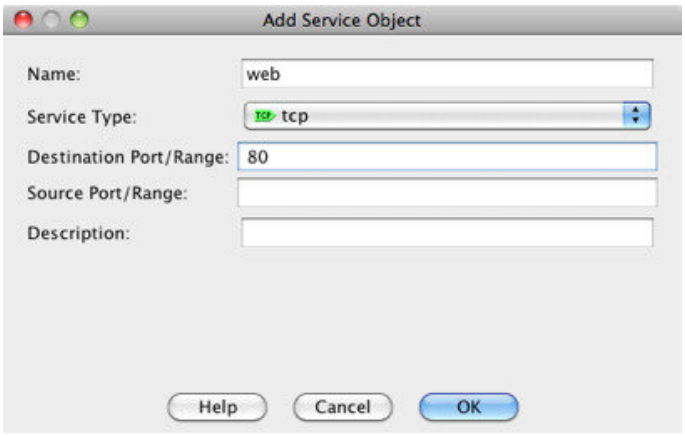
Si vous souhaitez traduire l'adresse de destination, le mappage statique est généralement un à un, de sorte que le nombre d'adresses réelles est égal au nombre d'adresses mappées. Vous pouvez, cependant, avoir des quantités différentes si vous le souhaitez. Pour en savoir plus, consultez NAT statique, à la page 166. Consultez Lignes directrices supplémentaires pour la NAT, à la page 129 pour en savoir plus sur les adresses IP mappées non autorisées.

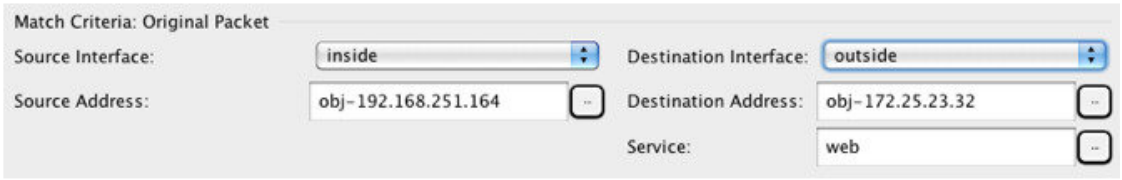
Étape 6 (Facultatif) Identifiez les ports de service de destination pour la traduction de service.

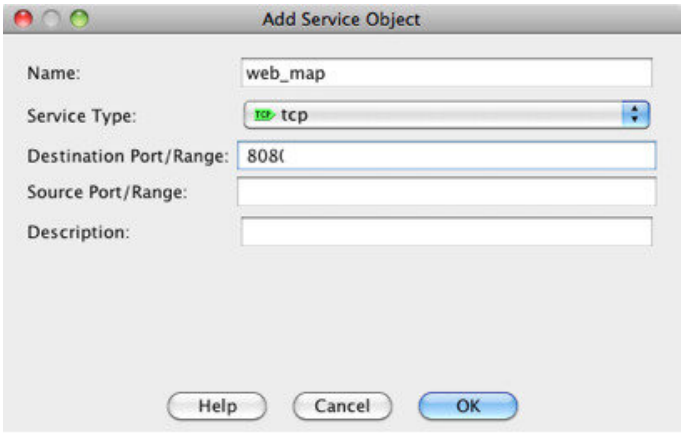
- Déterminez le port de paquet d'origine (le *port de destination mappé*). Pour **Match Criteria: Original Packet > Service** (Critères de correspondance : paquet d'origine > Service), cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie les ports TCP ou UDP, ou créez un nouvel objet dans la boîte de dialogue Browse Original Service (Parcourir le service d'origine).
- Déterminez le port de paquet traduit (le *port de destination réel*). Pour **Action: Translated Packet Service** (Action : service de paquet traduit), cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie les ports TCP ou UDP, ou créez un nouvel objet dans la boîte de dialogue Browse Translated Service (Parcourir le service traduit).

La NAT dynamique ne prend pas en charge la traduction de port. Cependant, comme la traduction de destination est toujours statique, vous pouvez effectuer la traduction de port pour le port de destination. Un objet de service peut contenir à la fois un port source et un port de destination, mais seul le port de destination est utilisé dans ce cas. Si vous spécifiez le port source, il sera ignoré. 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. L'opérateur « pas égal » (**!=**) n'est pas pris en charge.

Par exemple :



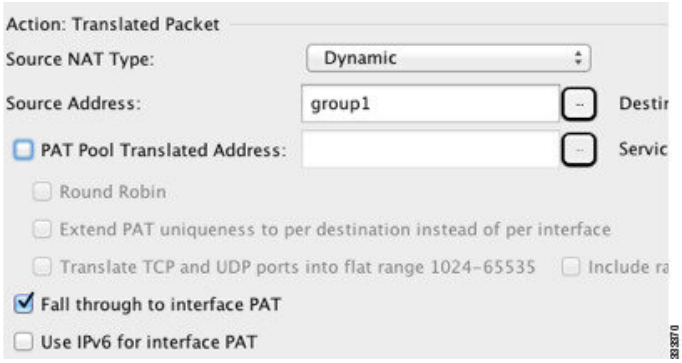




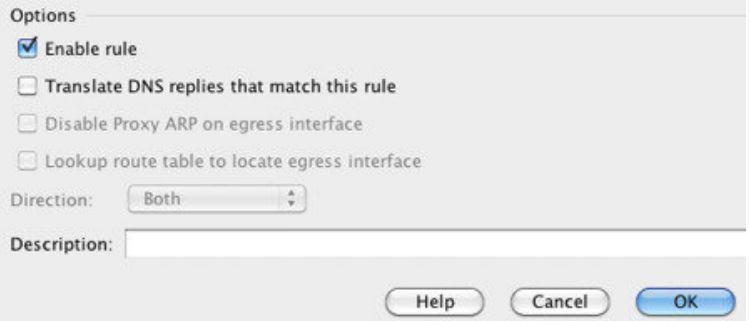


Étape 7 (Facultatif, lorsque l'interface mappée n'est pas membre d'un groupe de ponts uniquement.) Pour utiliser l'adresse IP de l'interface comme méthode de sauvegarde si les autres adresses source mappées sont déjà allouées, cochez la case **Fall through to interface PAT** (Basculer vers la PAT de l'interface). Pour utiliser l'adresse d'interface IPv6, cochez également la case **Use IPv6 for interface PAT** (Utiliser IPv6 pour la PAT de l'interface).

L'adresse IP de l'interface de destination est utilisée. Cette option est uniquement disponible si vous configurez une interface de destination spécifique.



Étape 8 (Facultatif) Configurez les options NAT dans la zone Options.



- **Enable rule** (Activer la règle) : active cette règle NAT. La règle est activée par défaut.
- (Pour une règle de source uniquement) **Translate DNS replies that match this rule** (Traduire les réponses DNS qui correspondent à cette règle) : réécrit l'enregistrement DNS A dans les réponses DNS. Assurez-vous que l'inspection DNS est activée (elle est activée par défaut). Vous ne pouvez pas configurer la modification DNS si vous configurez une adresse de destination. Consultez Réécriture des requêtes et des réponses DNS à l'aide de la NAT, à la page 244 pour de plus amples renseignements.
- **Description** : ajoute une description à la règle d'une longueur maximale de 200 caractères.

Étape 9 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

PAT dynamique

Les rubriques suivantes décrivent la PAT dynamique.

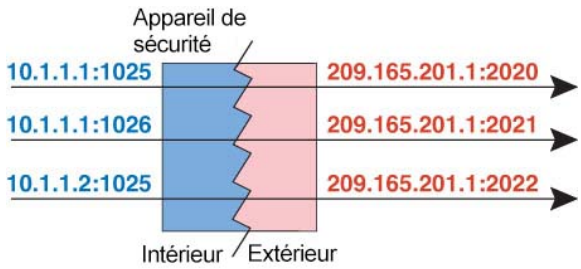
À propos de la PAT dynamique

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 10 : 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. Pour la PAT multisession, le délai d'expiration de la PAT est utilisé, soit 30 secondes par défaut. Pour les PAT par session, le xlate est immédiatement supprimé.



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 ASA comme adresse PAT.

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.

La PAT dynamique ne fonctionne pas avec certaines applications multimédias dont le flux de données est différent de celui du chemin de contrôle. Consultez Inspections par défaut et limites de la NAT, à la page 289 pour plus d'informations sur la prise en charge de NAT et PAT.

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. Vous pouvez configurer un pool d'adresses PAT et utiliser une attribution round-robin des adresses PAT pour atténuer cette situation.

Lignes directrices relatives aux objets de regroupement PAT

Lors de la création d'objets réseau pour un ensemble de PAT, suivez ces directives.

Pour un ensemble de PAT

- Les ports sont mappés à un port disponible dans la plage 1 024 à 65 535. Vous pouvez éventuellement inclure les ports réservés, ceux en dessous de 1024, pour rendre l'ensemble de la plage de ports disponible pour les traductions.

  Lors du fonctionnement dans une grappe, des blocs de 512 ports par adresse sont alloués aux membres de la grappe, et les mappages sont effectués dans ces blocs de ports. Si vous activez également l'allocation de blocs, les ports sont distribués en fonction de la taille de l'allocation de blocs, dont la taille par défaut est également de 512. Si vous modifiez la limite d'unité de grappe (la taille de la grappe), veillez à effacer les xlates ou à redémarrer les périphériques afin que les ensembles PAT puissent être réaffectés de manière appropriée aux unités de grappe.

- Si vous activez l'allocation de blocs pour un ensemble PAT, les blocs de ports sont alloués dans la plage 1 024 à 65535 uniquement. Ainsi, si une application nécessite un numéro de port faible (1 à 1023), elle peut ne pas fonctionner. Par exemple, une application demandant le port 22 (SSH) obtiendra un port mappé dans la plage 1 024 à 65535 et dans le bloc alloué à l'hôte.

- Si vous utilisez le même objet de pool PAT dans deux règles distinctes, veillez à spécifier les mêmes options pour chaque règle. Par exemple, si une règle spécifie une PAT étendue, l'autre règle doit également spécifier une PAT étendue.
- Si un hôte a une connexion existante, les connexions suivantes de cet hôte utilisent la même adresse IP PAT. Si aucun port n'est disponible, cela peut empêcher la connexion. Utilisez l'option tourniquet (round robin) pour éviter ce problème.
- Pour des performances optimales, limitez à 10 000 le nombre d'adresses IP dans un ensemble de PAT.

Pour PAT étendu pour un ensemble PAT

- De nombreuses inspections d'applications ne prennent pas en charge la PAT étendue. Consultez Inspections par défaut et limites de la NAT, à la page 289 pour obtenir une liste complète des inspections non prises en charge.
- Si vous activez la PAT étendue pour une règle PAT dynamique, vous ne pouvez pas utiliser une adresse dans l'ensemble PAT comme adresse PAT dans une NAT statique distincte avec règle de traduction de port. Par exemple, si l'ensemble PAT comprend l'adresse 10.1.1.1, vous ne pouvez pas créer de règle NAT statique avec traduction de port en utilisant 10.1.1.1 comme adresse PAT.
- Si vous utilisez un ensemble de PAT et que vous définissez une interface de secours, vous ne pouvez pas définir une PAT étendue.
- Pour les déploiements VoIP qui utilisent ICE ou TURN, n'utilisez pas la PAT étendue. ICE et TURN reposent sur la liaison PAT pour être la même pour toutes les destinations.
- Vous ne pouvez pas utiliser la PAT étendue sur les unités d'une grappe.
- La PAT étendue augmente l'utilisation de la mémoire sur le périphérique.

Pour un tourniquet (round robin) pour un ensemble de PAT

- Si un hôte a une connexion existante, les connexions suivantes de cet hôte utiliseront la même adresse IP PAT si des ports sont disponibles. Cependant, cette « permanence » ne survit pas à un basculement. Si le périphérique bascule, les connexions ultérieures à partir d'un hôte pourraient ne pas utiliser l'adresse IP initiale.
- La « permanence » d'adresse IP est également affectée si vous combinez des règles de pool PAT/round robin avec des règles PAT d'interface sur la même interface. Pour une interface donnée, choisissez un ensemble de PAT ou une PAT d'interface; ne créez pas de règles PAT concurrentes.
- La méthode « round robin », en particulier lorsqu'elle est combinée à une PAT étendue, peut consommer une grande quantité de mémoire. Étant donné que les ensembles NAT sont créés pour chaque protocole/adresse IP/plage de ports mappés, la répétition alternée entraîne la création d'un grand nombre d'ensembles NAT simultanés, qui utilisent de la mémoire. Une PAT étendue se traduit par un nombre encore plus important de pools NAT simultanés.

Configurer la PAT d'objet réseau dynamique (Masquer)

Cette section décrit comment configurer la NAT d'objet réseau pour la PAT dynamique (Masquer), qui utilise une adresse unique pour la traduction au lieu d'un ensemble de PAT.

Procédure

Étape 1 Ajouter la NAT à un objet réseau nouveau ou existant :

- Pour ajouter un nouvel objet réseau, choisissez **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)**, puis cliquez sur **Add (Ajouter) > Add Network Object NAT Rule (Ajouter une règle NAT d'objet réseau)**.
- Pour ajouter la NAT à un objet réseau existant, choisissez **Configuration > Firewall (Pare-feu) > Objects (Objets) > Network Objects/Groups (Objets/groupes réseau),** puis modifiez un objet réseau.

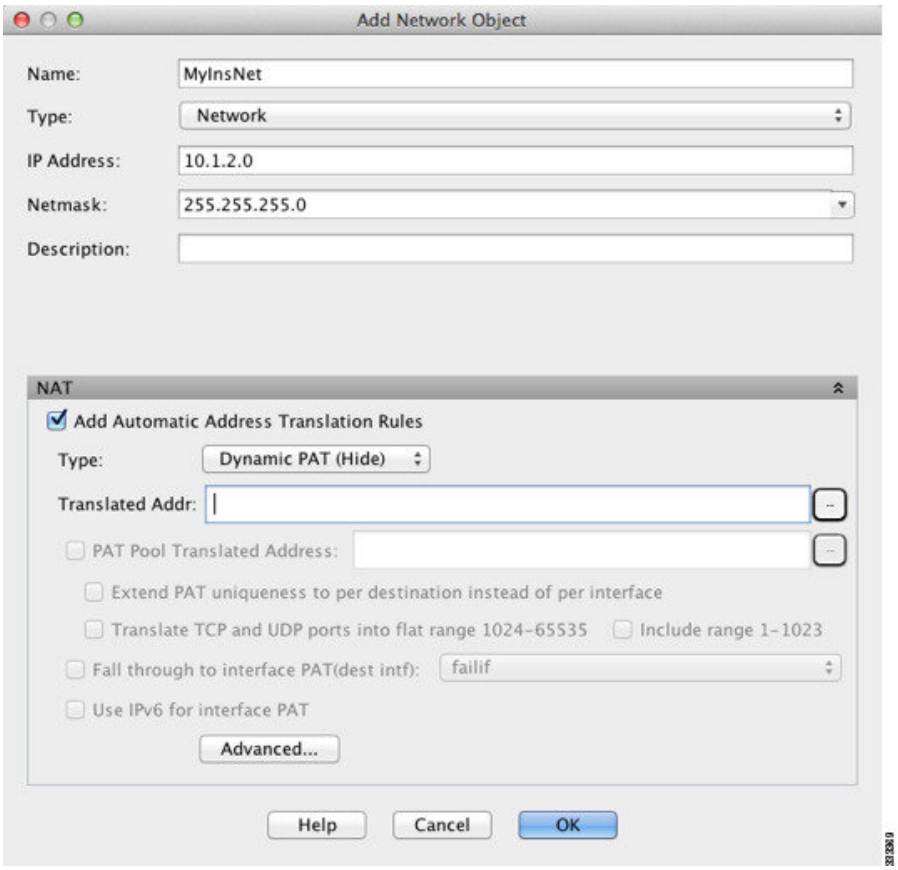
Étape 2 Pour un nouvel objet, renseignez les champs suivants :

a) **Name** : nom de l'objet. Utilisez les caractères a à z, A à Z, 0 à 9, un point, un tiret, une virgule ou un trait de soulignement. Le nom doit comporter au maximum 64 caractères.
b) **Type** : hôte, réseau ou plage.
c) **Adresses IP** : adresses IPv4 ou IPv6, une adresse unique pour un hôte, une adresse de début et de fin pour une plage et pour le sous-réseau, soit une adresse et un masque de réseau IPv4 (par exemple, 10.100.10.0 255.255.255.0) ou une adresse IPv6 et la longueur du préfixe (par exemple, 2001:DB8:0:CD30::/60).

Étape 3 Si la section NAT est masquée, cliquez sur **NAT** pour développer la section.

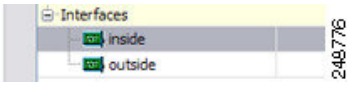
Étape 4 Cochez la case **Add Automatic Translation Rules** (Ajouter des règles de traduction automatique).

Étape 5 Dans la liste déroulante Type, choisissez **Dynamic PAT (Hide)** (PAT dynamique [Masquer]).



Étape 6 Précisez une adresse mappée unique. Dans le champ Adresse traduite, spécifiez l'adresse IP mappée en effectuant l'une des opérations suivantes :

- Tapez une adresse IP d'hôte.
- Cliquez sur le bouton de navigation et sélectionnez un objet réseau hôte (ou créez-en un nouveau).
- (Interfaces non membres d'un groupe de ponts uniquement.) Tapez un nom d'interface ou cliquez sur le bouton de navigation, puis choisissez une interface dans la boîte de dialogue Parcourir les adresses traduites.



Si vous spécifiez un nom d'interface, vous activez *l'interface PAT*, où l'adresse IP de l'interface spécifiée est utilisée comme adresse mappée. Pour utiliser l'adresse d'interface IPv6, vous devez également cocher la case **Use IPv6 for interface PAT** (Utiliser IPv6 pour la PAT de l'interface). Avec la PAT d'interface, la règle NAT s'applique uniquement à l'interface mappée spécifiée, qui ne peut pas être membre d'un groupe de ponts. (Si vous n'utilisez pas la PAT d'interface, la règle s'applique à toutes les interfaces par défaut.) Vous ne pouvez pas spécifier d'interface en mode transparent.

Étape 7 (Facultatif) Cliquez sur **Advanced** (Avancé), configurez les options suivantes dans la boîte de dialogue Advanced NAT Settings (Paramètres NAT avancés), puis cliquez sur **OK**.

- (Requis pour les interfaces membres d'un groupe de ponts.) **Interface** : spécifie l'interface réelle (**Source**) et l'interface mappée (**Destination**) auxquelles cette règle NAT s'applique. Par défaut, la règle s'applique à toutes les interfaces, à l'exception des interfaces membres des groupes de ponts.

Étape 8 Cliquez sur **OK**, puis sur **Apply**(appliquer).

Configurer la PAT d'objet réseau dynamique à l'aide d'un ensemble PAT

Cette section décrit comment configurer la NAT d'objet réseau pour la PAT dynamique à l'aide d'un pool PAT.

Procédure

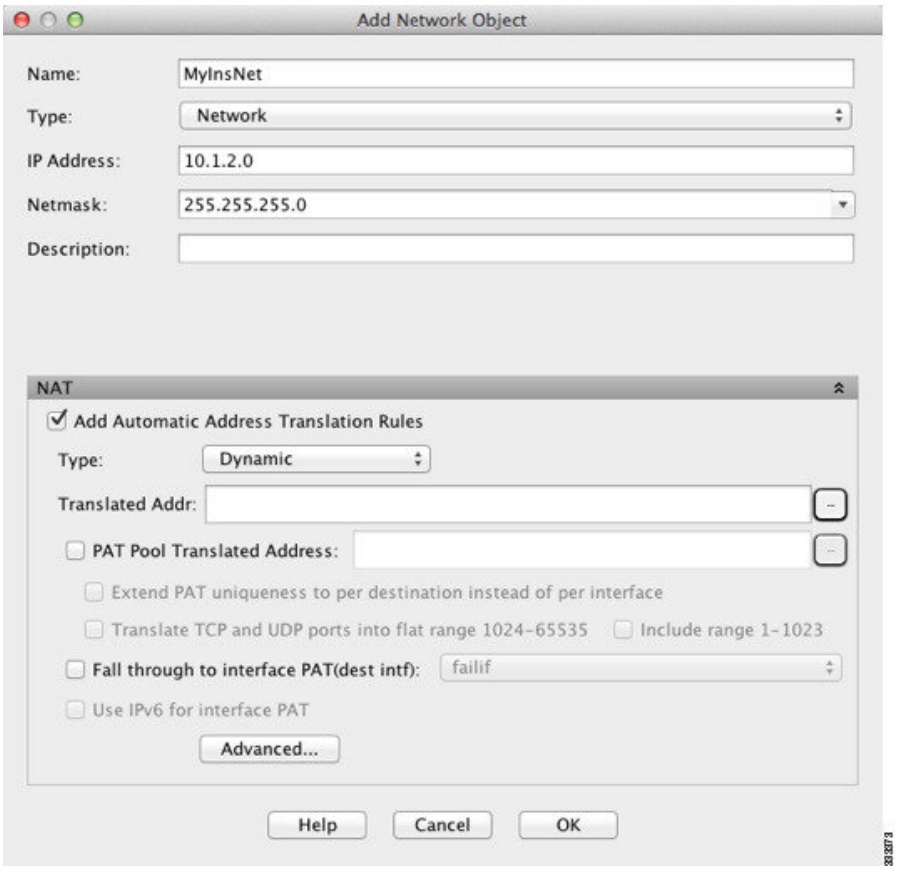
Étape 1 Ajouter la NAT à un objet réseau nouveau ou existant :

- Pour ajouter une nouvelle règle NAT d'objet réseau, choisissez **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)**, puis cliquez sur **Add (Ajouter)** > **Add Network Object NAT Rule (Ajouter une règle NAT d'objet réseau)**.
- Pour ajouter la NAT à un objet réseau existant, choisissez **Configuration** > **Firewall** > **(Pare-feu)** > **Objects** > **(Objets)** > **Network Objects/Groups** > **(Objets/groupes réseau),** puis modifiez un objet réseau.

Étape 2 Pour un nouvel objet, renseignez les champs suivants :

a) **Name** : nom de l'objet. Utilisez les caractères a à z, A à Z, 0 à 9, un point, un tiret, une virgule ou un trait de soulignement. Le nom doit comporter au maximum 64 caractères.
b) **Type** : hôte, réseau ou plage.
c) **IP Addresses** (Adresses IP) : adresses IPv4 ou IPv6, une adresse unique pour un hôte, une adresse de début et de fin pour une plage et, pour le sous-réseau, soit une adresse réseau IPv4 et un masque (par exemple, 10.100.10.0 255.255.255.0), soit une adresse IPv6 et une longueur de préfixe (par exemple, 2001:DB8:0:CD30::/60).

Étape 3 Si la section NAT est masquée, cliquez sur **NAT** pour développer la section.



Étape 4 Cochez la case **Add Automatic Translation Rules** (Ajouter des règles de traduction automatique).

Étape 5 Dans la liste déroulante Type, choisissez **Dynamic** (Dynamique) même si vous configurez la PAT dynamique avec un pool PAT.

Étape 6 Pour configurer le pool PAT :

a) Ne saisissez pas de valeur pour le champ de l'adresse traduite ; laissez-le vide.

b) Cochez la case **PAT Pool Translated Address** (Adresse traduite du pool PAT), puis cliquez sur le bouton de navigation et choisissez l'objet ou le groupe de réseau qui contient les adresses de pool PAT. Vous pouvez également créer un nouvel objet à partir de la boîte de dialogue Browse Translated PAT Pool Address (Parcourir les adresses de pool PAT traduites).

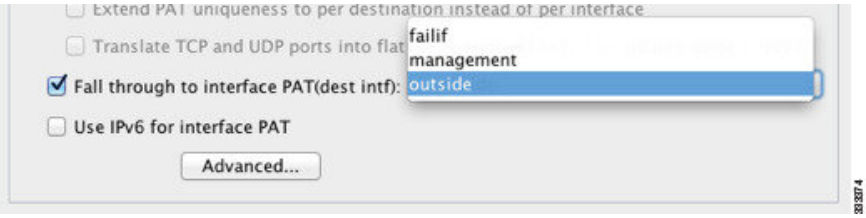
Remarque
L'objet ou le groupe de pool PAT ne peut pas contenir de sous-réseau. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses.



c) (Facultatif) Sélectionnez les options suivantes selon vos besoins :

- **Round Robin** : pour attribuer des adresses et ports de manière circulaire. Par défaut, sans l'affectation tourniquet (round robin), tous les ports pour une adresse PAT seront alloués avant que la prochaine adresse PAT soit utilisée. La méthode du tourniquet (round robin) attribue une adresse/un port à partir de chaque adresse PAT dans la réserve avant de réutiliser la première adresse, puis la deuxième adresse, etc.
- **Extend PAT uniqueness to per destination instead of per interface** (Étendre l'unicité de la PAT par destination plutôt que par interface) (8.4(3) et versions ultérieures, sans inclure 8.5(1) ni 8.6(1)) : pour utiliser la PAT étendue. La réserve PAT étendue fait appel à 65 535 ports par *service*, et non par adresse IP, en incluant l'adresse de destination et le port dans les informations de traduction. Normalement, le port et l'adresse de destination ne sont pas pris en compte lors de la création de traductions PAT. Cela limite donc vos options à 65 535 ports par adresse PAT. Par exemple, avec la réserve PAT étendue, vous pouvez créer une traduction de 10.1.1.1:1027 lorsque vous passez à 192.168.1.7:23 et une traduction de 10.1.1.1:1027 lorsque vous passez à 192.168.1.7:80.
- **Include Reserved Ports (1 to 1023)** (Inclure les ports réservés [1 à 1 023]) : comprend les ports réservés, de 1 à 1 023, dans la plage des ports disponibles pour la traduction d'adresses. Si vous ne spécifiez pas cette option, les adresses sont traduites uniquement vers des ports dans la plage de 1 024 à 65 535.
- **Enable Block Allocation** (Activer l'allocation de blocs) (9.5.1 et versions ultérieures) : active l'allocation de blocs de ports. Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois. Si vous attribuer un bloc de ports, les connexions suivantes de l'hôte utilisent de nouveaux ports sélectionnés au hasard dans le bloc. Au besoin, des blocs supplémentaires sont attribués si l'hôte dispose de connexions actives pour tous les ports du bloc d'origine. Les blocs de ports sont attribués uniquement dans la plage de 1024 à 65535. L'allocation de blocs de ports est compatible avec la méthode du tourniquet (round robin), mais vous ne pouvez pas l'utiliser avec le PAT étendu. Vous ne pouvez pas non plus utiliser l'option de rechange de PAT d'interface.

Étape 7 (Facultatif, lorsque l'interface mappée n'est pas membre d'un groupe de ponts uniquement.) Pour utiliser l'adresse IP de l'interface comme méthode de sauvegarde lorsque les autres adresses mappées sont déjà attribuées, cochez la case **Fall through to interface PAT** (Basculer vers la PAT d'interface) et choisissez l'interface dans la liste déroulante. Pour utiliser l'adresse IPv6 de l'interface, cochez également la case **Use IPv6 for interface PAT** (Utiliser IPv6 pour la PAT d'interface).



Étape 8 (Facultatif) Cliquez sur **Advanced** (Avancé), configurez les options suivantes dans la boîte de dialogue Advanced NAT Settings (Paramètres NAT avancés), puis cliquez sur **OK**.

- (Requis pour les interfaces membres d'un groupe de ponts.) **Interface** : spécifie l'interface réelle (**Source**) et l'interface mappée (**Destination**) auxquelles cette règle NAT s'applique. Par défaut, la règle s'applique à toutes les interfaces, à l'exception des interfaces membres des groupes de ponts.

Étape 9 Cliquez sur **OK**, puis sur **Apply**(appliquer).

Configurer la PAT Twice dynamique (Masquer)

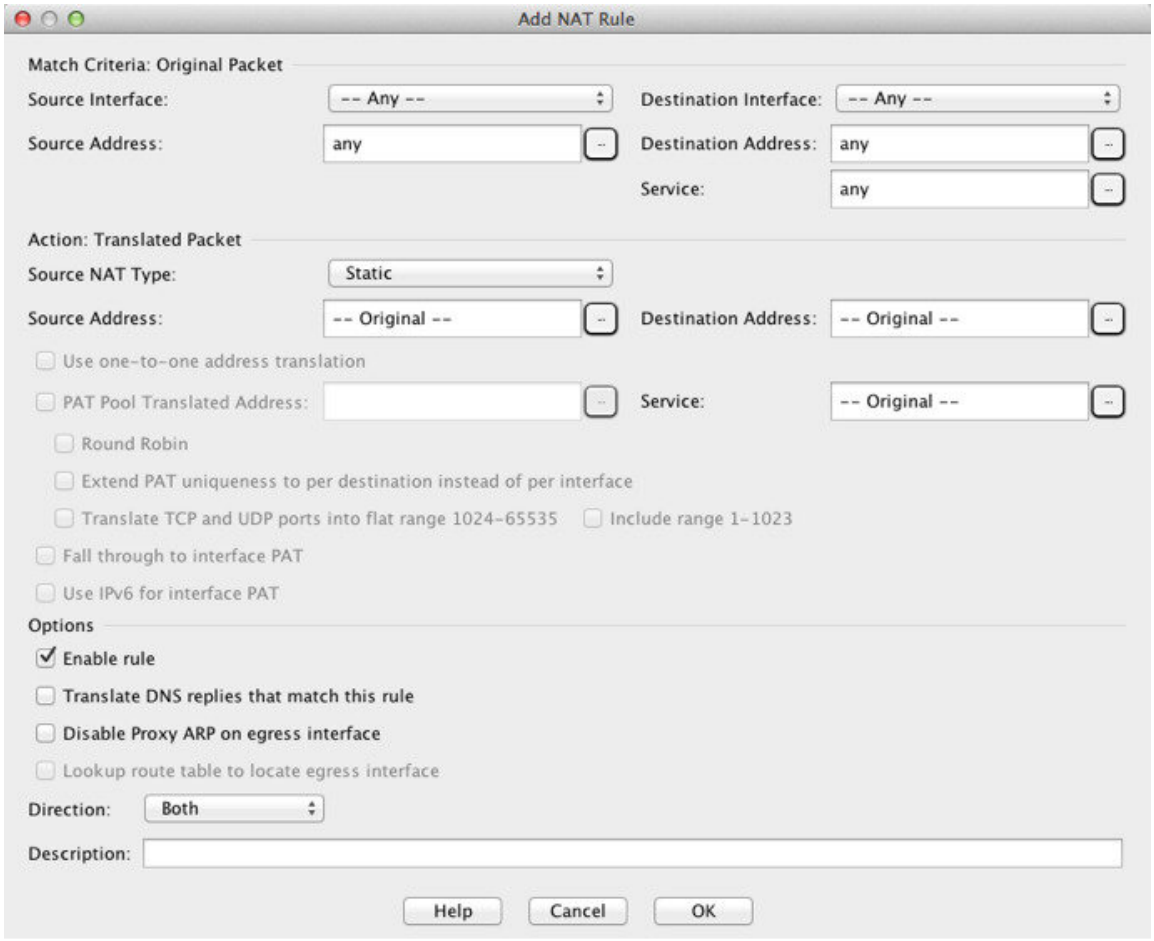
Cette section décrit comment configurer la NAT Twice pour la PAT dynamique (Masquer), qui utilise une adresse unique pour la traduction au lieu d'un pool PAT.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)** , puis effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter), ou **Add > Add NAT Rule Before Network Object NAT Rules** (Ajouter > Ajouter une règle NAT avant les règles NAT de l'objet réseau).
- Cliquez sur **Add > Add NAT Rule After Network Object NAT Rules** (Ajouter > Ajouter une règle NAT après les règles NAT de l'objet réseau).
- Sélectionnez une règle de NAT Twice et cliquez sur **Edit** (Modifier).

La boîte de dialogue Add NAT Rule (ajouter une règle NAT) apparaît.

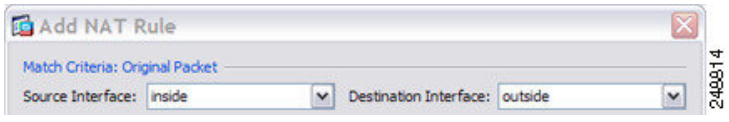


Étape 2 (Requis pour les interfaces membres d'un groupe de ponts.) Définissez les interfaces de source et de destination.

En mode routé, la valeur par défaut est n'importe quelle interface pour la source et la destination. Vous pouvez sélectionner des interfaces spécifiques pour l'une des options ou les deux. Cependant, vous devez sélectionner l'interface lors de l'écriture d'une règle pour les interfaces des membres du groupe de ponts ; « any » n'inclut pas ces interfaces.

a) Dans la liste déroulante **Match Criteria: Original Packet (Critères de correspondance : paquet d'origine) > Source Interface** (Interface source) , choisissez l'interface source.

b) Dans la liste déroulante **Match Criteria: Original Packet > Destination Interface** (Critères de correspondance : Paquet d'origine > Interface de destination), choisissez l'interface de destination.

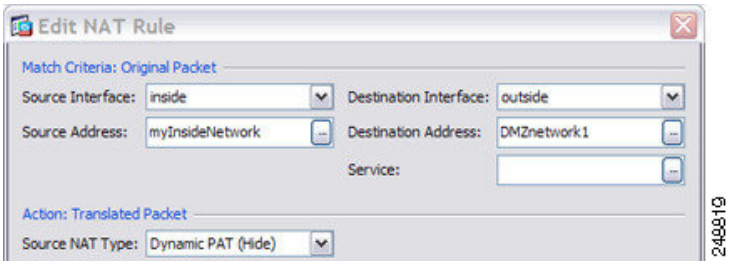


Étape 3 Choisissez **Dynamic PAT (Hide) (PAT dynamique [Masquer])** dans la liste déroulante **Action: Translated Packet** > **Source NAT Type** (Action : Paquet traduit > Type de NAT source).

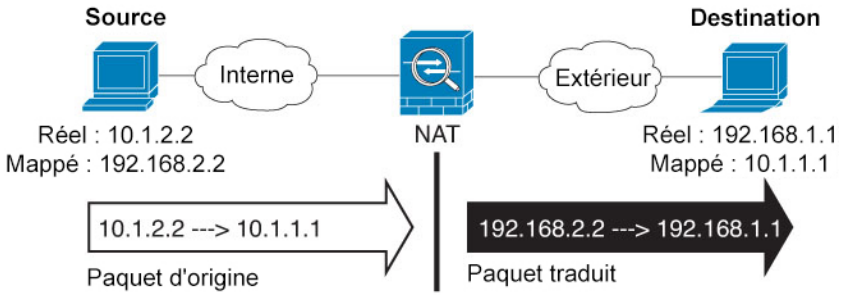
Ce paramètre s'applique uniquement à l'adresse source ; la traduction de destination est toujours statique.

Remarque

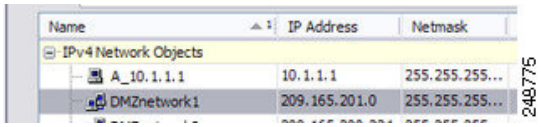
Pour configurer la PAT dynamique à l'aide d'un pool PAT, choisissez **Dynamic** (Dynamique) au lieu de Dynamic PAT (Hide) (PAT dynamique [Masquer]) ; consultez Configurer la PAT Twice dynamique à l'aide d'un ensemble PAT, à la page 157.



Étape 4 Identifiez les adresses de paquets d'origine, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface source (*l'adresse source réelle* et *l'adresse de destination mappée*). Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.



a) Pour **Match Criteria: Original Packet > Source Address** (Critères de correspondance : Paquet d'origine > Adresse source), cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant, ou créez un nouvel objet ou groupe dans la boîte de dialogue Browse Original Source Address (Parcourir l'adresse source d'origine). Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. La valeur par défaut est **any**.



b) (Facultatif) Pour **Match Criteria: Original Packet > Destination Address** (Critères de correspondance : Paquet d'origine > Adresse de destination), cliquez sur le bouton de navigation et choisissez un objet réseau, un groupe ou une interface existants (interfaces non membres de groupes de ponts uniquement), ou créez un nouvel objet ou groupe dans la boîte de dialogue Browse Original Destination Address (Parcourir l'adresse de destination d'origine). Un groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type.

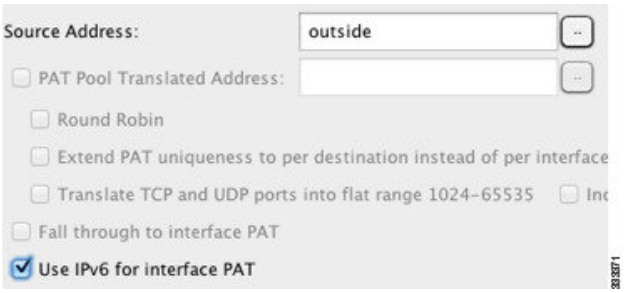
Bien que la fonctionnalité principale de la NAT Twice soit l'inclusion de l'adresse IP de destination, l'adresse IP de destination est facultative. Si vous précisez l'adresse de destination, vous pouvez configurer une traduction statique pour cette adresse ou simplement utiliser la NAT d'identité pour cette adresse. Vous pouvez configurer la NAT Twice sans adresse de destination pour profiter de certaines des autres qualités de la NAT Twice, y compris l'utilisation de groupes d'objets réseau pour les adresses réelles ou le tri manuel des règles. Pour en savoir plus, consultez Comparaison de NAT objet de réseau et Twice NAT (NAT en double), à la page 124.

Pour la NAT d'interface statique avec traduction de port uniquement, choisissez une interface dans la boîte de dialogue Browse (Parcourir). Assurez-vous de également configurer une traduction de service. Pour cette option, vous devez configurer une interface spécifique pour l'interface source. Consultez NAT statique avec traduction de port, à la page 167 pour de plus amples renseignements.

Étape 5 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 (l'*adresse source mappée* et l'*adresse de destination réelle*). Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

a) Pour **Action: Translated Packet > Source Address** (Action : Paquet traduit > Adresse source), cliquez sur le bouton de navigation et choisissez un objet réseau existant qui définit une adresse d'hôte, ou une interface, ou créez un nouvel objet dans la boîte de dialogue Browse Translated Source Address (Parcourir l'adresse source traduite). L'interface ne peut pas faire partie d'un groupe de pont.

Si vous souhaitez utiliser l'adresse IPv6 de l'interface, cochez la case **Use IPv6 for interface PAT** (Utiliser IPv6 pour la PAT d'interface).



b) (Facultatif) Pour **Action: Translated Packet > Destination Address** (Action : Paquet traduit > Adresse de destination), cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant, ou créez un nouvel objet ou groupe dans la boîte de dialogue Browse Translated Destination Address (Parcourir l'adresse de destination traduite). Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. Vous pouvez également utiliser un objet réseau FQDN pour l'adresse mappée de destination.

Pour la NAT d'identité pour l'adresse de destination, utilisez simplement le même objet ou groupe pour les adresses réelles et mappées.

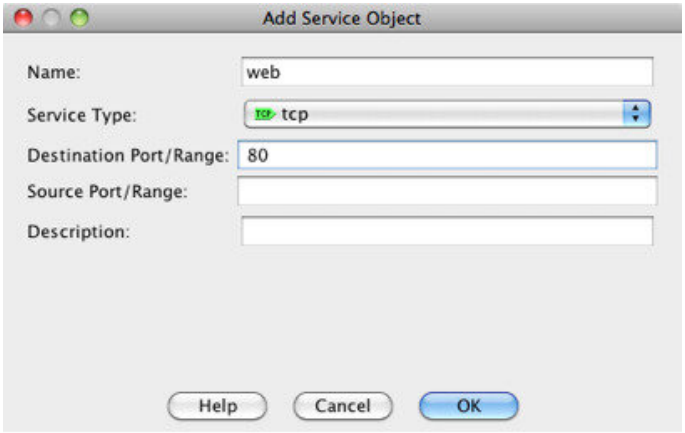
Si vous souhaitez traduire l'adresse de destination, le mappage statique est généralement un à un, de sorte que le nombre d'adresses réelles est égal au nombre d'adresses mappées. Vous pouvez, cependant, avoir des quantités différentes si vous le souhaitez. Pour en savoir plus, consultez NAT statique, à la page 166. Consultez Directives pour la NAT, à la page 127 pour en savoir plus sur les adresses IP mappées non autorisées.

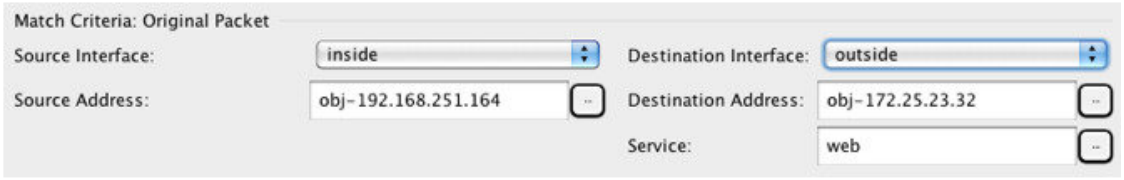
Étape 6 (Facultatif) Identifiez les ports de service de destination pour la traduction de service.

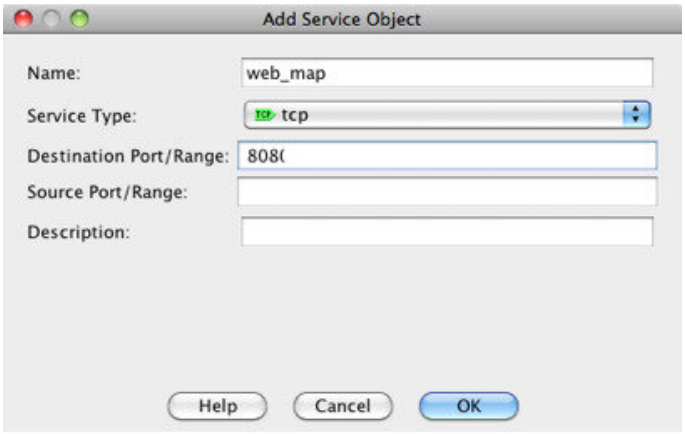
- Déterminez le port de paquet d'origine (le *port de destination mappé*). Pour **Match Criteria: Original Packet > Service** (Critères de correspondance : paquet d'origine > Service), cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie les ports TCP ou UDP, ou créez un nouvel objet dans la boîte de dialogue Browse Original Service (Parcourir le service d'origine).
- Déterminez le port de paquet traduit (le *port de destination réel*). Pour **Action: Translated Packet Service** (Action : service de paquet traduit), cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie les ports TCP ou UDP, ou créez un nouvel objet dans la boîte de dialogue Browse Translated Service (Parcourir le service traduit).

La NAT dynamique ne prend pas en charge la traduction de port. Cependant, comme la traduction de destination est toujours statique, vous pouvez effectuer la traduction de port pour le port de destination. Un objet de service peut contenir à la fois un port source et un port de destination, mais seul le port de destination est utilisé dans ce cas. Si vous spécifiez le port source, il sera ignoré. 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. L'opérateur « pas égal » (**!=**) n'est pas pris en charge.

Par exemple :

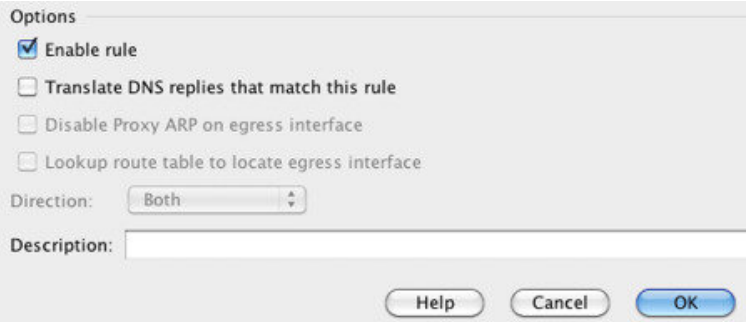








Étape 7 (Facultatif) Configurez les options de NAT dans la zone Options.



- **Enable rule** (Activer la règle) : active cette règle NAT. Cette fonction est activée par défaut.
- **Description** : ajoute une description à la règle d'une longueur maximale de 200 caractères.

Étape 8 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Configurer la PAT Twice dynamique à l'aide d'un ensemble PAT

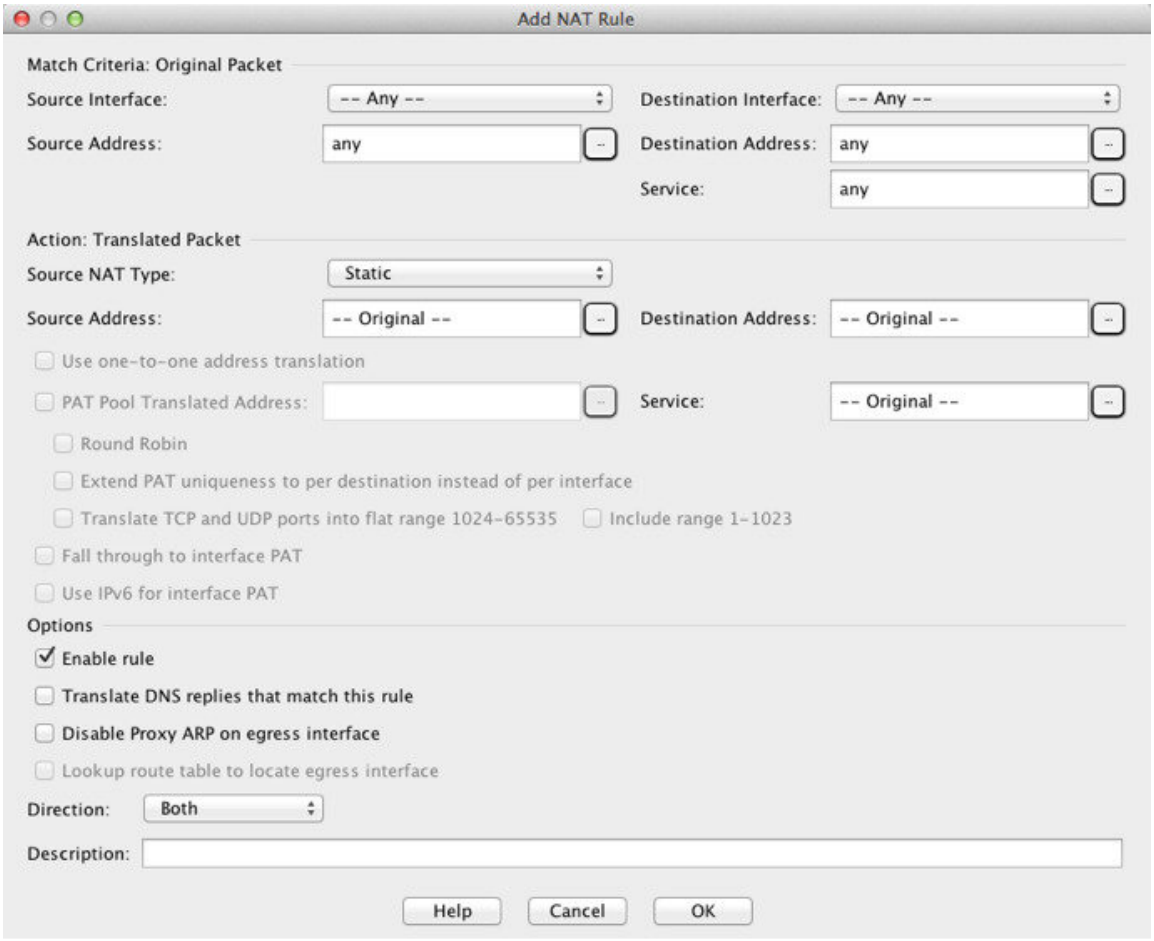
Cette section décrit comment configurer la NAT Twice pour la PAT dynamique à l'aide d'une réserve PAT.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)**, puis effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter), ou **Add** NAT **Rule Before Network Object NAT Rules** (Ajouter > Ajouter une règle NAT avant les règles NAT de l'objet réseau).
- Cliquez sur **Add** NAT **Rule After Network Object NAT Rules** (Ajouter > Ajouter une règle NAT après les règles NAT de l'objet réseau).
- Sélectionnez une règle de NAT Twice et cliquez sur **Edit** (Modifier).

La boîte de dialogue Add NAT Rule (ajouter une règle NAT) apparaît.



Étape 2 (Requis pour les interfaces membres d'un groupe de ponts.) Définissez les interfaces source et destination.

En mode routé, la valeur par défaut est toute interface pour la source et la destination. Vous pouvez sélectionner des interfaces spécifiques pour l'une des options ou les deux. Cependant, vous devez sélectionner l'interface lors de l'écriture d'une règle pour les interfaces des membres du groupe de ponts; « any » n'inclut pas ces interfaces.

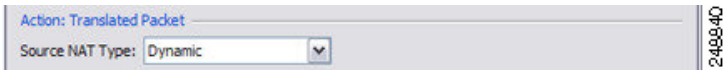
a) Dans la liste déroulante **Match Criteria: Original Packet** > **Source Interface** (Critères de correspondance : paquet d'origine > Interface source), choisissez l'interface source.

b) Dans la liste déroulante **Match Criteria: Original Packet** > **Destination Interface** (Critères de correspondance : paquet d'origine > Interface de destination), choisissez l'interface de destination.

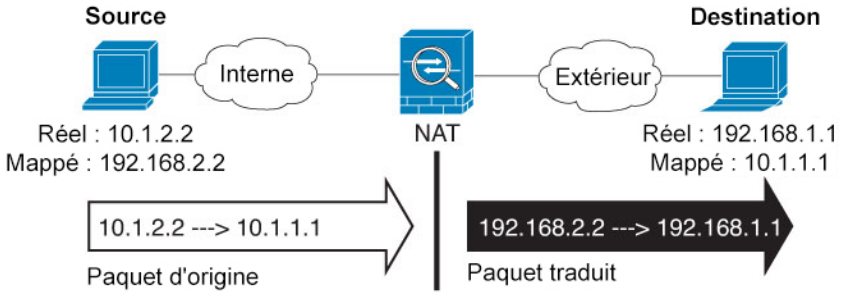


Étape 3 Choisissez **Dynamic** (Dynamique) dans la liste déroulante **Action: Translated Packet** > **Source NAT Type** (Action : paquet traduit > Type de NAT source).

Ce paramètre s'applique uniquement à l'adresse source; la traduction de destination est toujours statique.



Étape 4 Identifiez les adresses de paquets d'origine, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface source (*l'adresse source réelle* et *l'adresse de destination mappée*). Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.



a) Pour **Match Criteria: Original Packet** > **Source Address** (Critères de correspondance : paquet d'origine > Adresse source), cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant, ou créez un nouvel objet ou groupe dans la boîte de dialogue Browse Original Source Address (Parcourir l'adresse source d'origine). Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. La valeur par défaut est **any**.

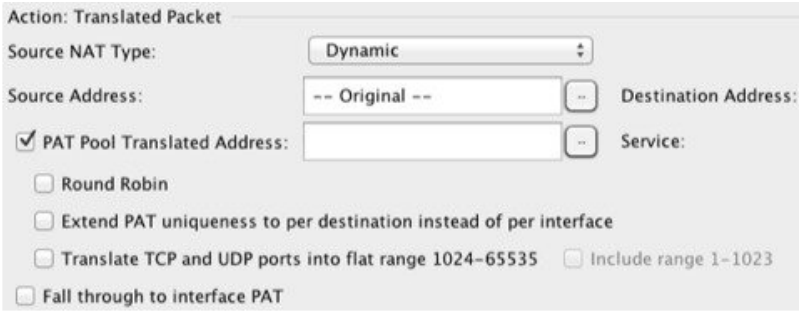
b) (Facultatif) Pour **Match Criteria: Original Packet** > **Destination Address** (Critères de correspondance : paquet d'origine > Adresse de destination), cliquez sur le bouton de navigation et choisissez un objet réseau, un groupe ou une interface existant (interfaces qui ne sont pas membres d'un groupe de ponts uniquement), ou créez un nouvel objet ou groupe dans la boîte de dialogue Browse Original Destination Address (Parcourir l'adresse de destination d'origine). Un groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type.

Bien que la fonctionnalité principale de la NAT Twice soit l'inclusion de l'adresse IP de destination, l'adresse IP de destination est facultative. 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 configurer la NAT Twice sans adresse de destination pour profiter de certaines des autres qualités de la NAT Twice, y compris l'utilisation de groupes d'objets réseau pour les adresses réelles ou le tri manuel des règles. Pour en savoir plus, consultez Comparaison de NAT objet de réseau et Twice NAT (NAT en double), à la page 124.

Pour la NAT d'interface statique avec traduction de port uniquement, choisissez une interface dans la boîte de dialogue Browse (Parcourir). Assurez-vous de également configurer une traduction de service. Pour cette option, vous devez configurer une interface spécifique pour l'interface source. Consultez NAT statique avec traduction de port, à la page 167 pour de plus amples renseignements.

Étape 5 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 (l'*adresse source mappée* et l'*adresse de destination réelle*). Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

a) Cochez la case **PAT Pool Translated Address** (Adresse traduite du pool PAT), puis cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant, ou créez un nouvel objet ou groupe dans la boîte de dialogue Browse Translated PAT Pool Address (Parcourir l'adresse du pool PAT traduit). **Remarque :** laissez le champ Adresse source vide.



Remarque
L'objet ou le groupe ne peut pas contenir de sous-réseau.

b) (Facultatif) Pour **Action: Translated Packet** > **Destination Address** (Action : paquet traduit > Adresse de destination), cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant, ou créez un nouvel objet ou groupe dans la boîte de dialogue Browse Translated Destination Address (Parcourir l'adresse de destination traduite).

Pour la NAT d'identité pour l'adresse de destination, utilisez simplement le même objet ou groupe pour les adresses réelles et mappées.

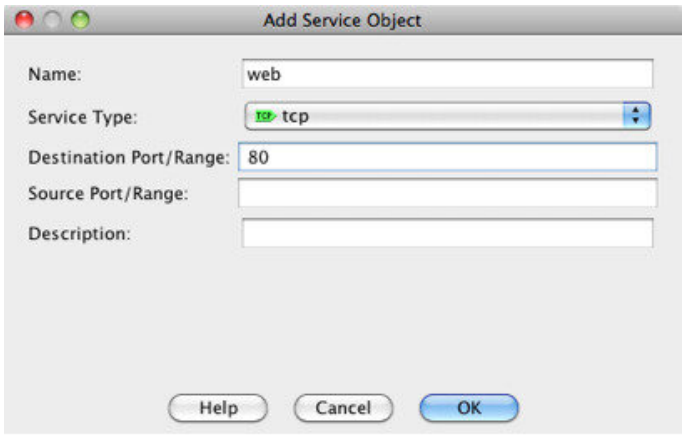
Si vous souhaitez traduire l'adresse de destination, le mappage statique est généralement un à un, de sorte que le nombre d'adresses réelles est égal au nombre d'adresses mappées. Vous pouvez, cependant, avoir des quantités différentes si vous le souhaitez. Pour en savoir plus, consultez NAT statique, à la page 166. Consultez Directives pour la NAT, à la page 127 pour en savoir plus sur les adresses IP mappées non autorisées.

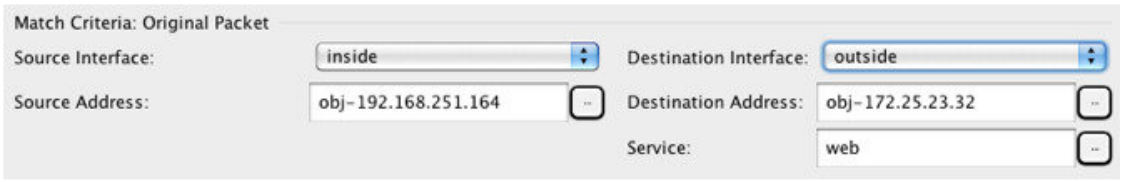
Étape 6 (Facultatif) Identifiez les ports de service de destination pour la traduction de service.

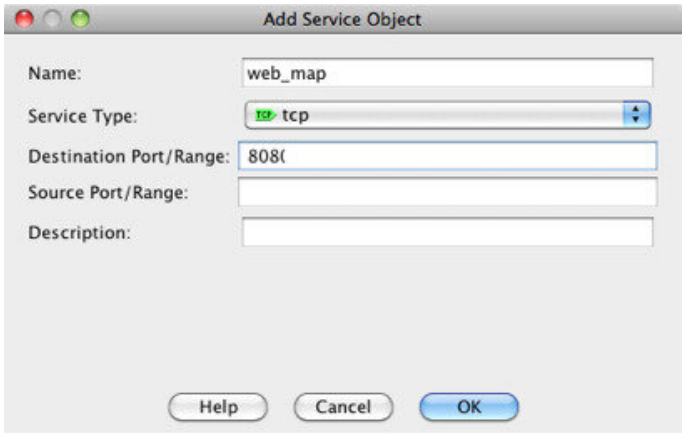
- Déterminez le port de paquet d'origine (le *port de destination mappé*). Pour **Match Criteria: Original Packet** > **Service** (Critères de correspondance : paquet d'origine > Service), cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie les ports TCP ou UDP, ou créez un nouvel objet dans la boîte de dialogue Browse Original Service (Parcourir le service d'origine).
- Déterminez le port de paquet traduit (le *port de destination réel*). Pour **Action: Translated Packet** > **Service** (Action : service de paquet traduit), cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie les ports TCP ou UDP, ou créez un nouvel objet dans la boîte de dialogue Browse Translated Service (Parcourir le service traduit).

La NAT dynamique ne prend pas en charge la traduction de port. Cependant, comme la traduction de destination est toujours statique, vous pouvez effectuer la traduction de port pour le port de destination. Un objet de service peut contenir à la fois un port source et un port de destination, mais seul le port de destination est utilisé dans ce cas. Si vous spécifiez le port source, il sera ignoré. 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. L'opérateur « pas égal » (**!=**) n'est pas pris en charge.

Par exemple :









Étape 7 (Facultatif) Pour un pool PAT, configurez les options suivantes selon les besoins :

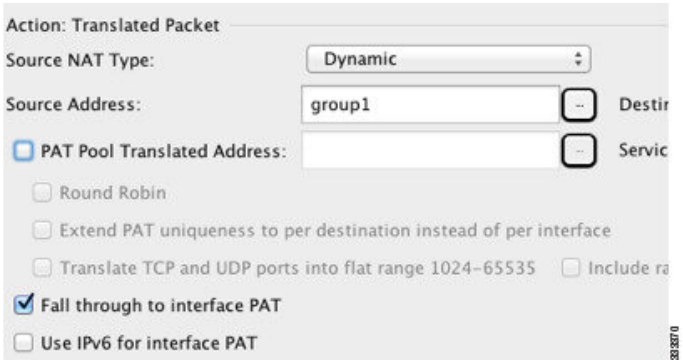
- **Round Robin** (Tourniquet) : permet d'attribuer des adresses/ports de manière circulaire. Par défaut, sans l'affectation tourniquet (round robin), tous les ports pour une adresse PAT seront alloués avant que la prochaine adresse PAT soit utilisée. La méthode du tourniquet (round robin) attribue une adresse/un port à partir de chaque adresse PAT dans la réserve avant de réutiliser la première adresse, puis la deuxième adresse, etc.
- **Extend PAT uniqueness to per destination instead of per interface** (Étendre l'unicité de la PAT par destination plutôt que par interface) (8.4(3) et versions ultérieures, sans inclure 8.5(1) ni 8.6(1)) : pour

utiliser la PAT étendue. La réserve PAT étendue fait appel à 65 535 ports par *service*, et non par adresse IP, en incluant l'adresse de destination et le port dans les informations de traduction. Normalement, le port et l'adresse de destination ne sont pas pris en compte lors de la création de traductions PAT. Cela limite donc vos options à 65 535 ports par adresse PAT. Par exemple, avec la réserve PAT étendue, vous pouvez créer une traduction de 10.1.1.1:1027 lorsque vous passez à 192.168.1.7:23 et une traduction de 10.1.1.1:1027 lorsque vous passez à 192.168.1.7:80.

- **Translate TCP or UDP ports into flat range (1024-65535)** (Traduire les ports TCP ou UDP en plage continue [1024 à 65 535]) (8.4(3) et versions ultérieures, sans inclure 8.5(1) ni 8.6(1)) : pour utiliser la plage de ports de 1 024 à 65 535 comme plage continue unique lors de l'allocation de ports. Lorsque vous choisissez le numéro de port mappé pour une traduction, l'ASA utilise le numéro du port source réel, s'il est disponible. Cependant, sans cette option, si le port réel n'est *pas* disponible, les ports mappés sont choisis par défaut dans la même plage de ports que le numéro de port réel : 1 à 511, 512 à 1023 ou 1024 à 65535. Pour éviter de manquer de ports dans les plages basses, configurez ce paramètre. Pour utiliser toute la plage de 1 à 65 535, cochez également la case **Include range 1 to 1 023** (Inclure la plage de 1 à 1 023).
- **Include Reserved Ports (1 to 1023)** (Inclure les ports réservés [1 à 1 023]) : comprend les ports réservés, de 1 à 1 023, dans la plage des ports disponibles pour la traduction d'adresses. Si vous ne spécifiez pas cette option, les adresses sont traduites uniquement vers des ports dans la plage de 1 024 à 65 535.
- **Enable Block Allocation** (Activer l'allocation de blocs) (9.5.1 et versions ultérieures) : active l'allocation de blocs de ports. Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois. Si vous attribuer un bloc de ports, les connexions suivantes de l'hôte utilisent de nouveaux ports sélectionnés au hasard dans le bloc. Au besoin, des blocs supplémentaires sont attribués si l'hôte dispose de connexions actives pour tous les ports du bloc d'origine. Les blocs de ports sont attribués uniquement dans la plage de 1024 à 65535. L'allocation de blocs de ports est compatible avec la méthode du tourniquet (round robin), mais vous ne pouvez pas l'utiliser avec le PAT étendu. Vous ne pouvez pas non plus utiliser l'option de rechange de PAT d'interface.

Étape 8 (Facultatif, lorsque l'interface mappée n'est pas membre d'un groupe de ponts uniquement.) Pour utiliser l'adresse IP de l'interface comme méthode de sauvegarde si les autres adresses source mappées sont déjà allouées, cochez la case **Fall through to interface PAT** (Basculer vers la PAT de l'interface). Pour utiliser l'adresse d'interface IPv6, cochez également la case **Use IPv6 for interface PAT** (Utiliser IPv6 pour la PAT de l'interface).

L'adresse IP de l'interface de destination est utilisée. Cette option est uniquement disponible si vous configurez une interface de destination spécifique.



Étape 9 (Facultatif) Configurez les options NAT dans la zone Options.



- **Enable rule** (Activer la règle) : active cette règle NAT. La règle est activée par défaut.
- **Description** : ajoute une description à la règle d'une longueur maximale de 200 caractères.

Étape 10 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Configurer PAT avec l'attribution de bloc de ports

Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois (Voir RFC 6888). Si vous attribuer un bloc de ports, les connexions suivantes de l'hôte utilisent de nouveaux ports sélectionnés au hasard dans le bloc. Au besoin, des blocs supplémentaires sont attribués si l'hôte dispose de connexions actives pour tous les ports du bloc d'origine. Les blocs sont libérés lorsque le dernier xlate qui utilise un port dans le bloc est supprimé.

La réduction de la journalisation est la principale raison de l'attribution de blocs de ports. L'attribution du bloc de ports est journalisée, les connexions sont journalisées, mais les xlates créés dans le bloc de ports ne sont pas journalisés. En revanche, cela rend l'analyse du journal plus difficile.

Les blocs de ports sont attribués uniquement dans la plage de 1024 à 65535. Il existe des blocs distincts pour les connexions TCP, UDP et ICMP, et ces blocs peuvent se chevaucher. Ainsi, si une application nécessite un numéro de port faible (1 à 1023), elle peut ne pas fonctionner. Par exemple, une application demandant le port 22 (SSH) obtiendra un port mappé dans la plage 1 024 à 65535 et dans le bloc alloué à l'hôte. Vous pouvez créer une règle NAT distincte qui n'utilise pas l'allocation de bloc pour les applications qui utilisent des numéros de port faibles; pour les NAT doubles, assurez-vous que la règle est placée avant la règle d'attribution Block (blocage).

Avant de commencer

Notes sur l'utilisation des règles NAT :

- Vous pouvez inclure l'option **Round Robin** (Round-robin), mais vous ne pouvez pas inclure les options permettant d'étendre l'unicité PAT, ou de basculer vers la PAT d'interface. D'autres informations sur le port et l'adresse de source ou de destination sont également autorisées.
- Comme pour toutes les modifications de NAT, si vous remplacez une règle existante, vous devez effacer les xlates liés à la règle remplacée pour que la nouvelle règle prenne effet. Vous pouvez les effacer explicitement ou simplement attendre qu'ils expirent. Cependant, lorsque vous fonctionnez dans une grappe, vous devez recharger la grappe pour que les unités puissent distribuer correctement les blocs.

Remarque Si vous basculez entre une PAT standard et une règle PAT d'attribution de blocs, pour la NAT d'objet, vous devez d'abord supprimer la règle, puis effacer les xlates. Vous pouvez ensuite créer la nouvelle règle NAT d'objet. Sinon, vous verrez des abandons pat-port-block-state-mismatch dans la sortie **show asp drop**.

- Pour un groupement (pool) PAT donné, vous devez préciser (ou ne pas préciser) l'allocation de bloc pour toutes les règles qui utilisent le groupement. Vous ne pouvez pas allouer de blocs dans une règle et pas dans une autre. Les groupements de PAT qui se chevauchent ne peuvent pas non plus combiner des paramètres d'allocation de bloc. Vous ne pouvez pas non plus superposer la NAT statique avec des règles de traduction de port avec le groupement.

Procédure

Étape 1 Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **PAT Port Block Allocation (Allocation de blocs de ports PAT)** et configurez les paramètres suivants :

- **Size of the block** (Taille du bloc) : nombre de ports dans chaque bloc. La plage est de 32 à 4096. La valeur par défaut est 512.

  Si vous n'utilisez pas la valeur par défaut, assurez-vous que la taille que vous choisissez est divisée de manière égale en 64 512 (le nombre de ports dans la plage 1024-65535). Sinon, certains ports ne pourront pas être utilisés. Par exemple, si vous spécifiez 100, il y aura 12 ports inutilisés.

- **Maximum block allocation per host** (Allocation maximale de blocs par hôte) : nombre maximal de blocs pouvant être alloués par hôte. La limite s'applique par protocole. Une limite de 4 signifie donc tout au plus 4 blocs UDP, 4 blocs TCP et 4 blocs ICMP par hôte. La plage est de 1 à 8, la valeur par défaut est 4.

- **PBA Interim Logging** (Journalisation intermédiaire PBA) : si vous saisissez une valeur, le système active la journalisation intermédiaire. Par défaut, le système génère des messages syslog lors de la création et de la suppression d'un bloc de port. Si vous activez la journalisation provisoire, le système génère le message suivant à l'intervalle que vous spécifiez. Les messages font état de tous les blocages de ports actifs à ce moment-là, y compris le protocole (ICMP, TCP, UDP), l'interface source et de destination, l'adresse IP et le blocage de ports. Vous pouvez spécifier un intervalle de 21 600 à 604 800 secondes (de 6 heures à 7 jours).

  %ASA-6-305017: Pba-interim-logging: Active *protocol* block of ports for translation from *real_interface*:*real_host_ip* to *mapped_interface*:*mapped_ip_address*/*start_port_num-end_port_num*

Étape 2 Ajoutez des règles NAT qui utilisent l'allocation de bloc de ports de groupement (pool) PAT.

a) Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)**.
b) Ajoutez ou modifiez une règle NAT d'objet ou de NAT Twice.
c) Configurez au moins les options suivantes :

- (NAT Twice.) Sélectionnez l'objet qui définit l'adresse source dans **Original Packet (Paquet d'origine)** > **Source Address (Adresse source)**.

- **Type** = **Dynamic** (dynamique).

- **PAT Pool Translated Address** (Adresse traduite du pool PAT). Sélectionnez un objet réseau qui définit le réseau de pool PAT.
- **Enable Block Allocation** (Activer l'allocation de blocs).

d) Cliquez sur **OK**.

Configurer la PAT par session ou la PAT multi-session (version 9.0(1) et versions ultérieures)

Par défaut, tout le trafic PAT TCP et tout le trafic DNS UDP utilisent une PAT par session. Pour utiliser la PAT multi-session pour le trafic, vous pouvez configurer des règles PAT par session : une règle d'autorisation utilise la PAT par session, et une règle de refus utilise la PAT multi-session.

La PAT par session améliore l'évolutivité de PAT et, pour la mise en grappe, permet à chaque nœud de données de posséder des connexions PAT; en revanche, les connexions PAT multi-sessions doivent être transférées au nœud de contrôle et détenues par celui-ci. À la fin d'une session PAT par session, l'ASA envoie une réinitialisation et supprime immédiatement le xlate. Cette réinitialisation force le nœud terminal à libérer immédiatement la connexion, évitant l'état TIME_WAIT. La PAT multi-session, en revanche, utilise le délai d'expiration PAT, par défaut de 30 secondes.

Pour le trafic « hit-and-run », comme HTTP ou HTTPS, la PAT par session peut augmenter considérablement le débit de connexion pris en charge par une adresse. Sans la PAT par session, le débit de connexion maximal pour une adresse pour un protocole IP est d'environ 2 000 par seconde. Avec la PAT par session, le débit de connexion pour une adresse pour un protocole IP est de 65 535/*average-lifetime*.

Pour le trafic qui peut bénéficier de la PAT multi-session, comme H.323, SIP ou Skinny, vous pouvez désactiver la PAT par session en créant une règle de refus par session. Toutefois, si vous souhaitez également utiliser la PAT par session pour les ports UDP utilisés par ces protocoles, vous devez créer les règles d'autorisation pour ceux-ci.

Avant de commencer

Par défaut, les règles suivantes sont installées :

- Autoriser le protocole TCP depuis n'importe quelle adresse (IPv4 et IPv6) vers n'importe quelle adresse (IPv4 et IPv6).
- Autoriser le protocole UDP depuis n'importe quelle adresse (IPv4 et IPv6) vers le port de domaine.

Ces règles ne s'affichent pas dans le tableau.

Vous ne pouvez pas supprimer ces règles, et elles existent toujours après toute règle créée manuellement. Comme les règles sont évaluées dans l'ordre, vous pouvez remplacer les règles par défaut. Par exemple, pour annuler complètement ces règles, vous pouvez ajouter les éléments suivants :

- Refuser le protocole TCP depuis n'importe quelle adresse (IPv4 et IPv6) vers n'importe quelle adresse (IPv4 et IPv6).
- Refuser le protocole UDP depuis n'importe quelle adresse (IPv4 et IPv6) vers le port de domaine.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Per-Session NAT Rules (Règles NAT par session)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Choisissez **Add (Ajouter) > Add Per-Session NAT Rule (Ajouter une règle NAT par session)**.
- Sélectionnez une règle et cliquez sur **Edit** (Modifier).

Étape 3 Configurez la règle :

- **Action** : cliquez sur **Permit** (Autoriser) ou **Deny** (Refuser). Une règle d'autorisation utilise la PAT par session ; une règle de refus utilise la PAT multi-session.
- Source : spécifiez l'adresse source en tapant une adresse ou en cliquant sur le bouton **...** pour choisir un objet. Pour le service, sélectionnez UDP ou TCP. Vous pouvez éventuellement préciser un port source, bien que, normalement, vous ne précisiez que le port de destination. Saisissez UDP/*port* ou TCP/*port*, ou cliquez sur le bouton**...** pour sélectionner une valeur commune ou un objet.
- Destination : spécifiez l'adresse de destination, soit en saisissant une adresse, soit en cliquant sur le bouton **...** pour choisir un objet. Pour le service, sélectionnez UDP ou TCP; il doit correspondre au service source. Vous pouvez éventuellement préciser un port de destination. Saisissez UDP/*port* ou TCP/*port*, ou cliquez sur le bouton**...** pour sélectionner une valeur commune ou un objet. Vous pouvez utiliser les opérateurs != (non égal à), > (supérieur à), < (inférieur à) ou spécifier une plage à l'aide d'un tiret, par exemple, 100-200.

Étape 4 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

NAT statique

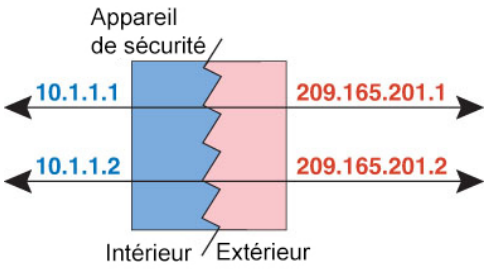
Les rubriques suivantes expliquent la NAT statique et comment la mettre en œuvre.

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 11 : NAT statique



Remarque Vous pouvez désactiver la bidirectionnalité si vous le souhaitez.

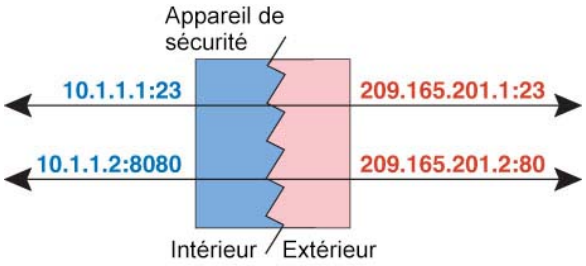
NAT statique avec traduction de port

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 12 : 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 twice NAT (NAT en double), 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). Pour plus de détails sur la façon de configurer cet exemple, consultez Adresse unique pour FTP, HTTP et SMTP (NAT statique avec traduction de port), à la page 204.

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

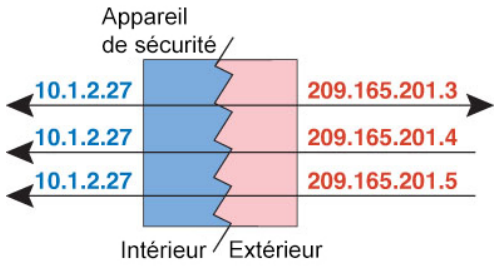
Vous pouvez configurer la NAT statique pour mapper une adresse réelle avec une combinaison adresse d'interface/port. Par exemple, si vous souhaitez rediriger l'accès Telnet pour l'interface externe du périphérique vers un hôte interne, vous pouvez mapper l'adresse IP/le port 23 de l'hôte interne avec 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-à-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.

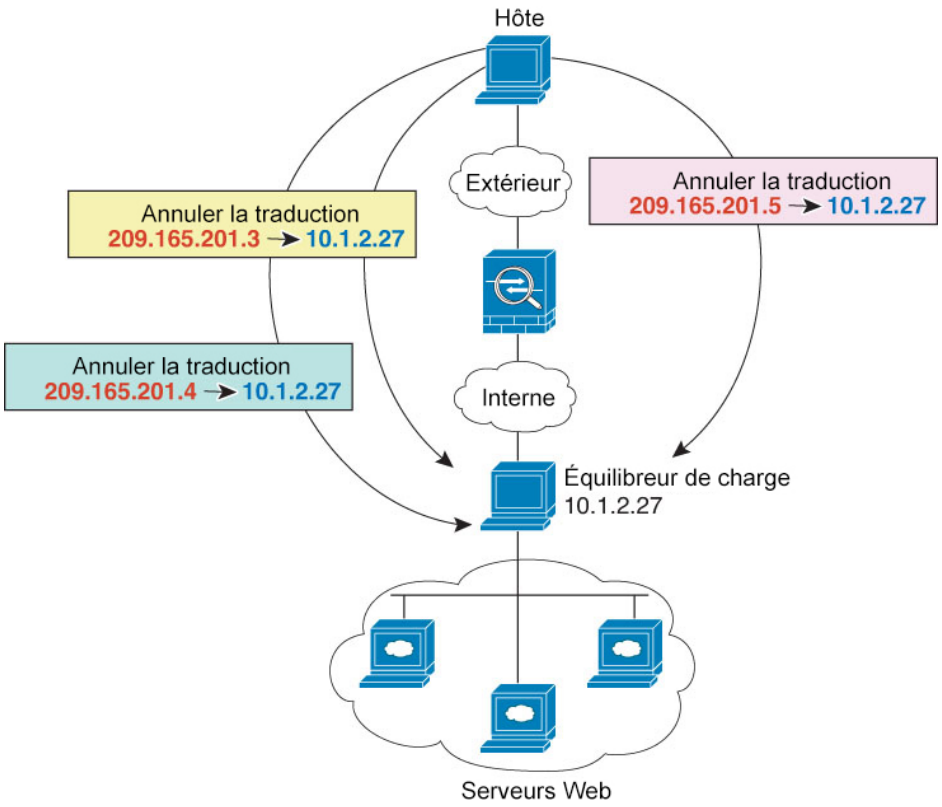
La figure suivante montre un scénario de NAT statique un-à-plusieurs typique. Comme le lancement par l'hôte réel utilise toujours la première adresse mappée, la traduction entre l'adresse IP de l'hôte réel et la première adresse IP mappée est techniquement la seule traduction bidirectionnelle.

Illustration 13 : 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. Pour plus de détails sur la façon de configurer cet exemple, consultez Équilibreur de charge interne avec plusieurs adresses mappées (NAT statique, un à plusieurs), à la page 202 .

Illustration 14 : Exemple de NAT statique un vers plusieurs



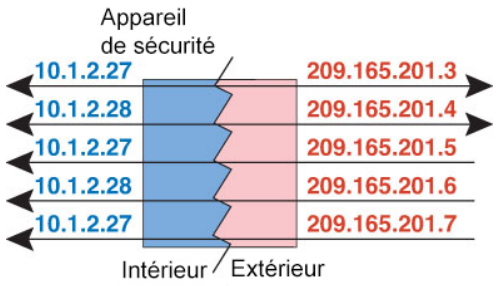
Autres scénarios de mappage (non recommandés)

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-à-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 15 : NAT statique quelques-uns vers plusieurs

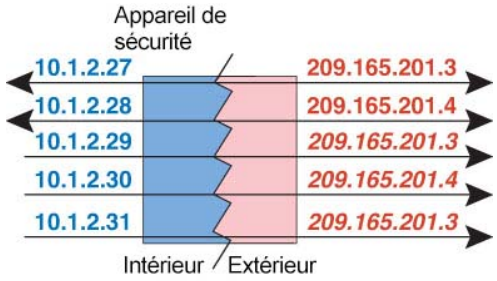


Pour une configuration plusieurs vers quelques ou plusieurs vers un, où vous avez plus d'adresses réelles que d'adresses mappées, vous manquez d'adresses mappées avant de manquer d'adresses réelles. Seuls les mappages entre les adresses IP réelles les plus basses et le groupement mappé entraînent un 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, protocole) 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 16 : 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 d'objet réseau statique ou la NAT statique avec traduction de port

Cette section décrit comment configurer une règle de NAT statique à l'aide de la NAT d'objet réseau.

Procédure

Étape 1 Ajouter la NAT à un objet réseau nouveau ou existant :

- Pour ajouter un nouvel objet réseau, choisissez **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)**, puis cliquez sur **Add (Ajouter) > Add Network Object NAT Rule (Ajouter une règle NAT d'objet réseau)**.
- Pour ajouter la NAT à un objet réseau existant, choisissez **Configuration > Firewall (Pare-feu) > Objects (Objets) > Network Objects/Groups (Objets/groupes réseau),** puis modifiez un objet réseau.

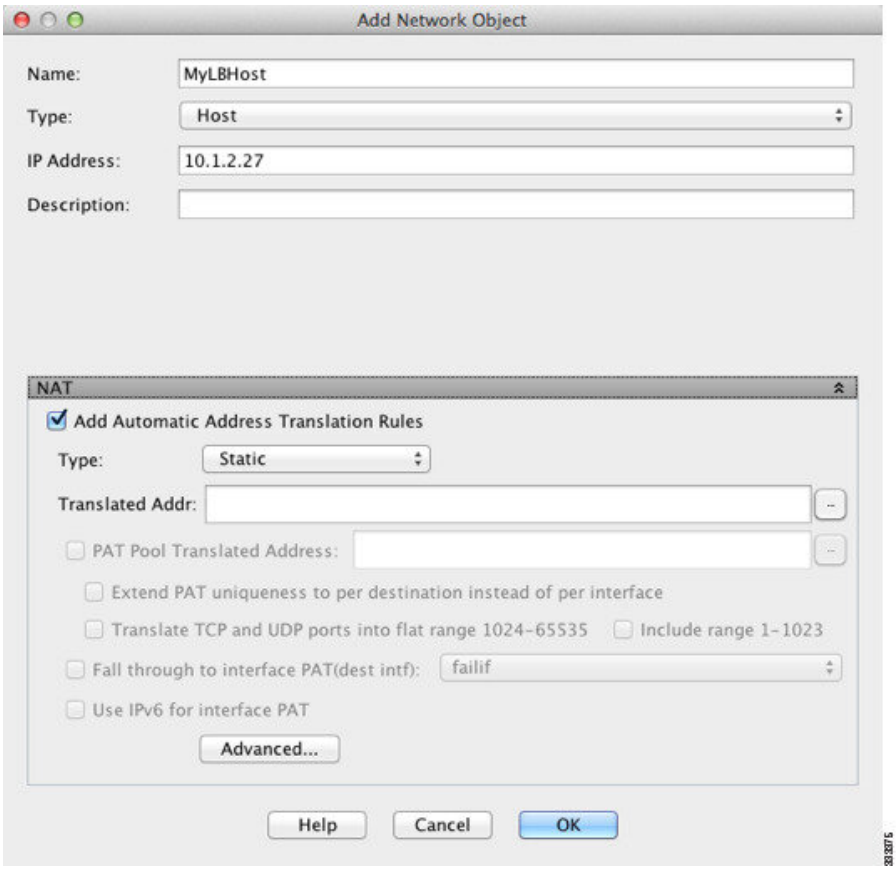
Étape 2 Pour un nouvel objet, renseignez les champs suivants :

- **Name** : nom de l'objet. Utilisez les caractères a à z, A à Z, 0 à 9, un point, un tiret, une virgule ou un trait de soulignement. Le nom doit comporter au maximum 64 caractères.
- **Type** : hôte, réseau ou plage.
- **Adresses IP** : adresses IPv4 ou IPv6, une adresse unique pour un hôte, une adresse de début et de fin pour une plage et pour le sous-réseau, soit une adresse et un masque de réseau IPv4 (par exemple, 10.100.10.0 255.255.255.0) ou une adresse IPv6 et la longueur du préfixe (par exemple, 2001:DB8:0:CD30::/60).

Étape 3 Si la section NAT est masquée, cliquez sur **NAT** pour développer la section.

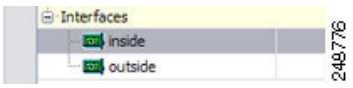
Étape 4 Cochez la case **Add Automatic Translation Rules** (Ajouter des règles de traduction automatique).

Étape 5 Dans la liste déroulante Type, choisissez **Static** (Statique).



Étape 6 Dans le champ Adresse traduite, spécifiez l'adresse IP mappée comme suit. 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. Pour en savoir plus, consultez NAT statique, à la page 166.

- Tapez une adresse IP d'hôte. Il s'agit d'un mappage un à un pour les objets hôtes. Pour les objets de sous-réseau, le même masque réseau est utilisé pour l'adresse de l'hôte en ligne, et vous obtenez des traductions un à un pour les adresses dans le sous-réseau de l'hôte en ligne mappé. Pour les objets de plage, l'adresse mappée comprend le même nombre d'hôtes que dans l'objet de plage, en commençant par l'adresse d'hôte mappée. Par exemple, si l'adresse réelle est définie comme une plage comprise entre 10.1.1.1 et 10.1.1.6, et que vous spécifiez 172.20.1.1 comme adresse mappée, la plage mappée inclura 172.20.1.1 à 172.20.1.6. Pour les traductions NAT46 ou NAT66, il peut s'agir d'une adresse réseau IPv6.
- Cliquez sur le bouton de navigation et sélectionnez un objet réseau (ou créez-en un nouveau). Pour effectuer un mappage un à un pour une plage d'adresses IP, sélectionnez un objet qui contient une plage avec le même nombre d'adresses.
- (Pour NAT statique avec traduction de port uniquement.) Tapez un nom d'interface ou cliquez sur le bouton de navigation, puis choisissez une interface dans la boîte de dialogue Parcourir les adresses traduites. Vous ne pouvez pas sélectionner une interface membre d'un groupe de ponts.



Pour utiliser l'adresse d'interface IPv6, vous devez également cocher la case **Use IPv6 for interface PAT** (Utiliser IPv6 pour la PAT de l'interface). Assurez-vous de cliquer également sur **Advanced**

(Avancé) et de configurer une traduction de port de service. (Vous ne pouvez pas spécifier d'interface en mode transparent.)

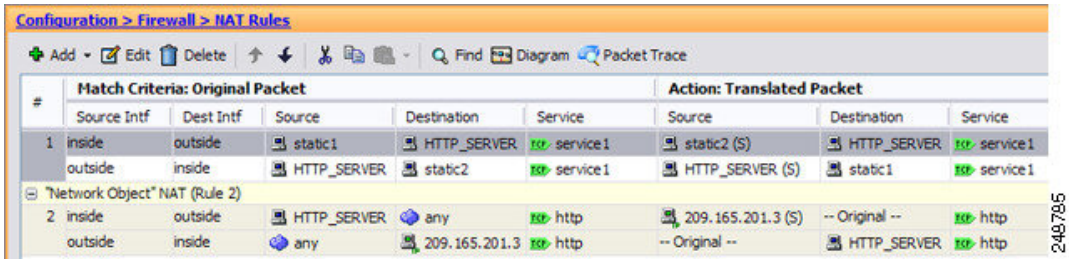
Étape 7 (Facultatif) Pour NAT46, cochez **Use one-to-one address translation** (Utiliser la traduction d'adresse un à un). Pour NAT46, spécifiez un à un pour traduire la première adresse IPv4 en première adresse IPv6, la seconde en seconde, et ainsi de suite. Sans cette option, la méthode intégrée à IPv4 est utilisée. Pour une traduction directe de chaque adresse, vous devez utiliser ce mot-clé.

Étape 8 (Facultatif) Cliquez sur **Avancé**, configurez les options suivantes dans la boîte de dialogue des paramètres NAT avancés, puis cliquez sur **OK**.

- **Traduire les réponses DNS pour la règle**—Traduit l'adresse IP dans les réponses DNS. Assurez-vous que l'inspection DNS est activée (elle est activée par défaut). Consultez Réécriture des requêtes et des réponses DNS à l'aide de la NAT, à la page 244 pour de plus amples renseignements.
- **Disable Proxy ARP on egress interface** (Désactiver le proxy ARP sur l'interface de sortie) : désactive le proxy ARP pour les paquets entrants destinés aux adresses IP mappées. Pour en savoir plus sur les conditions qui peuvent nécessiter la désactivation du proxy ARP, consultez Adresses mappées et routage, à la page 224.
- (Requis pour les interfaces membres d'un groupe de ponts.) **Interface** : spécifie l'interface réelle (**Source**) et l'interface mappée (**Destination**) auxquelles cette règle NAT s'applique. Par défaut, la règle s'applique à toutes les interfaces, à l'exception des interfaces membres des groupes de ponts.
- **Service** : configure la NAT statique avec traduction de port. Choisissez le protocole, puis saisissez le port réel et le port mappé. Vous pouvez utiliser des numéros de port ou un nom de port bien connu tel que http.

Étape 9 Cliquez sur **OK**, puis sur **Apply**(appliquer).

Comme les règles statiques sont bidirectionnelles (permettant l'initiation vers et depuis l'hôte réel), le tableau NAT Rules (Règles NAT) affiche deux lignes pour chaque règle statique, une pour chaque direction.



Configurer la NAT statique Twice ou la NAT statique avec traduction de port

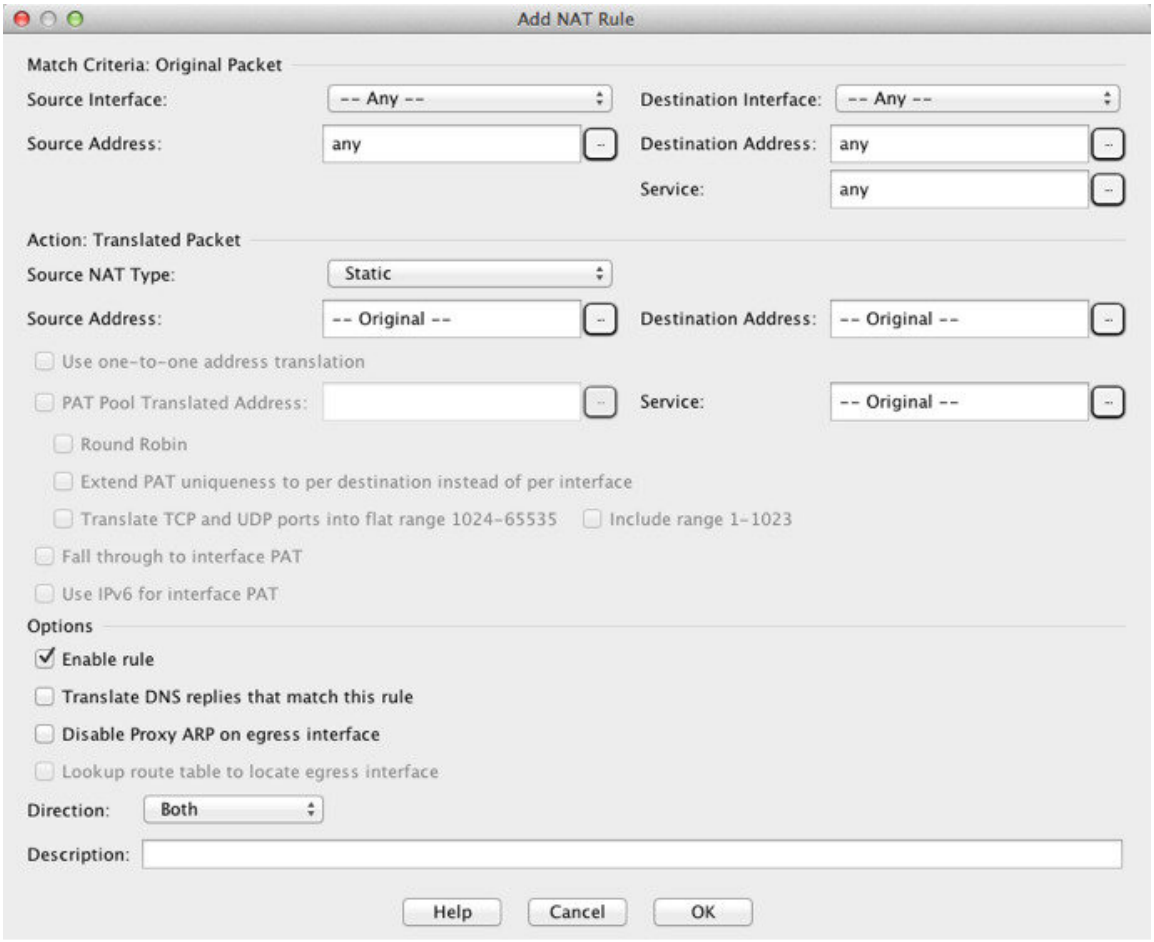
Cette section décrit comment configurer une règle de NAT statique à l'aide de la NAT Twice.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall** > **NAT Rules** (Configuration > Pare-feu > Règles NAT), puis effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter), ou **Add > Add NAT Rule Before Network Object NAT Rules** (Ajouter > Ajouter une règle NAT avant les règles NAT de l'objet réseau).
- Cliquez sur **Add > Add NAT Rule After Network Object NAT Rules** (Ajouter > Ajouter une règle NAT après les règles NAT de l'objet réseau).
- Sélectionnez une règle de NAT Twice et cliquez sur **Edit** (Modifier).

La boîte de dialogue Add NAT Rule (ajouter une règle NAT) apparaît.

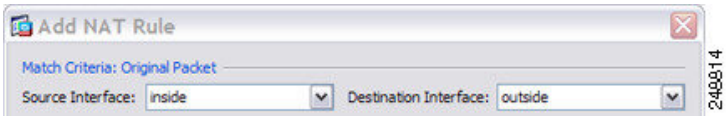


Étape 2 (Requis pour les interfaces membres d'un groupe de ponts.) Définissez les interfaces source et destination.

En mode routé, la valeur par défaut est n'importe quelle interface pour la source et la destination. Vous pouvez sélectionner des interfaces spécifiques pour l'une des options ou les deux. Cependant, vous devez sélectionner

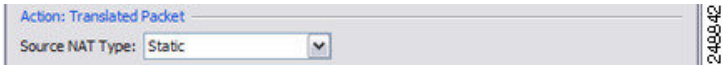
l'interface lors de l'écriture d'une règle pour les interfaces des membres du groupe de ponts; « any » n'inclut pas ces interfaces.

a) Dans la liste déroulante **Critères de correspondance : Paquet original > Interface source**, choisissez l'interface source.
b) Dans la liste déroulante **Correspondance des critères : paquet d'origine > interface de destination**, choisissez l'interface de destination.

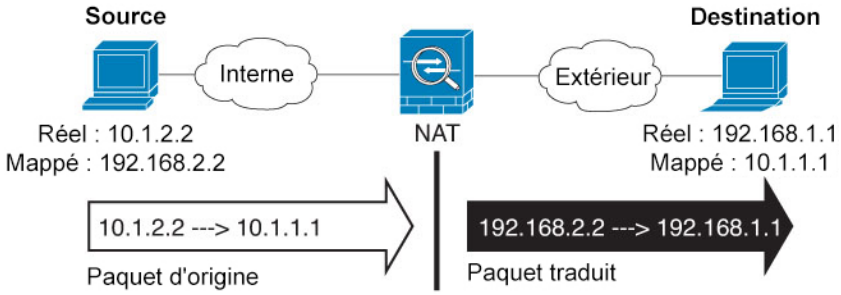


Étape 3 Choisissez **Static** (Statique) dans la liste déroulante **Action > Translated Packet** > **Source NAT Type** (Action > Paquet traduit > Type de NAT source). Statique est le paramètre par défaut.

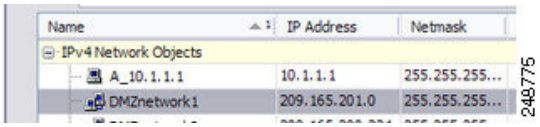
Ce paramètre s'applique uniquement à l'adresse source; la traduction de destination est toujours statique.



Étape 4 Identifiez les adresses de paquets d'origine, qu'elles soient IPv4 ou IPv6; c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface source (l'*adresse source réelle* et l'*adresse de destination mappée*). Voir la figure suivante pour un exemple du paquet original par rapport au paquet traduit.



a) Pour **les critères de correspondance : le paquet d'origine > l'adresse source**, cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse source d'origine. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. La valeur par défaut est **Any**, mais n'utilisez pas cette option, sauf pour la NAT d'identité.



b) (Facultatif) Pour **les critères de correspondance : le paquet d'origine > l'adresse de destination**, cliquez sur le bouton de navigation et choisissez un objet réseau, un groupe ou une interface réseau existant, ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse de destination d'origine.

Bien que la fonctionnalité principale de la NAT Twice soit l'inclusion de l'adresse IP de destination, l'adresse IP de destination est facultative. 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 configurer la NAT Twice sans adresse de destination pour profiter de certaines des autres qualités de la NAT Twice, y compris l'utilisation de groupes d'objets réseau pour les adresses réelles ou

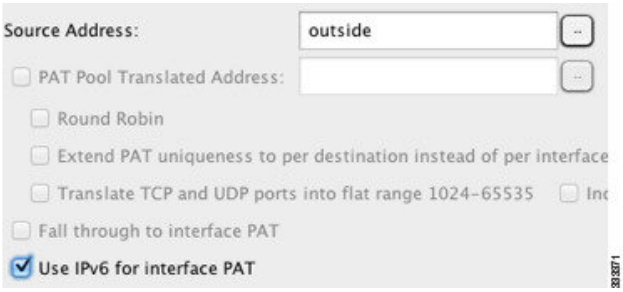
le tri manuel des règles. Pour en savoir plus, consultez Comparaison de NAT objet de réseau et Twice NAT (NAT en double), à la page 124.

Étape 5 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 (l'*adresse source mappée* et l'*adresse de destination réelle*). Vous pouvez traduire d'IPv4 à IPv6, si vous le souhaitez.

a) Pour **Action : Paquet traduit > Adresse source**, cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse source traduite.

Pour la NAT statique, le mappage est généralement un à un, de sorte que le nombre d'adresses réelles est égal au nombre d'adresses mappées. Vous pouvez, cependant, avoir des quantités différentes si vous le souhaitez.

Pour la NAT d'interface statique avec traduction de port, vous pouvez préciser l'interface au lieu d'un objet ou d'un groupe de réseau pour l'adresse mappée. Si vous souhaitez utiliser l'adresse IPv6 de l'interface, cochez la case **Utiliser IPv6 pour la PAT de l'interface**. Vous ne pouvez pas sélectionner un membre d'interface de groupe de pont.



Pour en savoir plus, consultez NAT statique avec traduction de port, à la page 167. Consultez Directives pour la NAT, à la page 127 pour en savoir plus sur les adresses IP mappées non autorisées.

b) (Facultatif) Pour **l'action : Paquet traduit > Adresse de destination**, cliquez sur le bouton de navigation et choisissez un objet ou un groupe de réseau existant, ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse de destination traduite. Vous pouvez également utiliser un objet réseau FQDN pour l'adresse mappée de destination.

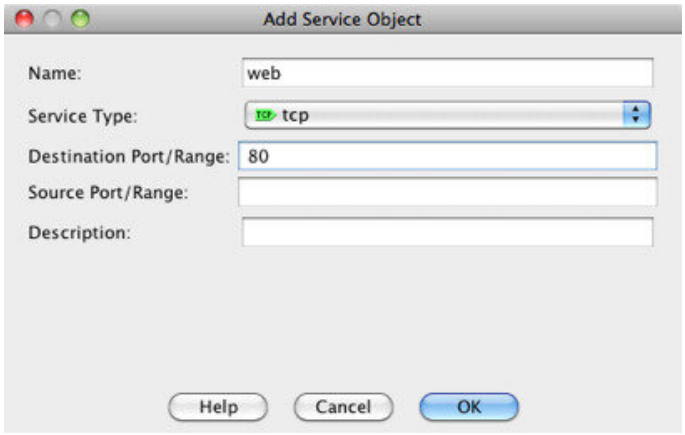
Étape 6 (Facultatif) Déterminez les ports du service source ou de destination pour la traduction de service.

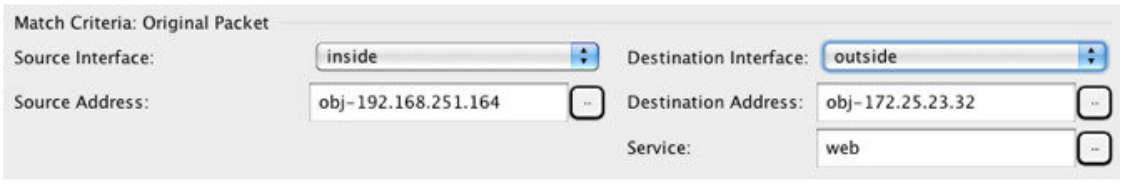
- Déterminez le port source ou de destination du paquet d'origine (le *port source réel* **ou** le *port de destination mappé*). Pour **les critères de correspondance : Paquet d'origine > Service**, cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie les ports ou créez un nouvel objet dans la boîte de dialogue Parcourir le service d'origine.
- Identifiez le port source ou de destination du paquet traduit (le *port source mappé* **ou** le *port de destination réel*). Pour **Action : Paquet traduit > Service**, cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie des ports, ou créez un nouvel objet à partir de la boîte de dialogue Parcourir le service traduit.

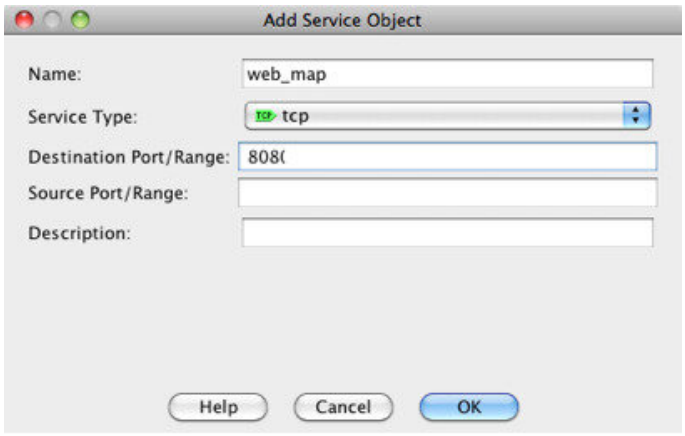
Un objet de service peut contenir à la fois un port source et un port de destination. Vous devez préciser *soit* le port source *soit* le port de destination pour les objets de service réels et mappés. Vous ne devez spécifier *les deux* ports source et de destination que si votre application utilise un port source fixe (comme certains serveurs DNS); mais les ports sources fixes sont rares. Dans le cas rare où vous spécifiez les deux ports source et de destination dans l'objet, l'objet du service de paquets d'origine contient le port source réel/port de

destination mappé; l'objet de service de paquets traduit contient le port source mappé/port de destination réel. Lorsque vous traduisez un port, assurez-vous que les protocoles des objets de service réel et mappé sont identiques (par exemple, TCP). Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés. L'opérateur "pas égal" (**!=**) n'est pas pris en charge.

Par exemple :





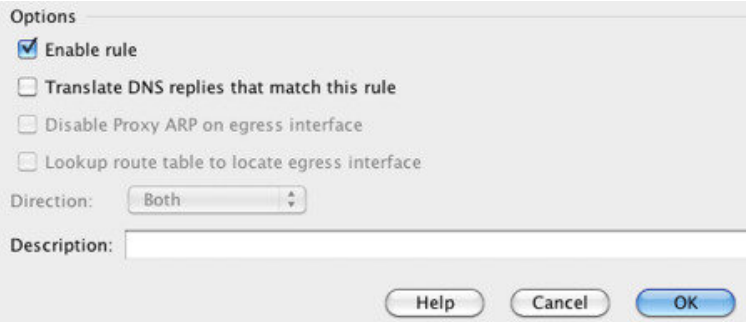




Étape 7 (Facultatif) Pour NAT46, cochez la case **Use one-to-one address translation** (Utiliser la traduction d'adresse un à un). Pour NAT46, spécifiez un à un pour traduire la première adresse IPv4 en première adresse IPv6, la

seconde en seconde, et ainsi de suite. Sans cette option, la méthode intégrée à IPv4 est utilisée. Pour une traduction directe de chaque adresse, vous devez utiliser ce mot-clé.

Étape 8 (Facultatif) Configurez les options NAT dans la zone Options.



- **Enable rule** (Activer la règle) : active cette règle NAT. La règle est activée par défaut.
- (Pour une règle de source uniquement.) **Translate DNS replies that match this rule** (Traduire les réponses DNS qui correspondent à cette règle) : réécrit l'enregistrement DNS A dans les réponses DNS. Assurez-vous que l'inspection DNS est activée (elle est activée par défaut). Vous ne pouvez pas configurer la modification DNS si vous configurez une adresse de destination. Consultez Réécriture des requêtes et des réponses DNS à l'aide de la NAT, à la page 244 pour de plus amples renseignements.
- **Disable Proxy ARP on egress interface** (Désactiver le proxy ARP sur l'interface de sortie) : désactive le proxy ARP pour les paquets entrants destinés aux adresses IP mappées. Consultez Adresses mappées et routage, à la page 224 pour de plus amples renseignements.
- **Direction** : pour rendre la règle unidirectionnelle, choisissez **Unidirectional** (Unidirectionnel). La valeur par défaut est les deux. Rendre la règle unidirectionnelle empêche les adresses de destination d'établir des connexions avec les adresses réelles.
- **Description** : ajoute une description à la règle d'une longueur maximale de 200 caractères.

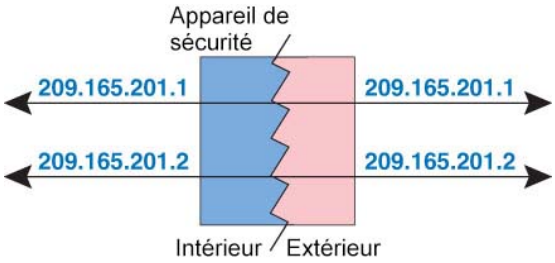
Étape 9 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

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 ce réseau vers lui-même. La NAT d'identité est nécessaire pour le VPN d'accès à distance, lorsque vous devez exclure le trafic client de la NAT.

La figure suivante montre un scénario de NAT d'identité typique.

Illustration 17 : NAT d'identité



Les rubriques suivantes expliquent comment configurer la NAT d'identité.

Configurer la NAT d'objet de réseau d'identité

Cette section décrit comment configurer une règle d'identité NAT à l'aide de la NAT d'objet réseau.

Procédure

Étape 1 Ajouter la NAT à un objet réseau nouveau ou existant :

- Pour ajouter un nouvel objet réseau, choisissez **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)**, puis cliquez sur **Add (Ajouter) > Add Network Object NAT Rule (Ajouter une règle NAT d'objet réseau)**.
- Pour ajouter la NAT à un objet réseau existant, choisissez **Configuration > Firewall (Pare-feu) > Objects (Objets) > Network Objects/Groups (Objets/groupes réseau),** puis modifiez un objet réseau.

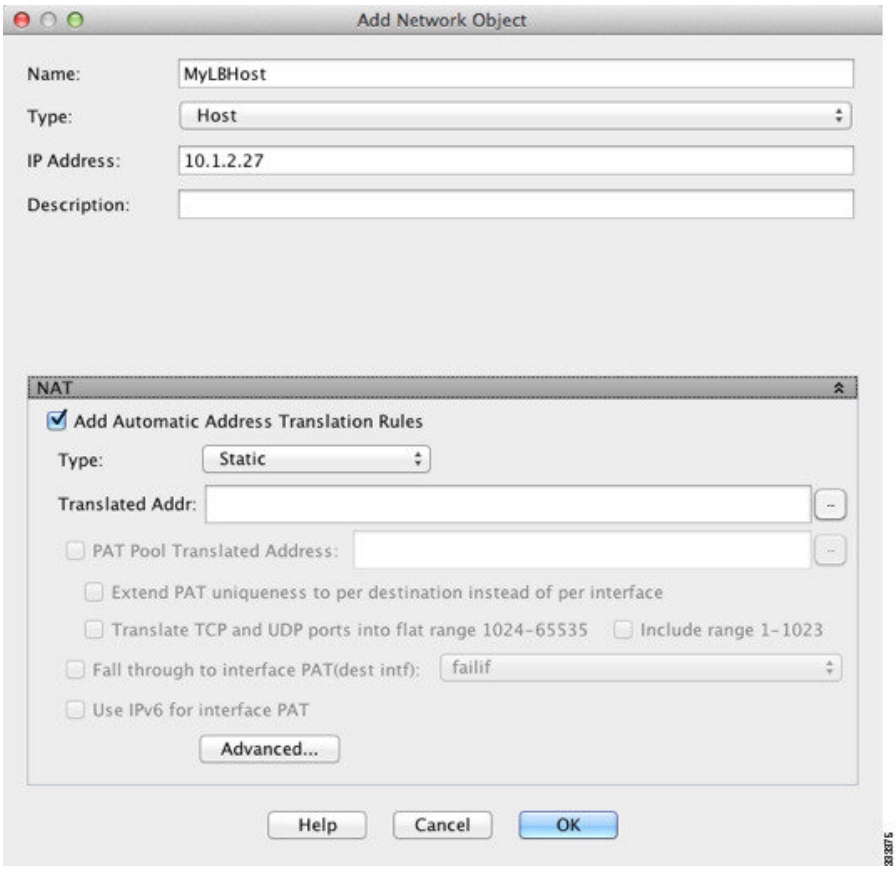
Étape 2 Pour un nouvel objet, renseignez les champs suivants :

- **Name** : nom de l'objet. Utilisez les caractères a à z, A à Z, 0 à 9, un point, un tiret, une virgule ou un trait de soulignement. Le nom doit comporter au maximum 64 caractères.
- **Type** : hôte, réseau ou plage.
- **Adresses IP** : adresses IPv4 ou IPv6, une adresse unique pour un hôte, une adresse de début et de fin pour une plage et pour le sous-réseau, soit une adresse et un masque de réseau IPv4 (par exemple, 10.100.10.0 255.255.255.0) ou une adresse IPv6 et la longueur du préfixe (par exemple, 2001:DB8:0:CD30::/60).

Étape 3 Si la section NAT est masquée, cliquez sur **NAT** pour développer la section.

Étape 4 Cochez la case **Add Automatic Translation Rules** (Ajouter des règles de traduction automatique).

Étape 5 Dans la liste déroulante Type, choisissez **Static** (Statique).



Étape 6 Dans l'adresse traduite , effectuez l'une des opérations suivantes :

- Pour les objets hôtes, saisissez la même adresse. Pour les objets de plage, saisissez la première adresse dans la plage réelle (le même nombre d'adresses dans la plage sera utilisée). Pour les objets de sous-réseau, saisissez n'importe quelle adresse dans le sous-réseau réel (toutes les adresses du sous-réseau seront utilisées).
- Cliquez sur le bouton de navigation et sélectionnez un objet réseau (ou créez-en un nouveau). Utilisez cette option lors de la configuration de la NAT d'identité pour une plage d'adresses.

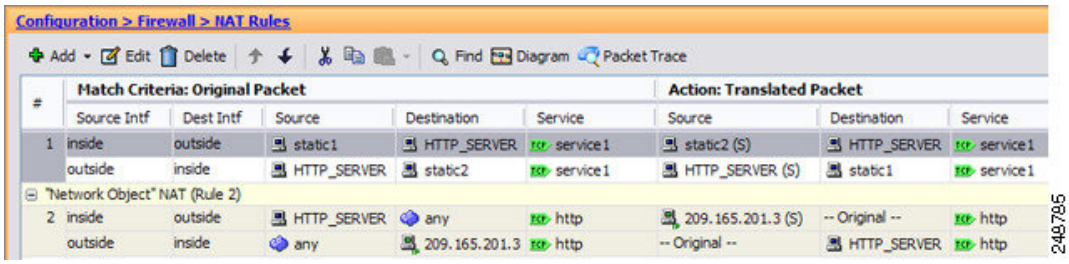
Étape 7 (Facultatif) Cliquez sur **Avancé**, configurez les options suivantes dans la boîte de dialogue des paramètres NAT avancés, puis cliquez sur **OK**.

- **Translate DNS replies for rule** (Traduire les réponses DNS pour la règle) : ne configurez pas cette option pour la NAT d'identité.
- **Disable Proxy ARP on egress interface** (Désactiver le proxy ARP sur l'interface de sortie) : désactive le proxy ARP pour les paquets entrants destinés aux adresses IP mappées. Pour en savoir plus sur les conditions qui peuvent nécessiter la désactivation du proxy ARP, consultez Adresses mappées et routage, à la page 224.
- (Mode routé ; interfaces précisées.) **Lookup route table to locate egress interface** (Rechercher la table de routage pour localiser l'interface de sortie) : détermine l'interface de sortie à l'aide d'une recherche de routage au lieu d'utiliser l'interface spécifiée dans la commande NAT. Consultez Détermination de l'interface de sortie, à la page 226 pour de plus amples renseignements.

- (Requis pour les interfaces membres d'un groupe de ponts.) **Interface** : spécifie l'interface réelle (**Source**) et l'interface mappée (**Destination**) auxquelles cette règle NAT s'applique. Par défaut, la règle s'applique à toutes les interfaces, à l'exception des interfaces membres des groupes de ponts.
- **Service** : ne configurez pas cette option pour la NAT d'identité.

Étape 8 Cliquez sur **OK**, puis sur **Apply**(appliquer).

Comme les règles statiques sont bidirectionnelles (permettant l'établissement de connexions vers et à partir de l'hôte réel), le tableau NAT Rules (Règles NAT) affiche deux lignes pour chaque règle statique, une pour chaque direction, sauf si vous sélectionnez l'option de recherche de routage.



Configurer la NAT d'identité Twice

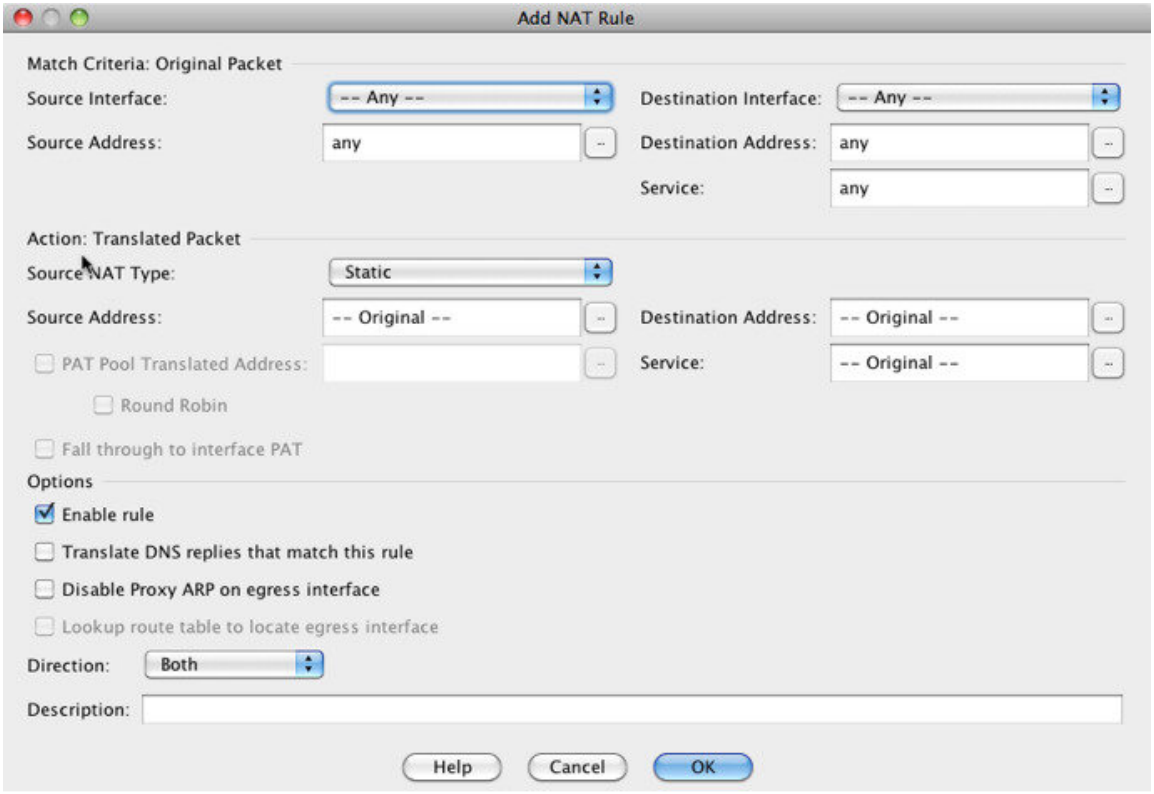
Cette section décrit comment configurer une règle de NAT d'identité à l'aide de la NAT Twice.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall** > **NAT Rules** (Configuration > Pare-feu > Règles NAT), puis effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter), ou **Add > Add NAT Rule Before Network Object NAT Rules** (Ajouter > Ajouter une règle NAT avant les règles NAT de l'objet réseau).
- Cliquez sur **Add > Add NAT Rule After Network Object NAT Rules** (Ajouter > Ajouter une règle NAT après les règles NAT de l'objet réseau).
- Sélectionnez une règle de NAT Twice et cliquez sur **Edit** (Modifier).

La boîte de dialogue Add NAT Rule (ajouter une règle NAT) apparaît.

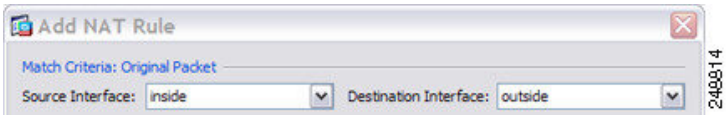


Étape 2 (Requis pour les interfaces membres d'un groupe de ponts.) Définissez les interfaces source et destination.

En mode routage, la valeur par défaut est toute interface pour la source et la destination. Vous pouvez sélectionner des interfaces spécifiques pour l'une des options ou les deux. Cependant, vous devez sélectionner l'interface lors de l'écriture d'une règle pour les interfaces des membres du groupe de ponts ; « any » n'inclut pas ces interfaces.

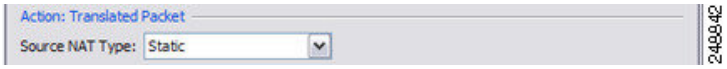
a) Dans la liste déroulante **Match Criteria: Original Packet (Critères de correspondance : paquet d'origine) > Source Interface** (Interface source) , choisissez l'interface source.

b) Dans la liste déroulante **Correspondance des critères : paquet d'origine > interface de destination**, choisissez l'interface de destination.



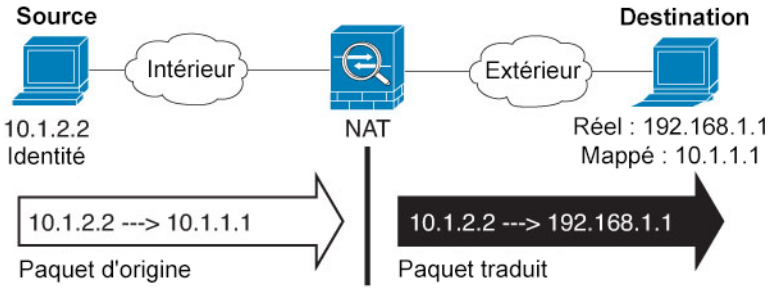
Étape 3 Choisissez **Static** (Statique) dans la liste déroulante **Action > Translated Packet** > **Source NAT Type** (Action > Paquet traduit > Type de NAT source). Statique est le paramètre par défaut.

Ce paramètre s'applique uniquement à l'adresse source; la traduction de destination est toujours statique.

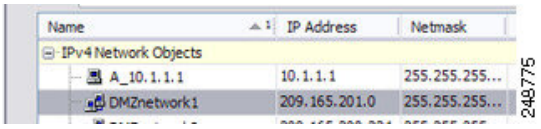


Étape 4 Identifiez les adresses de paquets d'origine, qu'elles soient IPv4 ou IPv6, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface source (*l'adresse source réelle* et *l'adresse de destination*

mappée). 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.



a) Pour **les critères de correspondance : le paquet d'origine > l'adresse source**, cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse source d'origine. Le groupe ne peut pas contenir à la fois des adresses IPv4 et IPv6; il ne doit contenir qu'un seul type d'adresses. La valeur par défaut est **Any**; Utilisez uniquement cette option lorsque vous définissez l'adresse mappée sur **Any**.



b) (Facultatif) Pour **les critères de correspondance : le paquet d'origine > l'adresse de destination**, cliquez sur le bouton de navigation et choisissez un objet réseau, un groupe ou une interface réseau existant, ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse de destination d'origine.

Bien que la fonctionnalité principale de la NAT Twice soit l'inclusion de l'adresse IP de destination, l'adresse IP de destination est facultative. 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 configurer la NAT Twice sans adresse de destination pour profiter de certaines des autres qualités de la NAT Twice, y compris l'utilisation de groupes d'objets réseau pour les adresses réelles ou le tri manuel des règles. Pour en savoir plus, consultez Comparaison de NAT objet de réseau et Twice NAT (NAT en double), à la page 124.

Pour la NAT d'interface statique avec traduction de port uniquement, choisissez une interface. Si vous spécifiez une interface, veillez à configurer une traduction de service. Pour en savoir plus, consultez NAT statique avec traduction de port, à la page 167.

Étape 5 Identifiez les adresses de paquets traduites, c'est-à-dire les adresses de paquets telles qu'elles apparaissent sur le réseau de l'interface de destination (l'*adresse source mappée* et l'*adresse de destination réelle*).

a) Pour **Action: Translated Packet > Source Address** (Action : Paquet traduit > Adresse source), cliquez sur le bouton de navigation et choisissez le même objet ou groupe réseau dans la boîte de dialogue Browse Translated Source Address (Parcourir l'adresse source traduite) que vous avez choisi pour l'adresse source réelle. Utilisez **any** si vous avez spécifié **any** pour l'adresse réelle.

b) Pour **les critères de correspondance : Paquet traduit > Adresse de destination**, cliquez sur le bouton de navigation et choisissez un objet ou un groupe réseau existant, ou créez un nouvel objet ou un groupe dans la boîte de dialogue Parcourir l'adresse de destination traduite. Vous pouvez également utiliser un objet réseau FQDN pour l'adresse mappée de destination.

Pour la NAT d'identité pour l'adresse de destination, utilisez simplement le même objet ou groupe pour les adresses réelles et mappées.

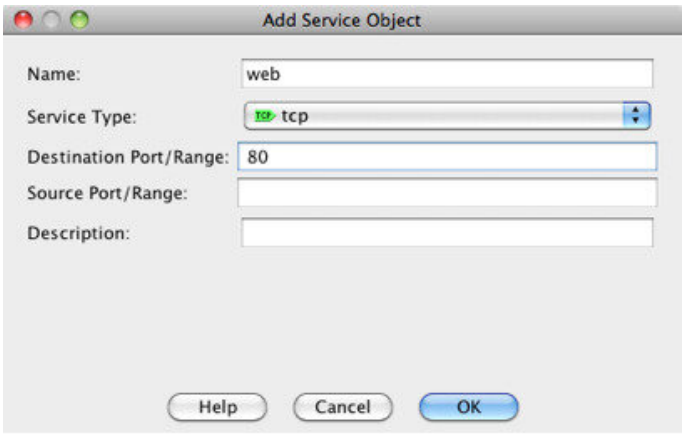
Si vous souhaitez traduire l'adresse de destination, le mappage statique est généralement un à un, de sorte que le nombre d'adresses réelles est égal au nombre d'adresses mappées. Vous pouvez, cependant, avoir des quantités différentes si vous le souhaitez. Pour en savoir plus, consultez NAT statique, à la page 166. Consultez Directives pour la NAT, à la page 127 pour en savoir plus sur les adresses IP mappées non autorisées.

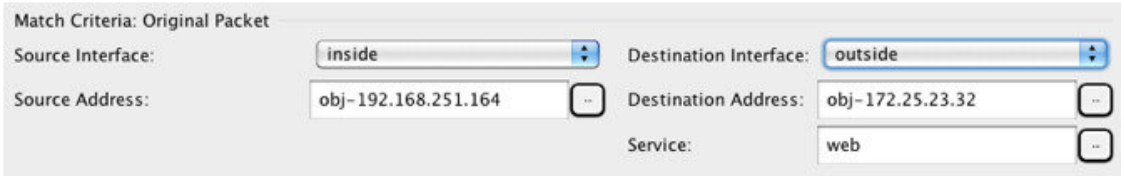
Étape 6 (Facultatif) Déterminez les ports du service source ou de destination pour la traduction de service.

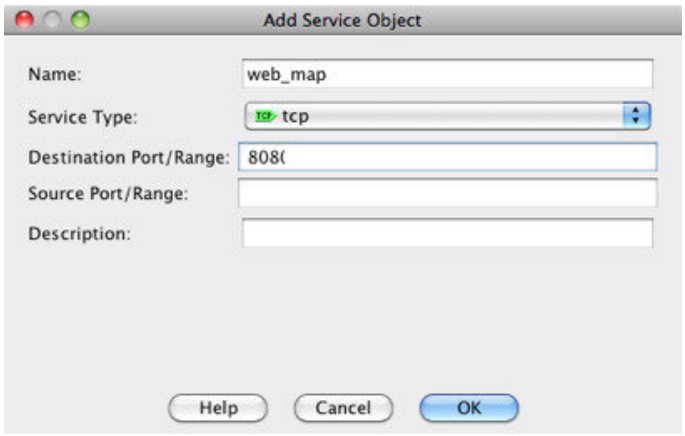
- Déterminez le port source ou de destination du paquet d'origine (le *port source réel* **ou** le *port de destination mappé*). Pour **les critères de correspondance : Paquet d'origine > Service**, cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie les ports ou créez un nouvel objet dans la boîte de dialogue Parcourir le service d'origine.
- Identifiez le port source ou de destination du paquet traduit (le *port source mappé* **ou** le *port de destination réel*). Pour **Action : Paquet traduit > Service**, cliquez sur le bouton de navigation et choisissez un objet de service existant qui spécifie des ports, ou créez un nouvel objet à partir de la boîte de dialogue Parcourir le service traduit.

Un objet de service peut contenir à la fois un port source et un port de destination. Vous devez préciser *soit* le port source *soit* le port de destination pour les objets de service réels et mappés. Vous ne devez spécifier *les deux* ports source et de destination que si votre application utilise un port source fixe (comme certains serveurs DNS) ; mais les ports sources fixes sont rares. Dans le cas rare où vous spécifiez les deux ports source et de destination dans l'objet, l'objet du service de paquets d'origine contient le port source réel/port de destination mappé; l'objet de service de paquets traduit contient le port source mappé/port de destination réel. 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. L'opérateur « pas égal » (**!=**) n'est pas pris en charge.

Par exemple :









Étape 7 (Facultatif) Configurez les options de NAT dans la zone Options.



- **Enable rule** (Activer la règle) : active cette règle NAT. La règle est activée par défaut.
- (Pour une règle de source uniquement.) **Traduire les réponses DNS qui correspondent à cette règle** : bien que cette option soit disponible si vous ne configurez pas d'adresse de destination, elle ne s'applique pas à la NAT d'identité, car vous traduisez l'adresse en elle-même, de sorte que la réponse DNS ne nécessite pas de modification.
- **Disable Proxy ARP on egress interface** (Désactiver le proxy ARP sur l'interface de sortie) : désactive le proxy ARP pour les paquets entrants destinés aux adresses IP mappées. Consultez Adresses mappées et routage, à la page 224 pour de plus amples renseignements.
- (Mode routé ; interfaces précisées.) **Lookup route table to locate egress interface** (Rechercher la table de routage pour localiser l'interface de sortie) : détermine l'interface de sortie à l'aide d'une recherche de routage au lieu d'utiliser l'interface spécifiée dans la commande NAT. Consultez Détermination de l'interface de sortie, à la page 226 pour de plus amples renseignements.
- **Direction** : pour rendre la règle unidirectionnelle, choisissez **Unidirectional** (Unidirectionnel). La valeur par défaut est Both (Les deux). Rendre la règle unidirectionnelle empêche le trafic d'établir des connexions avec les adresses réelles. Vous pouvez utiliser ce paramètre à des fins de test.

- **Description** : ajoute une description à la règle d'une longueur maximale de 200 caractères.

Étape 8 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Surveillance de la NAT

Vous pouvez afficher les graphiques liés à la NAT à partir des pages suivantes :

- **Monitoring (Surveillance) > Properties (Propriétés) > Connection Graphs (Graphiques de connexion) > Xlates** : sélectionnez le graphique Xlate Utilization (Utilisation de Xlate) pour afficher les xlates en cours d'utilisation et les plus utilisés. Cela équivaut à la commande **show xlate**.
- **Monitoring (Surveillance) > Properties (Propriétés) > Connection Graphs (Graphiques de connexion) > Perfmon** : sélectionnez le graphique Xlate Perfmon (Perfmon Xlate) pour afficher les informations sur les performances de la NAT. Cela équivaut aux informations xlate de la commande **show perfmon**.

Historique de la NAT

Nom de la caractéristique	Versions de plateforme	Description
NAT d'objet réseau	8.3(1)	Configure la NAT pour une ou plusieurs adresses IP d'objet réseau. Nous avons introduit ou modifié les écrans suivants : Configuration > Firewall (Pare-feu) > NAT Rules (Règles NAT); Configuration (Configuration) > Firewall (Pare-feu) > Objects (Objets) > Network Objects/Groups (Objets/groupes réseau)
NAT Twice	8.3(1)	NAT Twice vous permet d'identifier l'adresse source et l'adresse de destination en une seule règle. Nous avons modifié l'écran suivant : Configuration (Configuration) > Firewall (Pare-feu) > NAT Rules (Règles NAT).

Nom de la caractéristique	Versions de plateforme	Description
Recherche de routage et d'ARP configurable pour la NAT d'identité	8.4(2)/8.5(1)	Dans les versions précédentes de la NAT d'identité, le proxy ARP était désactivé et une recherche de routage était toujours utilisée pour déterminer l'interface de sortie. Vous ne pouviez pas configurer ces paramètres. Dans les versions 8.4(2) et ultérieures, le comportement par défaut de la NAT d'identité a été modifié pour correspondre à celui des autres configurations NAT statiques : le proxy ARP est activé et la configuration NAT détermine l'interface de sortie (si spécifiée) par défaut. Vous pouvez laisser ces paramètres tels quels, ou les activer ou les désactiver discrètement. Notez que vous pouvez désormais désactiver le proxy ARP pour la NAT statique normale. Pour les configurations antérieures à la version 8.3, la migration des règles d'exemption de NAT (la commande nat **0 access-list**) vers la version 8.4(2) et les versions ultérieures comprend désormais les mots-clés suivants pour désactiver le proxy ARP et utiliser une recherche de routage : **no-proxy-arp** et **route-lookup**. Le mot-clé **unidirectionnal** qui a été utilisé pour la migration vers les versions 8.3(2) et 8.4(1) n'est plus utilisé pour la migration. Lors de la mise à niveau vers la version 8.4(2) à partir des versions 8.3(1), 8.3(2) et 8.4(1), toutes les configurations NAT d'identité incluront désormais les mots clés **no-proxy-arp** et **route-lookup**, pour maintenir les fonctionnalités existantes. Le mot clé **unidirectional** est supprimé. Nous avons modifié les écrans suivant : Configuration > Firewall (Pare-feu) > NAT Rules (Règles NAT) > Add/Edit Network Object (Ajouter/Modifier un objet réseau) > Advanced NAT Settings (Paramètres NAT avancés); Configuration (Configuration) > Firewall (Pare-feu) > NAT Rules (Règles NAT) > Add/Edit NAT Rule (Ajouter/Modifier une règle NAT).

Nom de la caractéristique	Versions de plateforme	Description
Affectation d'adresses de pool PAT et round-robin	8.4(2)/8.5(1)	Vous pouvez désormais spécifier un pool d'adresses PAT au lieu d'une adresse unique. Vous pouvez également éventuellement activer l'affectation round-robin des adresses PAT au lieu d'utiliser d'abord tous les ports d'une adresse PAT avant d'utiliser l'adresse suivante dans le regroupement. Ces fonctionnalités aident à éviter qu'un grand nombre de connexions à partir d'une seule adresse PAT ne semble faire partie d'une attaque DoS et facilitent la configuration d'un grand nombre d'adresses PAT. Nous avons modifié les écrans suivants : Configuration > Firewall (Pare-feu) > NAT Rules (Règles NAT) > Add/Edit Network Object (Ajouter/Modifier un objet réseau); Configuration (Configuration) > Firewall (Pare-feu) > NAT Rules (Règles NAT) > Add/Edit NAT Rule (Ajouter/Modifier une règle NAT).
L'allocation de pool PAT round-robin utilise la même adresse IP pour les hôtes existants	8.4(3)	Lors de l'utilisation d'un pool PAT avec affectation round-robin, si un hôte a une connexion existante, les connexions suivantes de cet hôte utiliseront la même adresse IP PAT si des ports sont disponibles. Nous n'avons pas modifié d'écrans. *Cette fonctionnalité n'est pas disponible dans les versions 8.5(1) ou 8.6(1).*
Plage uniforme de ports PAT pour un pool PAT	8.4(3)	S'il est disponible, le numéro de port source réel est utilisé pour le port mappé. Cependant, sans cette option, si le port réel n'est *pas* disponible, les ports mappés sont choisis par défaut dans la même plage de ports que le numéro de port réel : 1 à 511, 512 à 1023 ou 1 024 à 65 535. Par conséquent, les ports inférieurs à 1024 ont seulement un petit pool PAT. Si une grande partie du trafic utilise les plages de ports inférieures, lors de l'utilisation d'un pool PAT, vous pouvez désormais spécifier une plage uniforme de ports à utiliser au lieu des trois niveaux de taille inégal: 1024 à 65 535 ou 1 à 65 535. Nous avons modifié les écrans suivants : Configuration > Firewall (Pare-feu) > NAT Rules (Règles NAT) > Add/Edit Network Object (Ajouter/Modifier un objet réseau); Configuration (Configuration) > Firewall (Pare-feu) > NAT Rules (Règles NAT) > Add/Edit NAT Rule (Ajouter/Modifier une règle NAT). *Cette fonctionnalité n'est pas disponible dans les versions 8.5(1) ou 8.6(1).*

Nom de la caractéristique	Versions de plateforme	Description
PAT étendu pour un pool PAT	8.4(3)	Chaque adresse IP PAT permet jusqu'à 65 535 ports. Si 65 535 ports ne fournissent pas assez de traductions, vous pouvez maintenant activer la PAT étendue pour un pool PAT. La réserve PAT étendue fait appel à 65 535 ports par *service*, et non par adresse IP, en incluant l'adresse de destination et le port dans les informations de traduction. Nous avons modifié les écrans suivants : Configuration > Firewall (Pare-feu) > NAT Rules (Règles NAT) > Add/Edit Network Object (Ajouter/Modifier un objet réseau); Configuration (Configuration) > Firewall (Pare-feu) > NAT Rules (Règles NAT) > Add/Edit NAT Rule (Ajouter/Modifier une règle NAT). *Cette fonctionnalité n'est pas disponible dans les versions 8.5(1) ou 8.6(1).*

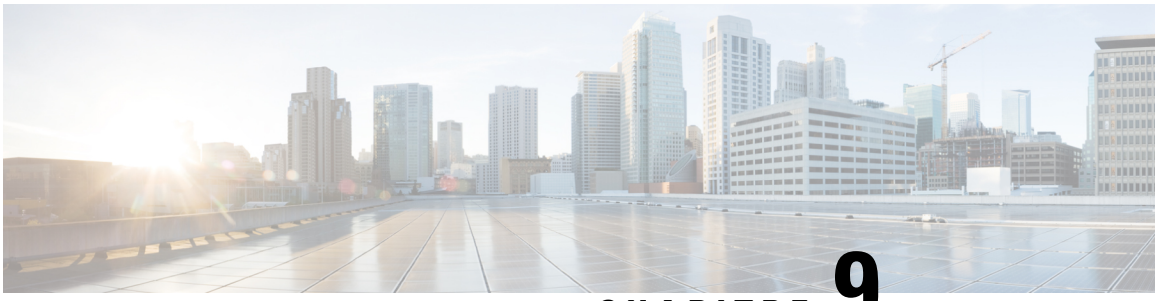
Nom de la caractéristique	Versions de plateforme	Description
Règles de NAT automatiques pour traduire l'adresse IP locale d'un homologue de VPN en adresse IP réelle de l'homologue	8.4(3)	Dans de rares cas, vous pouvez utiliser l'adresse IP réelle d'un homologue VPN sur le réseau interne au lieu d'une adresse IP locale attribuée. Normalement avec le VPN, l'homologue reçoit une adresse IP locale attribuée pour accéder au réseau interne. Cependant, vous pouvez traduire l'adresse IP locale en adresse IP publique réelle de l'homologue si, par exemple, vos serveurs internes et la sécurité du réseau sont basés sur l'adresse IP réelle de l'homologue. Vous pouvez activer cette fonctionnalité sur une interface par groupe de tunnels. Les règles de NAT d'objet sont ajoutées et supprimées dynamiquement lorsque la session VPN est établie ou déconnectée. Vous pouvez afficher les règles à l'aide de la commande **show nat** . En raison de problèmes de routage, nous ne recommandons pas l'utilisation de cette fonctionnalité, sauf si vous savez que vous en avez besoin; communiquez avec le centre d'assistance technique Cisco pour confirmer la compatibilité de la fonctionnalité avec votre réseau. Voir les limitations suivantes : • Ne prend en charge que Cisco IPsec et Secure Client. • Le trafic de retour vers les adresses IP publiques doit être acheminé vers l'ASA pour que la politique de NAT et la politique de VPN puissent être appliquées. • Ne prend pas en charge l'équilibrage de la charge (en raison de problèmes de routage). • Ne prend pas en charge l'itinérance (modification d'adresse IP publique). ASDM ne prend pas en charge cette commande; entrez la commande à l'aide de Command Line Tool (Outil de ligne de commande).
Prise en charge de la NAT pour IPv6	9.0(1)	La NAT prend désormais en charge le trafic IPv6 ainsi que la traduction entre IPv4 et IPv6. La traduction entre IPv4 et IPv6 n'est pas prise en charge en mode transparent. Nous avons modifié les écrans suivants : Configuration > Firewall (Pare-feu) > Objects (Objets) > Network Objects/Group (Objets/groupe réseau); Configuration (Configuration) > Firewall (Pare-feu) > NAT Rules (Règles NAT).
Prise en charge de la NAT pour les recherches DNS inversées	9.0(1)	La NAT prend maintenant en charge la traduction de l'enregistrement DNS PTR pour les recherches DNS inversées lors de l'utilisation de la NAT IPv4, de la NAT IPv6 et de NAT64 avec l'inspection DNS activée pour la règle NAT.

Nom de la caractéristique	Versions de plateforme	Description
PAT par session	9.0(1)	La fonctionnalité PAT par session améliore l'évolutivité de PAT et, pour la mise en grappe, permet à chaque unité membre de détenir des connexions PAT ; les connexions PAT multi-session doivent être transférées et détenues par l'unité de contrôle. À la fin d'une session PAT par session, l'ASA envoie une réinitialisation et supprime immédiatement le xlate. Cette réinitialisation force le nœud terminal à libérer immédiatement la connexion, en évitant l'état TIME_WAIT. La PAT multi-session, en revanche, utilise le délai d'expiration PAT, par défaut de 30 secondes. Pour le trafic « hit-and-run », comme HTTP ou HTTPS, la fonctionnalité par session peut augmenter considérablement le débit de connexion pris en charge par une adresse. Sans la fonctionnalité par session, le débit de connexion maximal pour une adresse pour un protocole IP est d'environ 2 000 par seconde. Avec la fonctionnalité par session, le débit de connexion pour une adresse pour un protocole IP est de 65535/*average-lifetime* . Par défaut, tout le trafic TCP et le trafic DNS UDP utilisent une xlate PAT par session. Pour le trafic qui nécessite une PAT multi-session, comme H.323, SIP ou Skinny, vous pouvez désactiver la PAT par session en créant une règle de refus par session. Nous avons introduit l'écran suivant : Configuration > Firewall (Pare-feu) > Advanced (Avancé) > Per-Session NAT Rules (Règles NAT par session).
Modèle de validation transactionnelle sur le moteur de règles NAT	9.3(1)	Lorsque cette option est activée, une mise à jour de règle NAT est appliquée une fois la compilation de la règle terminée; sans affecter la performance de correspondance de la règle. Nous avons ajouté la NAT à l'écran suivant : Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > Rule Engine (Moteur de règles).
Améliorations de la NAT de niveau opérateur	9.5(1)	Pour une PAT de niveau fournisseur de services ou à grande échelle, vous pouvez attribuer un bloc de ports pour chaque hôte, au lieu de demander à la NAT d'attribuer une traduction de port à la fois (Voir RFC 6888). Nous avons ajouté la commande suivante : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **PAT Port Block Allocation (Allocation de blocs de ports PAT)**. Nous avons ajouté les boîtes de dialogue **Enable Block Allocation** (Activer l'allocation de blocage) pour l'objet NAT et la NAT Twice.

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de la NAT pour SCTP	9.5(2)	Vous pouvez maintenant spécifier les ports SCTP dans les règles NAT des objets réseau statiques. L'utilisation de SCTP dans la NAT Twice statique n'est pas recommandée. La NAT/PAT dynamique ne prend pas en charge SCTP. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **NAT** Add/Edit static network object NAT rule (Ajouter/Modifier une règle NAT d'objet réseau statique), boîte de dialogue **Advanced NAT Settings** (Paramètres NAT avancés).
Journalisation provisoire pour l'allocation de bloc de ports NAT.	9.12(1)	Lorsque vous activez l'allocation de bloc de ports pour la NAT, le système génère des messages de journal système lors de la création et de la suppression d'un bloc de port. Si vous activez la journalisation provisoire, le système génère le message 305017 à l'intervalle que vous spécifiez. Les messages font état de tous les blocages de ports actifs à ce moment-là, y compris le protocole (ICMP, TCP, UDP), l'interface source et de destination, l'adresse IP et le blocage de ports. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **PAT Port Block Allocation (Allocation de blocs de ports PAT)** .

Nom de la caractéristique	Versions de plateforme	Description
Modifications apportées à l'attribution d'adresses PAT dans la mise en grappe. L'option **flat** de l'ensemble PAT est désormais activée par défaut et n'est pas configurable.	9.15(1)	La façon dont les adresses PAT sont distribuées aux membres d'une grappe est modifiée. Auparavant, les adresses étaient distribuées aux membres de la grappe, de sorte que votre ensemble de PAT avait besoin d'au moins une adresse par membre de la grappe. Désormais, l'unité de contrôle divise plutôt chaque adresse de pool PAT en blocs de ports de taille égale et les répartit entre les membres de la grappe. Chaque membre dispose de blocs de ports pour les mêmes adresses PAT. Ainsi, vous pouvez réduire la taille de l'ensemble PAT, même à une seule adresse IP, en fonction du nombre de connexions généralement nécessaires à PAT. Les blocs de ports sont attribués en blocs de port 512 uniquement dans la plage de 1024 à 65535. Vous pouvez éventuellement inclure les ports réservés, 1 à 1023, dans cette allocation de bloc lorsque vous configurez les règles de l'ensemble PAT. Par exemple, dans une grappe de 4 nœuds, chaque nœud reçoit 32 blocs, avec lesquels il sera en mesure de gérer 16 384 connexions par adresse IP d'ensemble PAT, contre un seul nœud pouvant gérer les 65 535 connexions par adresse IP d'ensemble PAT. Dans le cadre de ce changement, les regroupements de PAT pour tous les systèmes, qu'ils soient autonomes ou en grappe, utilisent désormais une plage de ports uniforme de 1023 à 65 535. Auparavant, vous pouviez éventuellement utiliser une plage à plat en incluant le mot clé **flat** dans une règle d'ensembles de PAT. Le mot clé **flat** n'est plus pris en charge : l'ensemble de PAT est désormais toujours à plat. Le mot clé **include-reserve** , qui était auparavant un sous-mot clé de **flat** , est maintenant un mot clé indépendant dans la configuration de l'ensemble de PAT. Cette option vous permet d'inclure la plage de 1 à 1 023 ports dans l'ensemble de PAT. Notez que si vous configurez l'allocation de bloc de ports (l'option d'ensemble de PAT **block-allocation**), la taille de votre allocation de bloc est utilisée plutôt que le bloc de 512 ports par défaut. En outre, vous ne pouvez pas configurer la PAT étendue pour un ensemble PAT pour les systèmes d'une grappe. Écrans nouveaux ou modifiés : configuration de l'ensemble de PAT NAT.

Nom de la caractéristique	Versions de plateforme	Description
Nouvelle section 0 pour les règles NAT définies par le système.	9.16(1)	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** .
Prise en charge de la NAT Twice pour les objets de nom de domaine complet (FQDN) en tant que destination (mappée) de la traduction.	9.17(1)	Vous pouvez utiliser un objet de réseau FQDN, par exemple spécifiant www.exemple.com, comme adresse de destination (mappée) de la traduction dans les règles NAT doubles. Le système configure la règle en fonction de l'adresse IP renvoyée par le serveur DNS.



CHAPITRE 9

Exemples et références de NAT

Les rubriques suivantes fournissent des exemples de configuration de la NAT, ainsi que des renseignements sur la configuration et le dépannage avancés.

- Exemples de NAT d'objets réseau, à la page 195
- Exemples relatifs à la NAT Twice, à la page 208
- NAT en mode routé et transparent, à la page 221
- Routage des paquets NAT, à la page 223
- NAT pour VPN, à la page 227
- Traduction des réseaux IPv6, à la page 233
- Réécriture des requêtes et des réponses DNS à l'aide de la NAT, à la page 244

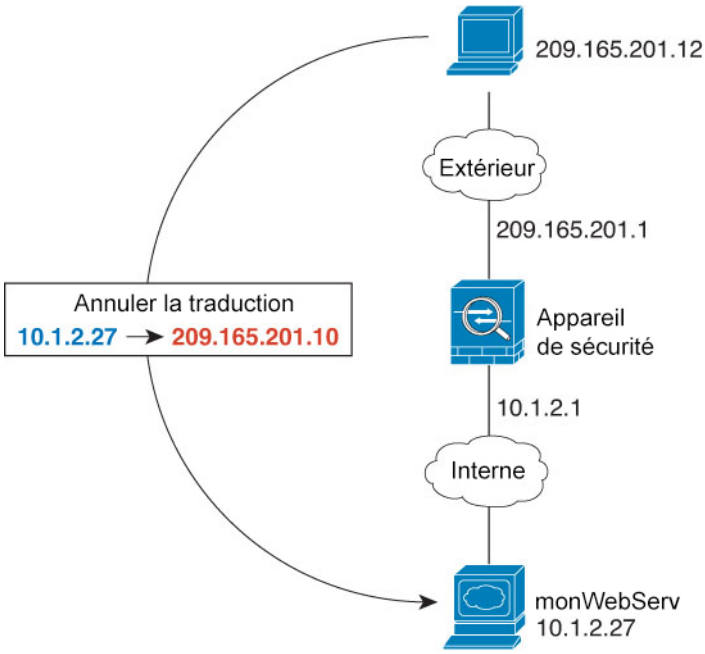
Exemples de NAT d'objets réseau

Voici quelques exemples de configuration pour la NAT d'objet réseau.

Fournir l'accès à un serveur Web interne (NAT 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.

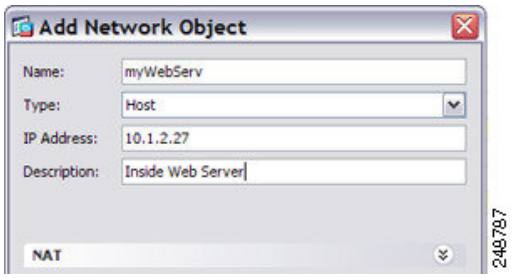
Illustration 18 : NAT statique pour un serveur Web interne



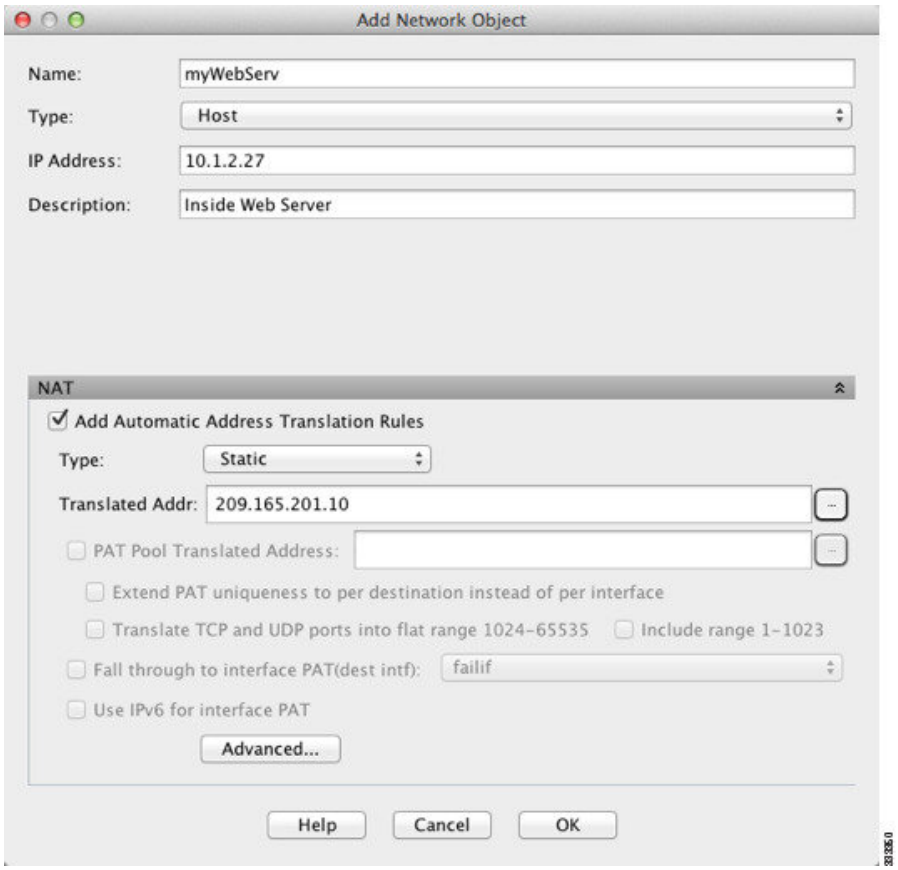
Procédure

Étape 1 Choisissez **Configuration** > **Firewall** > **(Pare-feu)** > **NAT**.

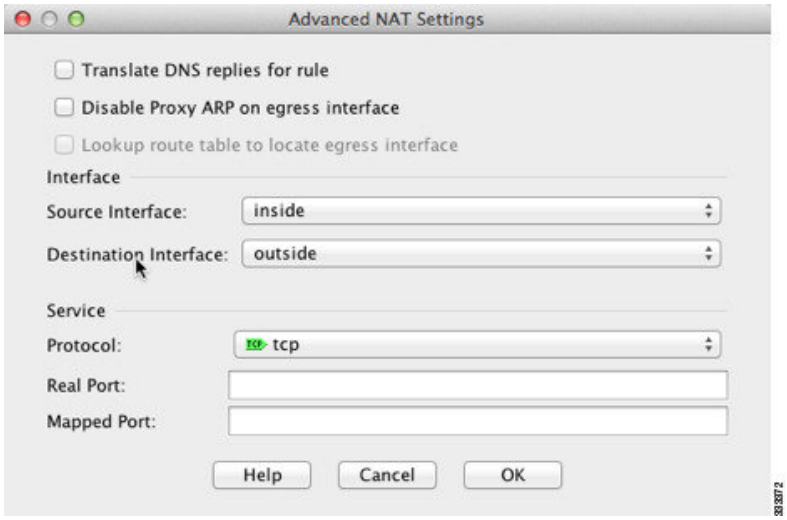
Étape 2 Choisissez **Add (Ajouter)** > **Network Object NAT Rule (Règle NAT d'objet réseau)**, nommez le nouvel objet réseau et définissez l'adresse de l'hôte du serveur Web.



Étape 3 Configurez la NAT statique pour l'objet



Étape 4 Cliquez sur **Advanced** (Avancé) et configurez les interfaces réelles et mappées.

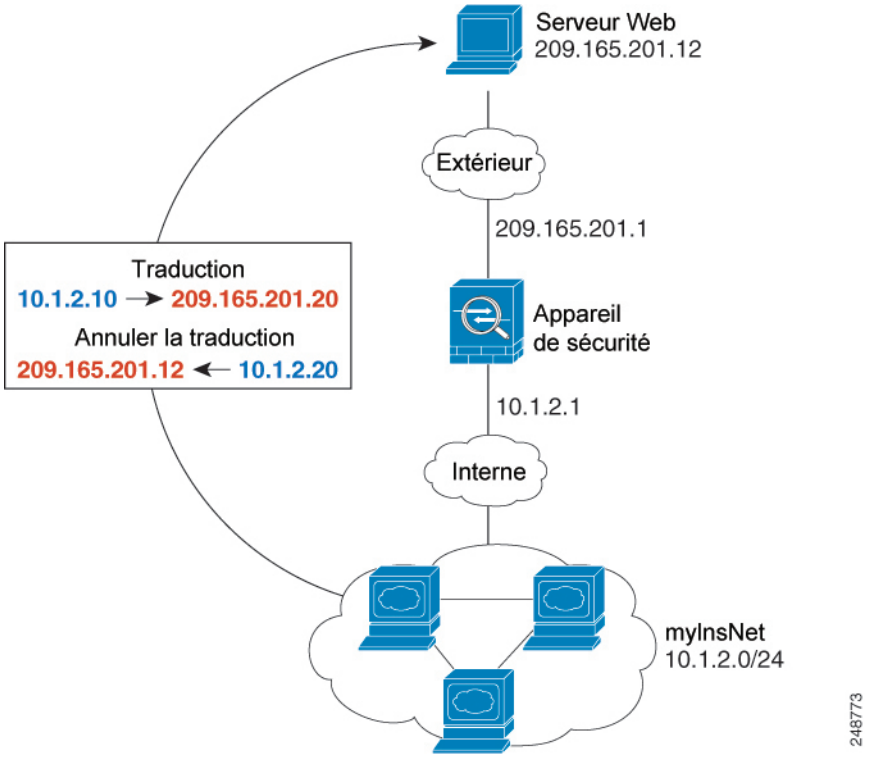


Étape 5 Cliquez sur **OK** pour revenir à la boîte de dialogue Edit Network Object (modifier l'objet de réseau), cliquez de nouveau sur **OK**, puis cliquez sur **Apply** (Appliquer).

NAT pour les hôtes internes (NAT dynamique) et NAT pour un serveur Web externe (NAT statique)

Dans l'exemple suivant, la NAT dynamique est configurée pour les utilisateurs internes sur un réseau privé lorsqu'ils accèdent à l'extérieur. De plus, lorsque des utilisateurs internes se connectent à un serveur Web externe, l'adresse du serveur Web est traduite en une adresse qui semble se trouver sur le réseau interne.

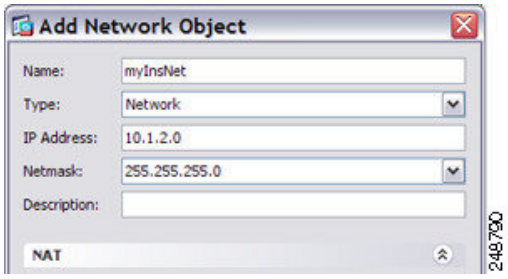
Illustration 19 : NAT dynamique pour l'interne, NAT statique pour le serveur Web externe



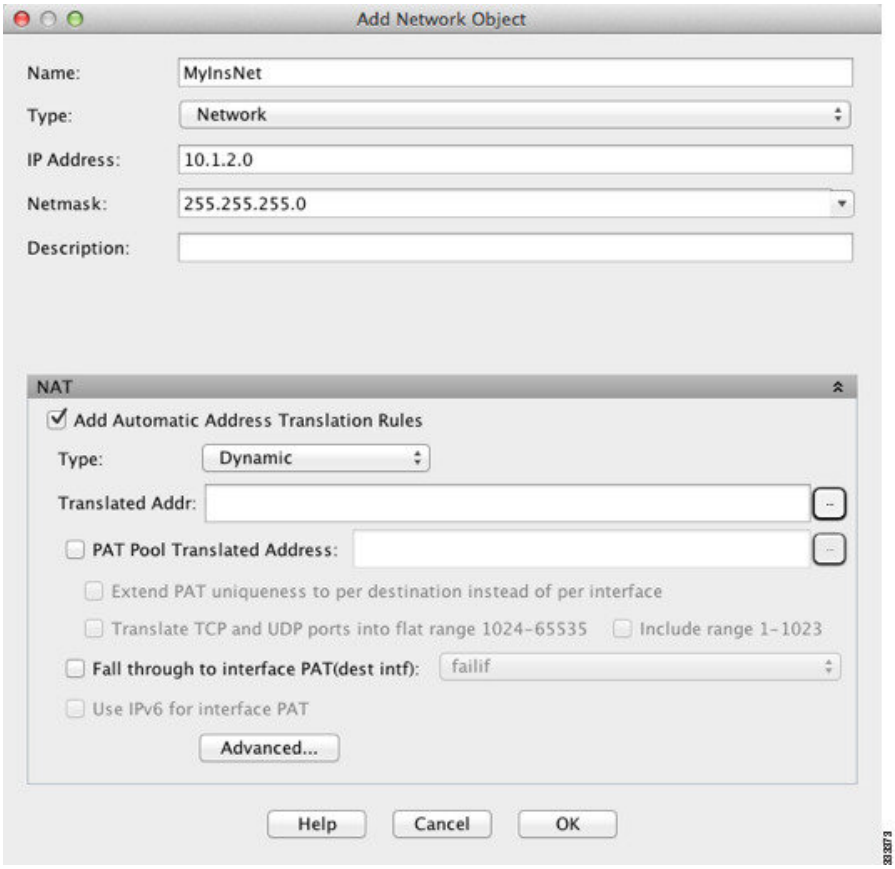
Procédure

Étape 1 Choisissez **Configuration** > **Firewall** > **(Pare-feu)** > **NAT**.

Étape 2 Choisissez **Add (Ajouter)** > **Network Object NAT Rule (Règle NAT d'objet réseau)**, nommez le nouvel objet réseau et définissez le réseau interne.

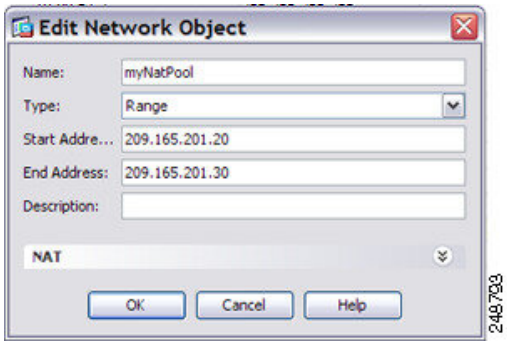


Étape 3 Activez la NAT dynamique pour le réseau interne.

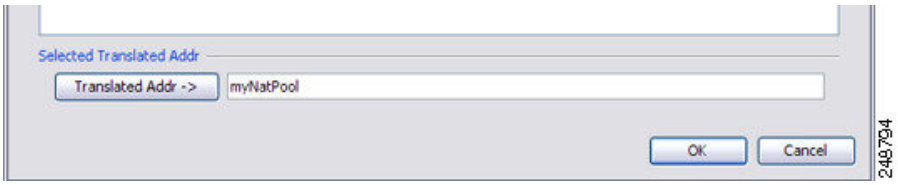


Étape 4 Pour le champ Translated Addr (adresse traduite), ajoutez un nouvel objet réseau pour le pool NAT dynamique vers lequel vous souhaitez traduire les adresses internes en cliquant sur le bouton Parcourir.

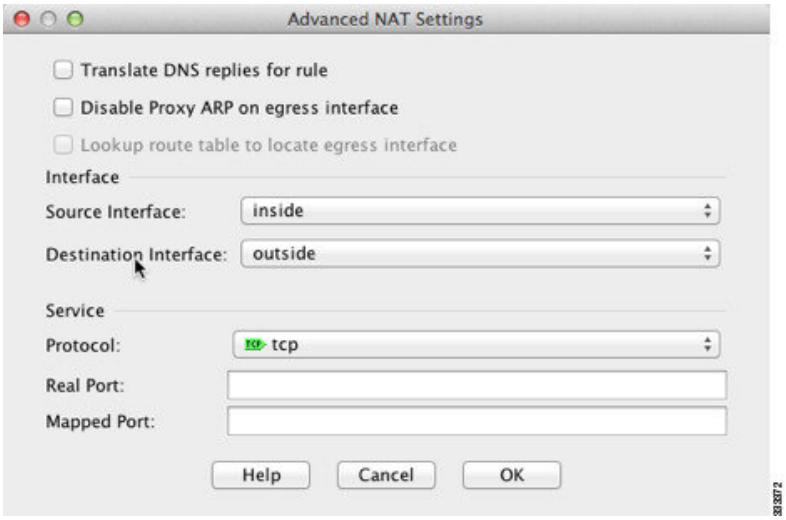
a) Choisissez **Add > Network Object** (Ajouter > Objet réseau), nommez le nouvel objet, définissez la plage d'adresses dans le pool NAT, puis cliquez sur **OK**.



b) Choisissez le nouvel objet réseau en double- cliquant dessus. Cliquez sur **OK** pour revenir à la configuration de la NAT.

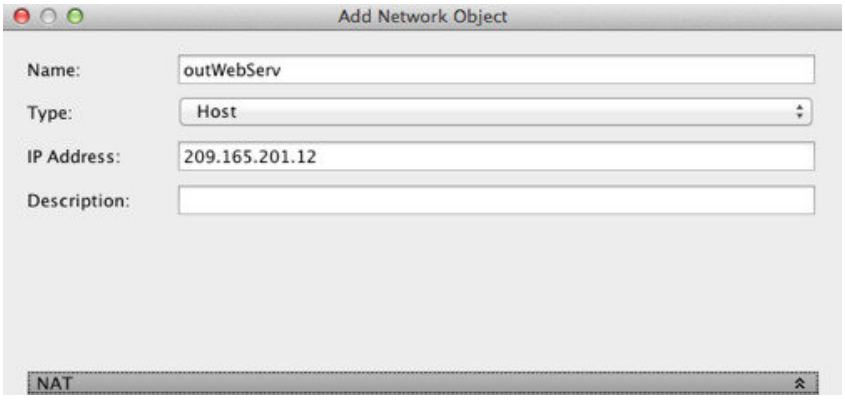


Étape 5 Cliquez sur **Advanced** (Avancé) et configurez les interfaces réelles et mappées.

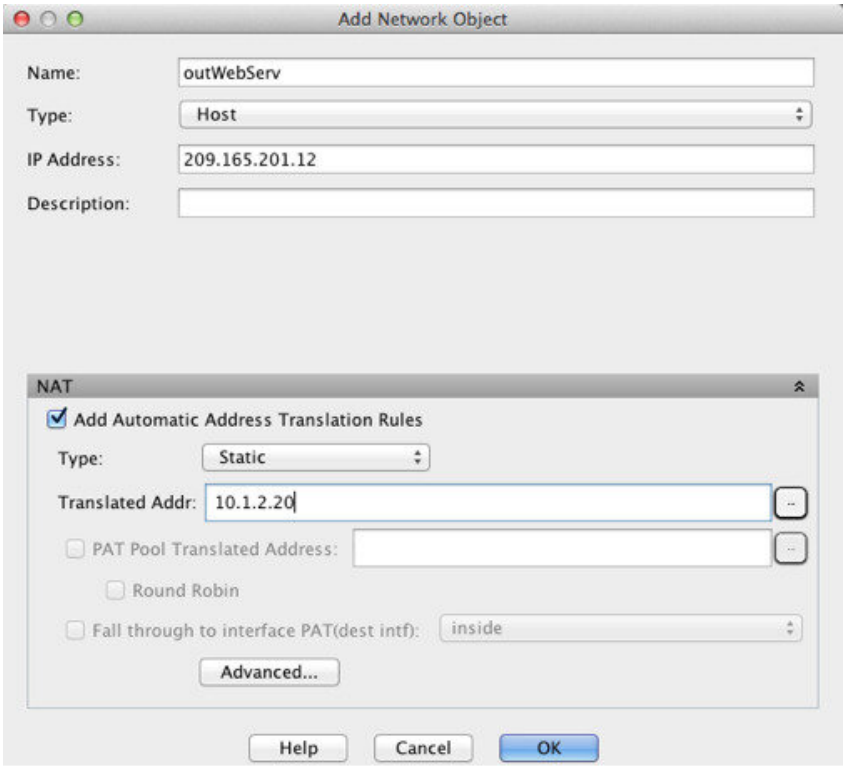


Étape 6 Cliquez sur **OK** pour revenir à la boîte de dialogue Edit Network Object (Modifier l'objet réseau), puis cliquez de nouveau sur **OK** (pour revenir au tableau NAT Rules (Règles NAT).

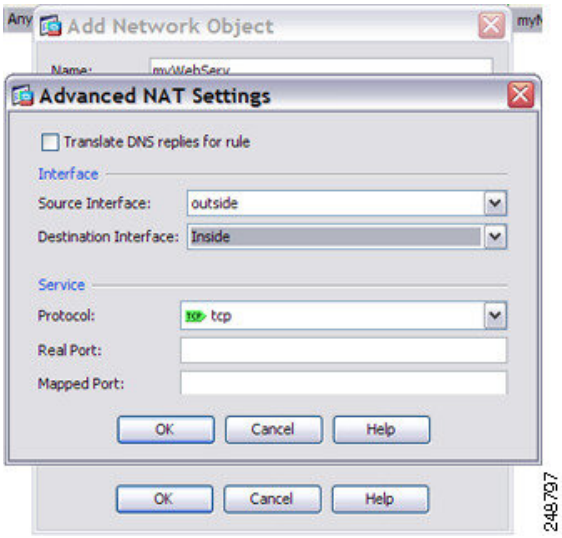
Étape 7 Choisissez **Add (Ajouter)** > **Network Object NAT Rule (Règle NAT d'objet réseau)** et créez un objet pour le serveur Web externe.



Étape 8 Configurez la NAT statique pour le serveur Web.



Étape 9 Cliquez sur **Advanced** (Avancé) et configurez les interfaces réelles et mappées.

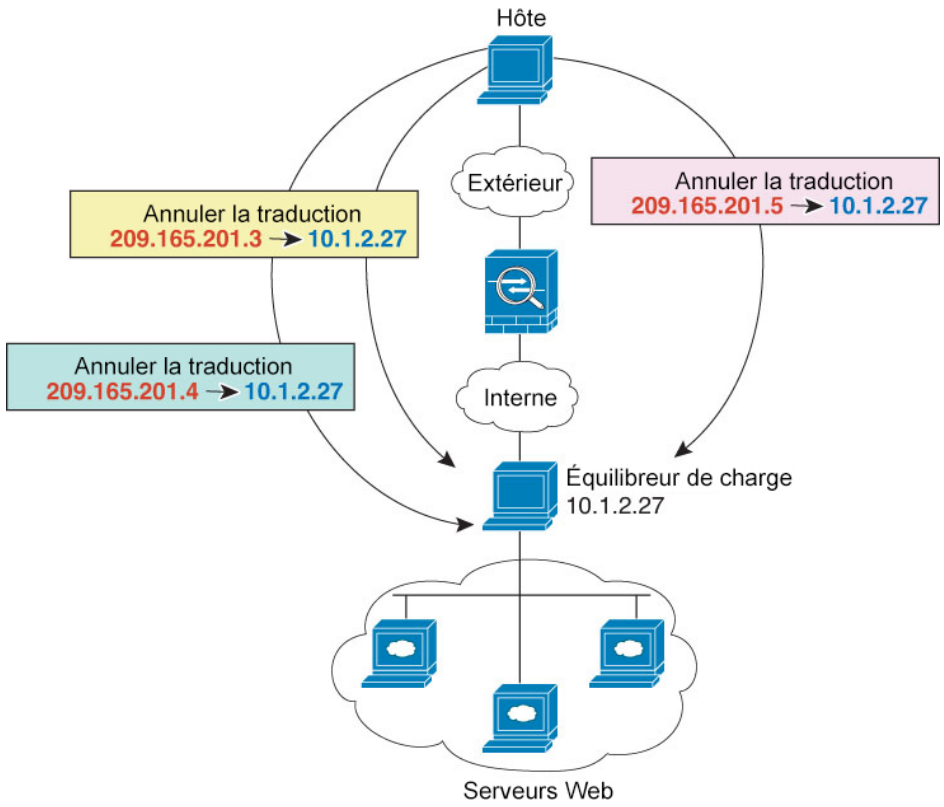


Étape 10 Cliquez sur **OK** pour revenir à la boîte de dialogue Edit Network Object (modifier l'objet de réseau), cliquez de nouveau sur **OK**, puis cliquez sur **Apply** (Appliquer).

Équilibreur de charge interne avec plusieurs adresses mappées (NAT statique, un à plusieurs)

L'exemple suivant montre un équilibreur de charge interne dont l'adresse est traduite en plusieurs adresses IP. Lorsqu'un hôte externe accède à l'une des adresses IP mappées, celle-ci n'est pas traduite en adresse unique de l'équilibreur de charge. Selon l'URL demandée, il redirige le trafic vers le bon serveur Web.

Illustration 20 : NAT statique avec règle One-to-Many (un vers plusieurs) pour un équilibreur de charge interne



Procédure

Étape 1 Choisissez **Configuration** > **Firewall** > **(Pare-feu)** > **NAT**.

Étape 2 Choisissez **Add** > **Network Object NAT Rule** (Ajouter > Règle NAT de l'objet réseau), nommez le nouvel objet réseau et définissez l'adresse de l'équilibreur de charge.

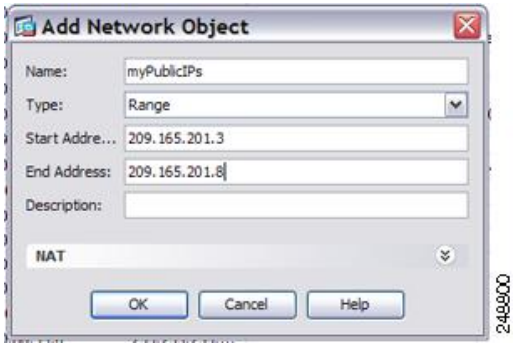


Étape 3 Activer la NAT statique pour l'équilibreur de charge :



Étape 4 Pour le champ Translated Addr, (adresse traduite) ajoutez un nouvel objet réseau pour le groupe d'adresses NAT statique vers lequel vous souhaitez traduire l'adresse de l'équilibreur de charge en cliquant sur le bouton Parcourir.

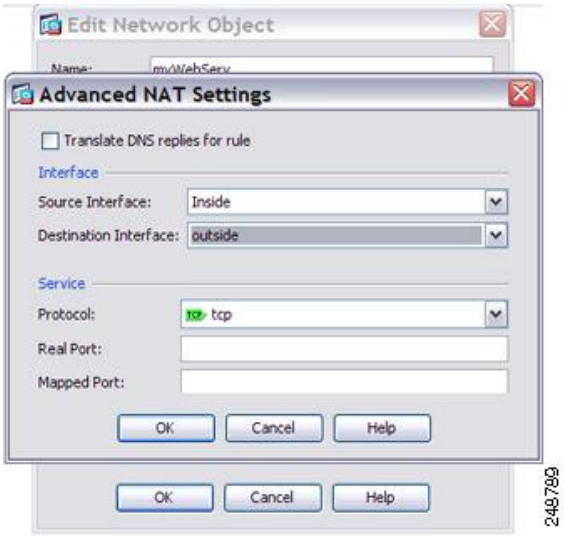
a) Choisissez **Add > Network Object** (Ajouter > Objet réseau), nommez le nouvel objet, définissez la plage d'adresses, puis cliquez sur **OK**.



b) Choisissez le nouvel objet réseau en double- cliquant dessus. Cliquez sur **OK** pour revenir à la configuration de la NAT.



Étape 5 Cliquez sur **Advanced** (Avancé) et configurez les interfaces réelles et mappées.

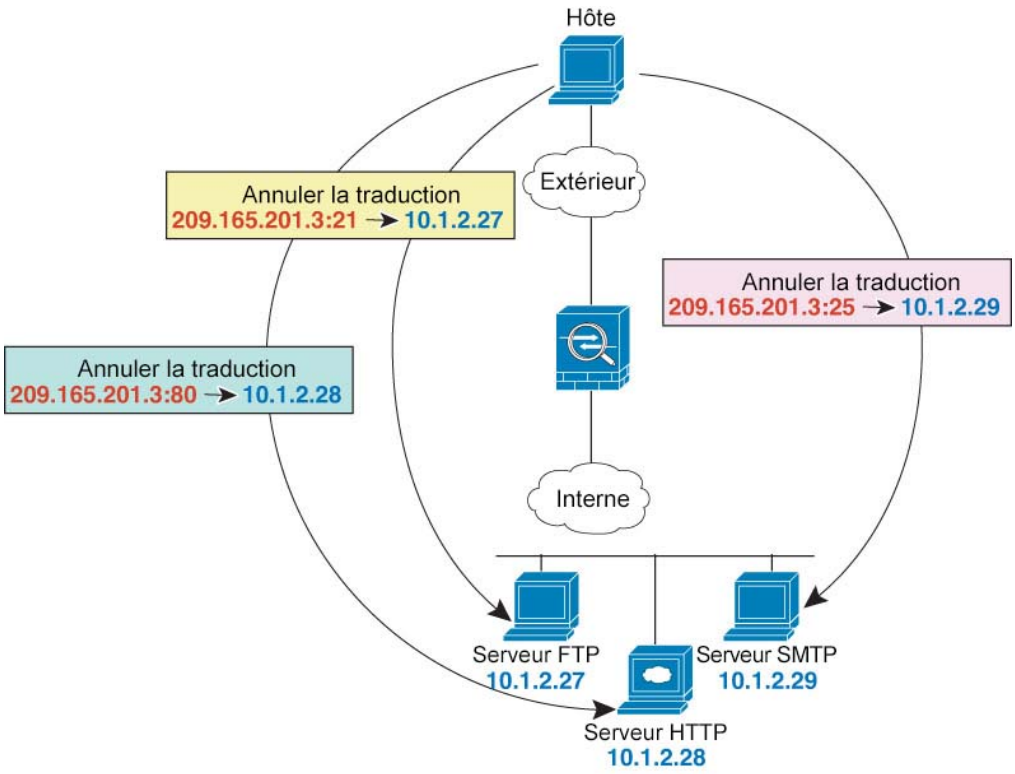


Étape 6 Cliquez sur **OK** pour revenir à la boîte de dialogue Edit Network Object (modifier l'objet de réseau), cliquez de nouveau sur **OK**, puis cliquez sur **Apply** (Appliquer).

Adresse unique pour FTP, HTTP et SMTP (NAT statique avec traduction de port)

L'exemple de NAT statique avec traduction de port 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.

Illustration 21 : NAT statique avec traduction de port



Procédure

Étape 1 Choisissez **Configuration** > **Firewall** > **(Pare-feu)** > **NAT**.

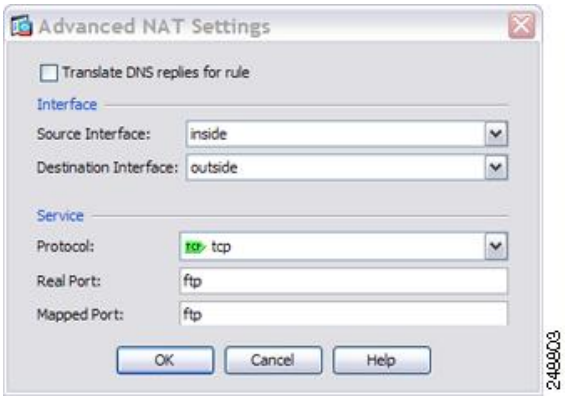
Étape 2 Configurez la NAT de l'objet de réseau statique avec la règle de traduction de port pour le serveur FTP.

a) Choisissez **Add > Network Object NAT Rule** (Ajouter > Règle NAT d'objet réseau).

b) Nommez le nouvel objet réseau, définissez l'adresse du serveur FTP, activez la NAT statique et saisissez l'adresse traduite.



c) Cliquez sur **Advanced** (Avancé) et configurez les interfaces réelles et mappées ainsi que la traduction de port pour FTP, en mappant le port FTP sur lui-même.



d) Cliquez sur **OK**, puis à nouveau sur **OK** pour enregistrer la règle et revenir à la page NAT.

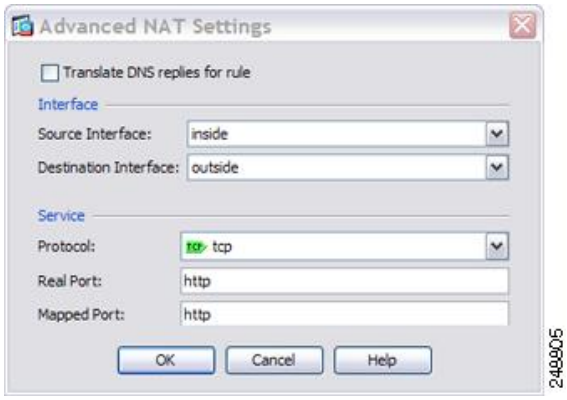
Étape 3 Configurez la NAT de l'objet de réseau statique avec la règle de traduction de port pour le serveur HTTP.

a) Choisissez **Add > Network Object NAT Rule** (Ajouter > Règle NAT d'objet réseau).

b) Nommez le nouvel objet réseau, définissez l'adresse du serveur HTTP, activez la NAT statique et saisissez l'adresse traduite.



c) Cliquez sur **Advanced** (Avancé) et configurez les interfaces réelles et mappées ainsi que la traduction de port pour HTTP, en mappant le port HTTP sur lui-même.



d) Cliquez sur **OK**, puis à nouveau sur **OK** pour enregistrer la règle et revenir à la page NAT.

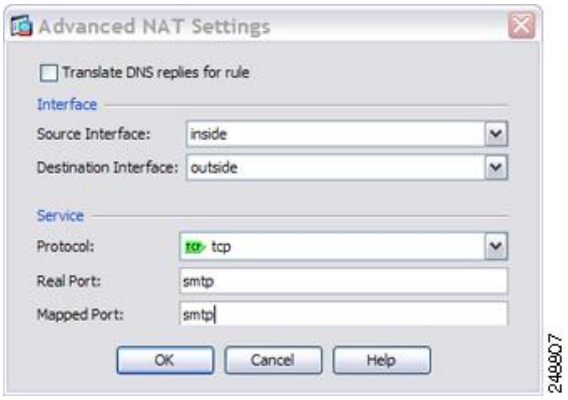
Étape 4 Configurez la NAT de l'objet de réseau statique avec la règle de traduction de port pour le serveur SMTP.

a) Choisissez **Add > Network Object NAT Rule** (Ajouter > Règle NAT d'objet réseau).

b) Nommez le nouvel objet réseau, définissez l'adresse du serveur SMTP, activez la NAT statique et saisissez l'adresse traduite.



c) Cliquez sur **Advanced** (Avancé) et configurez les interfaces réelles et mappées ainsi que la traduction de port pour SMTP, en mappant le port SMTP sur lui-même.



d) Cliquez sur **OK** pour revenir à la boîte de dialogue Edit Network Object (modifier l'objet de réseau), cliquez de nouveau sur **OK**, puis cliquez sur **Apply** (Appliquer).

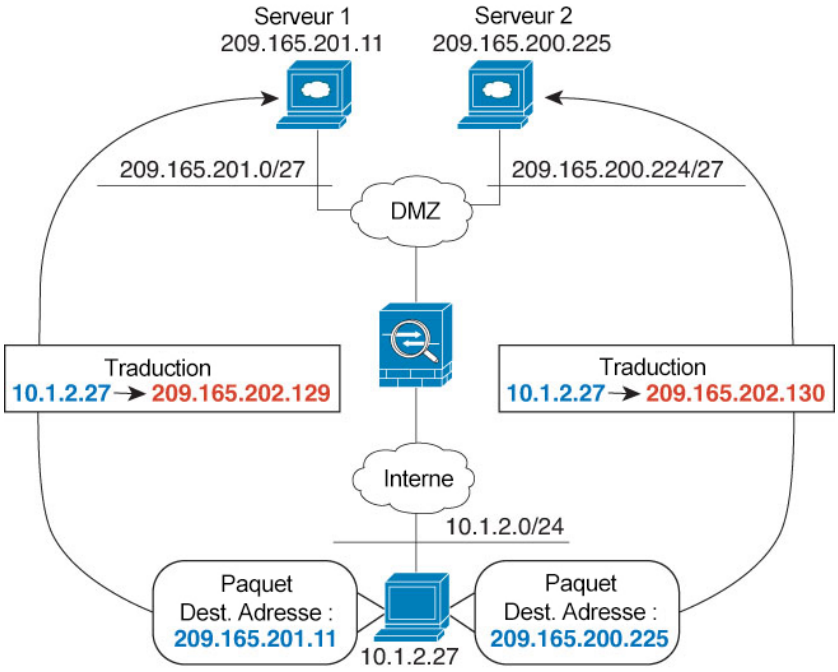
Exemples relatifs à la NAT Twice

Cette section inclut les exemples de configuration suivants :

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 209.165.202.130 :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.

Illustration 22 : NAT manuelle avec différentes adresses de destination

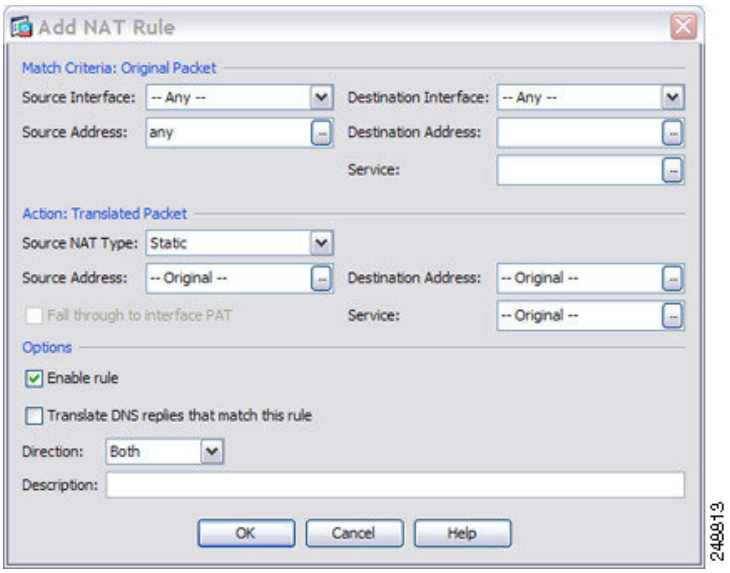


Procédure

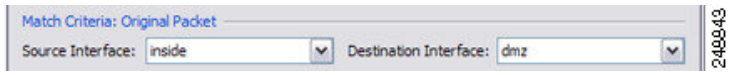
Étape 1 Sur la page **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)**, cliquez sur **Add (Ajouter)** > **Add NAT Rule Before Network Object NAT Rules (Ajouter une règle NAT avant les règles NAT d'objet réseau)** pour ajouter une règle NAT pour le trafic du réseau interne vers le réseau DMZ 1.

Si vous souhaitez ajouter une règle NAT à la section 3, après les règles NAT d'objet réseau, choisissez **Add NAT Rule After Network Object NAT Rules** (Ajouter une règle NAT après les règles NAT d'objet réseau).

La boîte de dialogue Add NAT Rule (ajouter une règle NAT) apparaît.



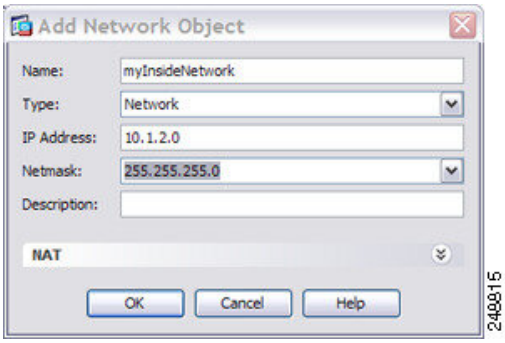
Étape 2 Définissez les interfaces de source et de destination.



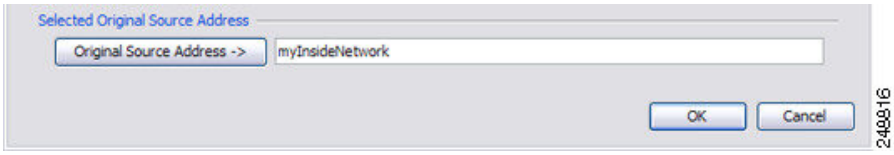
Étape 3 Pour Original Source Address (Adresse source d'origine), cliquez sur le bouton de navigation pour ajouter un nouvel objet réseau pour le réseau interne dans la boîte de dialogue Browse Original Source Address (Parcourir l'adresse source d'origine).

a) Sélectionnez **Add (Ajouter) > Network Object (Objet réseau)**.

b) Définissez les adresses de réseau internes, puis cliquez sur **OK**.



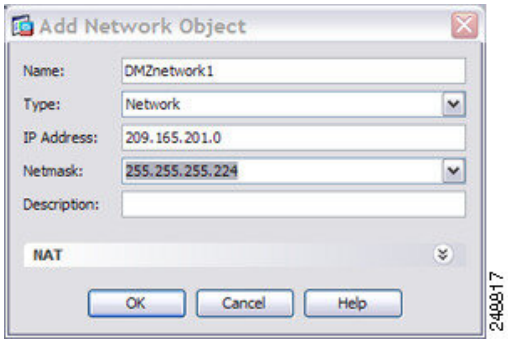
c) Choisissez le nouvel objet réseau en double- cliquant dessus. Cliquez sur **OK** pour revenir à la configuration de la NAT.



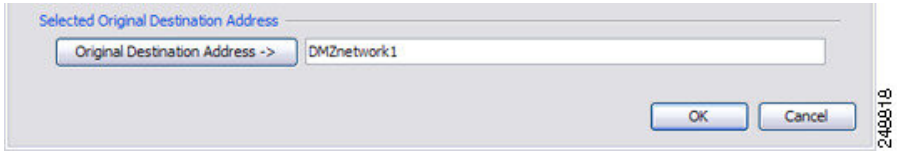
Étape 4 Pour Original Destination Address (Adresse de destination d'origine), cliquez sur le bouton de navigation pour ajouter un nouvel objet réseau pour le réseau DMZ 1 dans la boîte de dialogue Browse Original Destination Address (Parcourir l'adresse de destination d'origine).

a) Sélectionnez **Add (Ajouter) > Network Object (Objet réseau)**

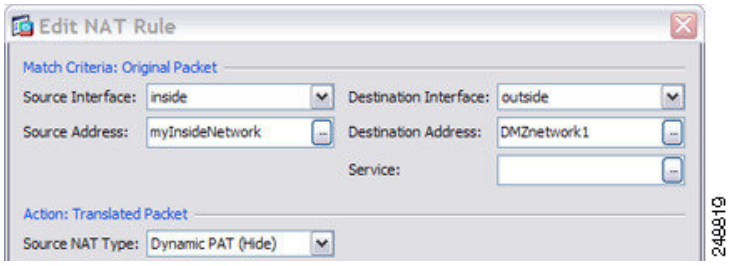
b) Définissez les adresses du réseau DMZ 1, puis cliquez sur **OK**.



c) Choisissez le nouvel objet réseau en double- cliquant dessus. Cliquez sur **OK** pour revenir à la configuration de la NAT.



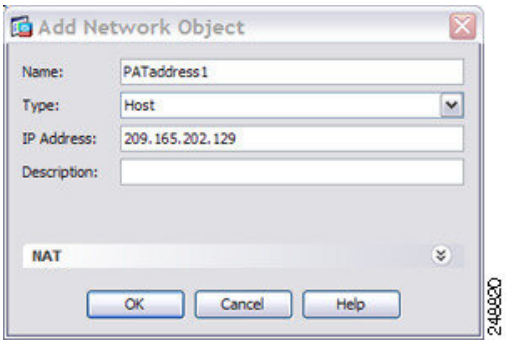
Étape 5 Définissez NAT Type (Type de NAT) sur **Dynamic PAT (Hide) (PAT dynamique [Masquer])** :



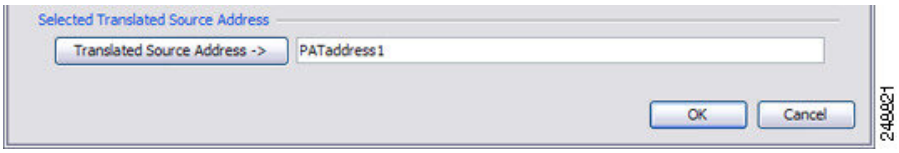
Étape 6 Pour Translated Source Address (Adresse source traduite), cliquez sur le bouton de navigation pour ajouter un nouvel objet réseau pour l'adresse PAT dans la boîte de dialogue Browse Translated Source Address (Parcourir l'adresse source traduite).

a) Sélectionnez **Add (Ajouter) > Network Object (Objet réseau)**

b) Définissez l'adresse PAT, puis cliquez sur **OK**.

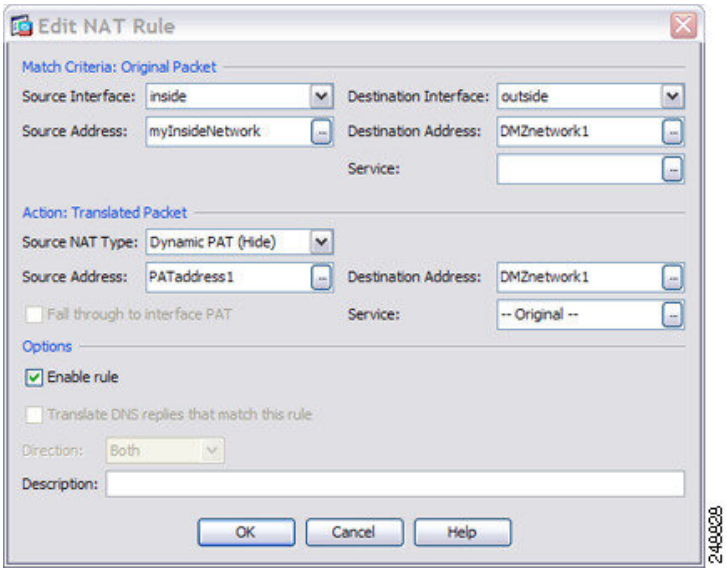


c) Choisissez le nouvel objet réseau en double- cliquant dessus. Cliquez sur **OK** pour revenir à la configuration de la NAT.



Étape 7 Pour Translated Destination Address (Adresse de destination traduite), saisissez le nom indiqué dans Original Destination Address (Adresse de destination d'origine) (DMZnetwork1) ou cliquez sur le bouton de navigation pour la sélectionner.

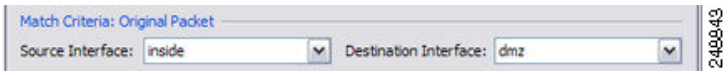
Comme vous ne souhaitez pas traduire l'adresse de destination, vous devez configurer la NAT d'identité en utilisant la même adresse pour les adresses de destination originale et traduite.



Étape 8 Cliquez sur **OK** pour ajouter la règle à la table NAT.

Étape 9 Cliquez sur **Add (Ajouter)** > **Add NAT Rule Before Network Object NAT Rules (Ajouter une règle NAT avant les règles NAT d'objet réseau)** ou sur **Add NAT Rule After Network Object NAT Rules (Ajouter une règle NAT après les règles NAT d'objet réseau)** pour ajouter une règle NAT pour le trafic du réseau interne vers le réseau DMZ 2.

Étape 10 Définissez les interfaces de source et de destination.

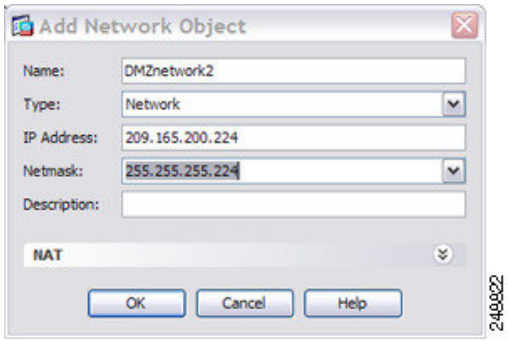


Étape 11 Pour Original Source Address (Adresse source d'origine), saisissez le nom de l'objet réseau interne (myInsideNetwork) ou cliquez sur le bouton de navigation pour le sélectionner.

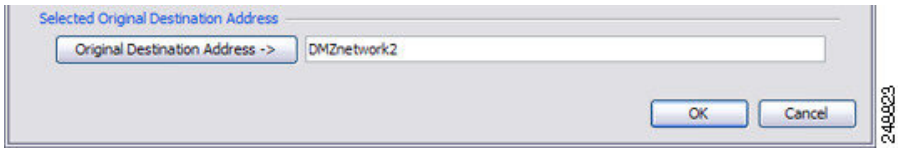
Étape 12 Pour Original Destination Address (Adresse de destination d'origine), cliquez sur le bouton de navigation pour ajouter un nouvel objet réseau pour le réseau DMZ 2 dans la boîte de dialogue Browse Original Destination Address (Parcourir l'adresse de destination d'origine).

a) Sélectionnez **Add (Ajouter) > Network Object (Objet réseau)**

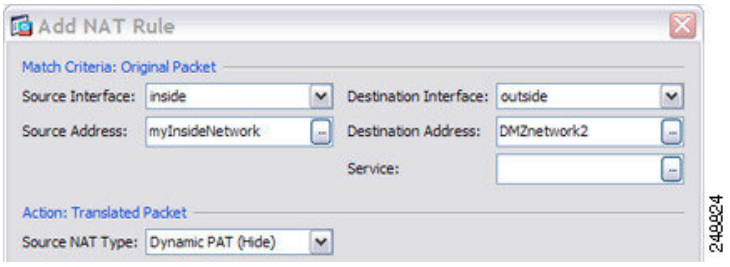
b) Définissez les adresses du réseau DMZ 2, puis cliquez sur **OK**.



c) Choisissez le nouvel objet réseau en double- cliquant dessus. Cliquez sur **OK** pour revenir à la configuration de la NAT.



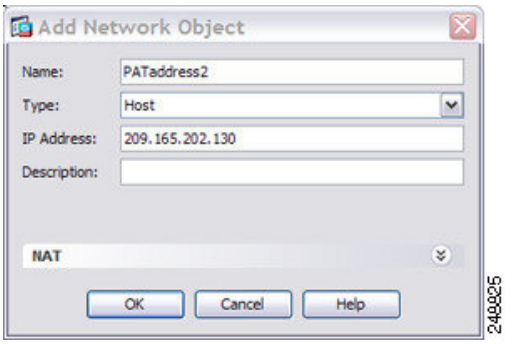
Étape 13 Définissez NAT Type (Type de NAT) sur **Dynamic PAT (Hide) (PAT dynamique [Masquer])** :



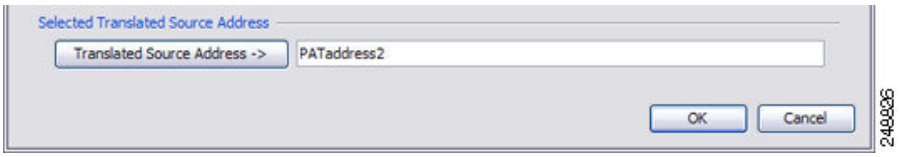
Étape 14 Pour Translated Source Address (Adresse source traduite), cliquez sur le bouton de navigation pour ajouter un nouvel objet réseau pour l'adresse PAT dans la boîte de dialogue Browse Translated Source Address (Parcourir l'adresse source traduite).

a) Sélectionnez **Add (Ajouter) > Network Object (Objet réseau)**

b) Définissez l'adresse PAT, puis cliquez sur **OK**.

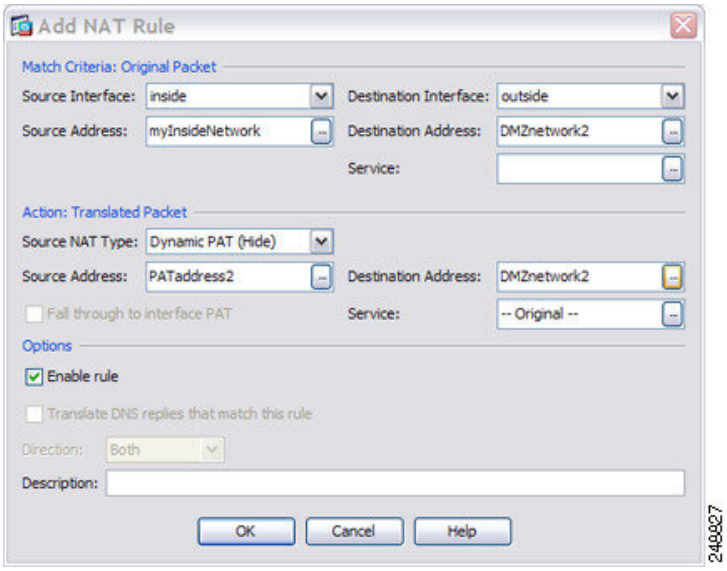


c) Choisissez le nouvel objet réseau en double- cliquant dessus. Cliquez sur **OK** pour revenir à la configuration de la NAT.



Étape 15 Pour Translated Destination Address (Adresse de destination traduite), saisissez le nom indiqué dans Original Destination Address (Adresse de destination d'origine) (DMZnetwork2) ou cliquez sur le bouton de navigation pour la sélectionner.

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.



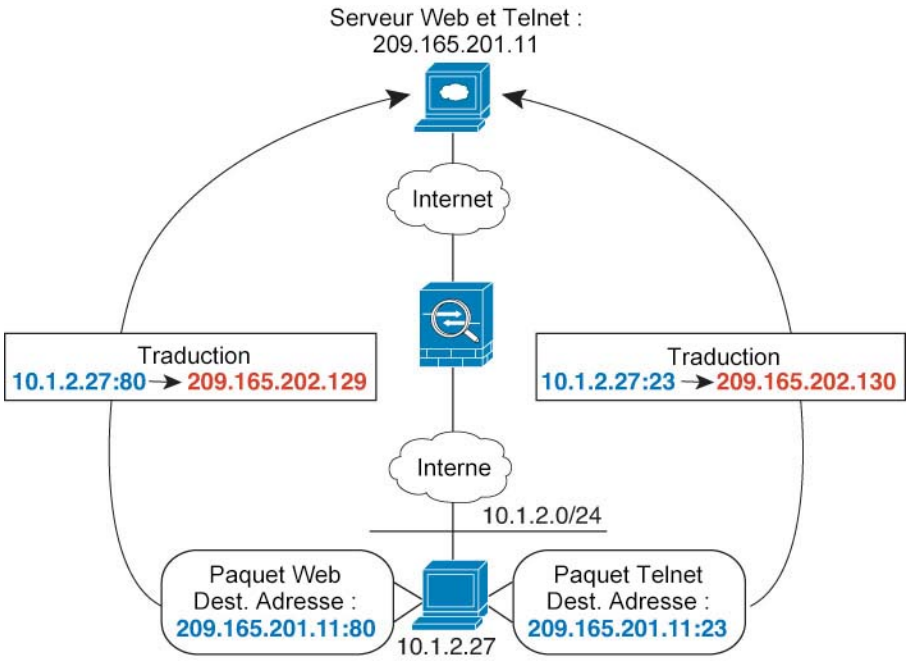
Étape 16 Cliquez sur **OK** pour ajouter la règle à la table NAT.

Étape 17 Cliquez sur **Apply** (Appliquer).

Traduction différente selon l'adresse et le port de destination (PAT 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 209.165.202.130 :port. Lorsque l'hôte accède au même serveur pour les services Web, l'adresse réelle est traduite par 209.165.202.130 :port.

Illustration 23 : NAT Twice avec différents ports de destination

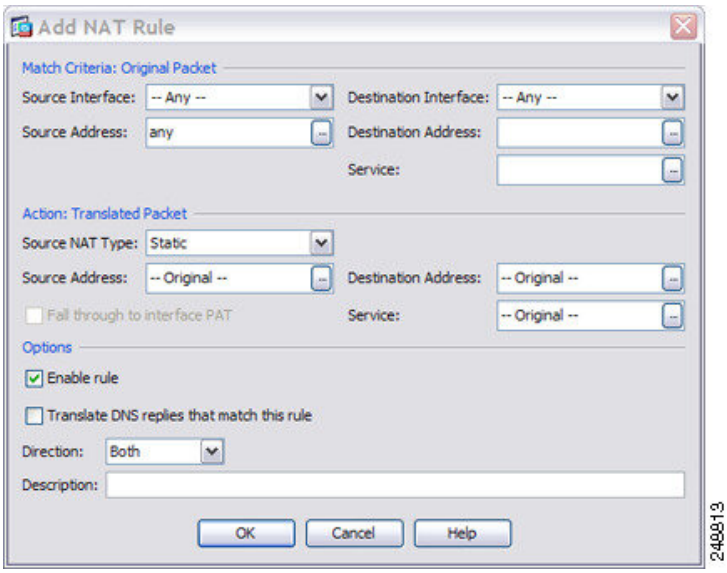


Procédure

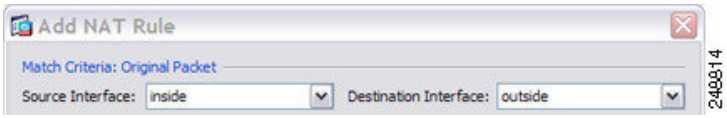
Étape 1 Sur la page **Configuration** > **Firewall (Pare-feu)** > **NAT Rules (Règles NAT)**, cliquez sur **Add (Ajouter)** > **Add NAT Rule Before Network Object NAT Rules (Ajouter une règle NAT avant les règles NAT d'objet réseau)** pour ajouter une règle NAT pour le trafic du réseau interne vers le réseau Telnet.

Si vous souhaitez ajouter une règle NAT à la section 3, après les règles NAT d'objet réseau, choisissez **Add NAT Rule After Network Object NAT Rules** (Ajouter une règle NAT après les règles NAT d'objet réseau).

La boîte de dialogue Add NAT Rule (ajouter une règle NAT) apparaît.



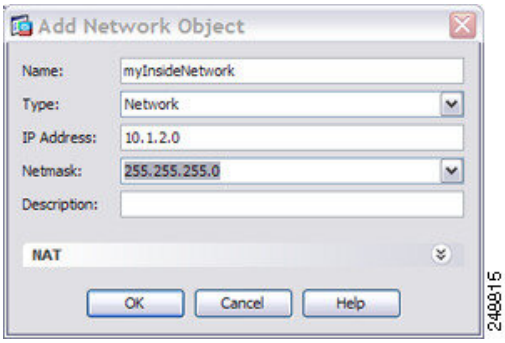
Étape 2 Définissez les interfaces source et destination.



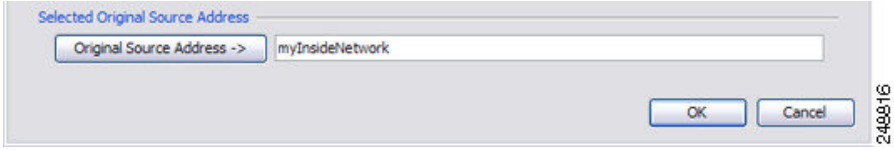
Étape 3 Pour Original Source Address (Adresse source d'origine), cliquez sur le bouton de navigation pour ajouter un nouvel objet réseau pour le réseau interne dans la boîte de dialogue Browse Original Source Address (Parcourir l'adresse source d'origine).

a) Sélectionnez **Add (Ajouter) > Network Object (Objet réseau)**

b) Définissez les adresses de réseau internes, puis cliquez sur **OK**.



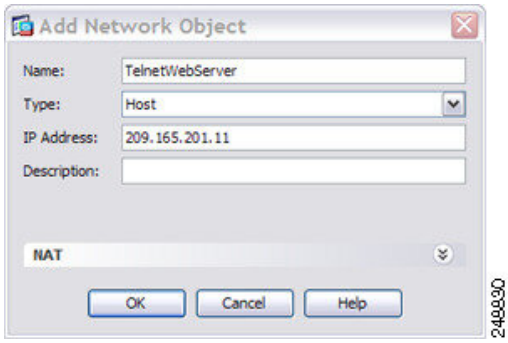
c) Choisissez le nouvel objet réseau en double- cliquant dessus. Cliquez sur **OK** pour revenir à la configuration de la NAT.



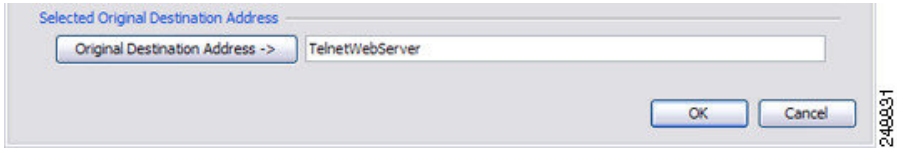
Étape 4 Pour Original Destination Address (Adresse de destination d'origine), cliquez sur le bouton de navigation pour ajouter un nouvel objet réseau pour le serveur Telnet/Web dans la boîte de dialogue Browse Original Destination Address (Parcourir l'adresse de destination d'origine).

a) Sélectionnez **Add (Ajouter) > Network Object (Objet réseau)**

b) Définissez l'adresse du serveur, puis cliquez sur **OK**.



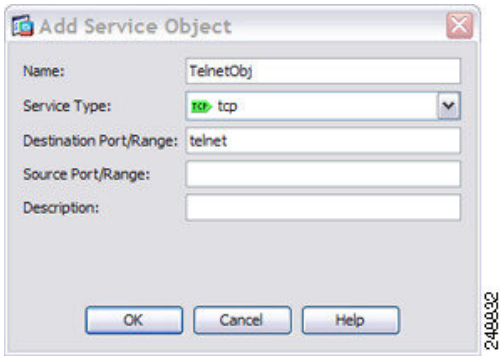
c) Choisissez le nouvel objet réseau en double- cliquant dessus. Cliquez sur **OK** pour revenir à la configuration de la NAT.



Étape 5 Pour Original Service (Service d'origine), cliquez sur le bouton de navigation pour ajouter un nouvel objet de service pour Telnet dans la boîte de dialogue Browse Original Service (Parcourir le service d'origine).

a) Sélectionnez **Add (Ajouter) > Service Object (Objet de service)**.

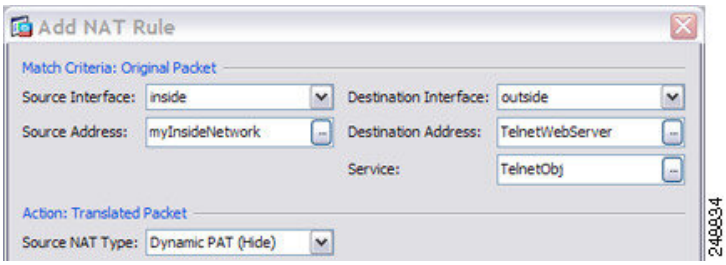
b) Définissez le protocole et le port, puis cliquez sur **OK**.



c) Choisissez le nouvel objet de service en double-cliquant dessus. Cliquez sur **OK** pour revenir à la configuration de la NAT.



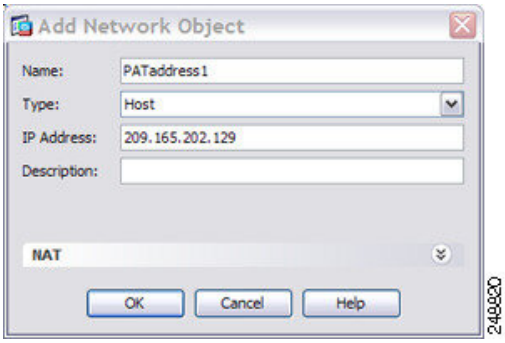
Étape 6 Définissez NAT Type (Type de NAT) sur **Dynamic PAT (Hide) (PAT dynamique [Masquer])** :



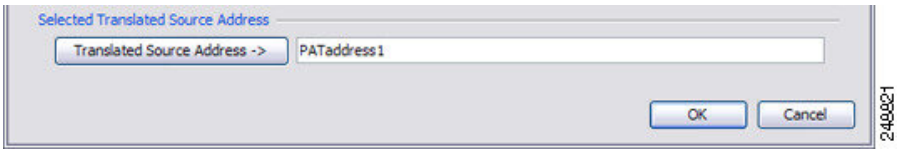
Étape 7 Pour Translated Source Address (Adresse source traduite), cliquez sur le bouton de navigation pour ajouter un nouvel objet réseau pour l'adresse PAT dans la boîte de dialogue Browse Translated Source Address (Parcourir l'adresse source traduite).

a) Sélectionnez **Add (Ajouter) > Network Object (Objet réseau)**

b) Définissez l'adresse PAT, puis cliquez sur **OK**.

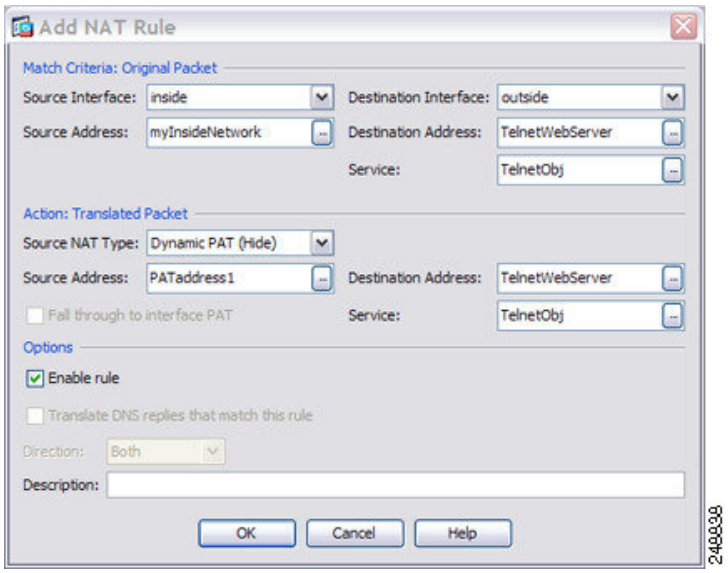


c) Choisissez le nouvel objet réseau en double- cliquant dessus. Cliquez sur **OK** pour revenir à la configuration de la NAT.



Étape 8 Pour Translated Destination Address (Adresse de destination traduite), saisissez le nom indiqué dans Original Destination Address (Adresse de destination d'origine) (TelnetWebServer) ou cliquez sur le bouton de navigation pour la sélectionner.

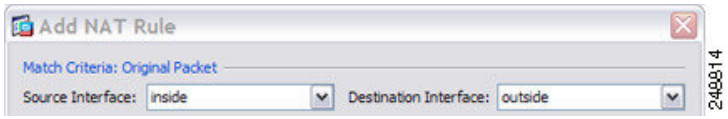
Comme vous ne souhaitez pas traduire l'adresse de destination, vous devez configurer la NAT d'identité en utilisant la même adresse pour les adresses de destination originale et traduite.



Étape 9 Cliquez sur **OK** pour ajouter la règle au tableau NAT.

Étape 10 Cliquez sur **Add (Ajouter)** > **Add NAT Rule Before Network Object NAT Rules (Ajouter une règle NAT avant les règles NAT d'objet réseau)** ou sur **Add NAT Rule After Network Object NAT Rules (Ajouter une règle NAT après les règles NAT d'objet réseau)** pour ajouter une règle NAT pour le trafic du réseau interne vers le serveur Web.

Étape 11 Définissez les interfaces réelles et mappées.



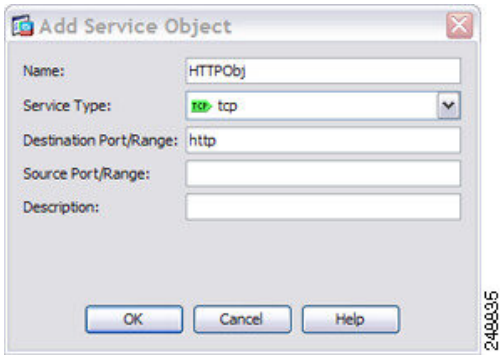
Étape 12 Pour l'adresse source d'origine, saisissez le nom de l'objet réseau interne (myInsideNetwork) ou cliquez sur le bouton de navigation pour le sélectionner.

Étape 13 Pour l'adresse de destination d'origine, saisissez le nom de l'objet réseau Telnet/serveur Web (TelnetWebServer) ou cliquez sur le bouton de navigation pour le sélectionner.

Étape 14 Pour Original Service (Service d'origine), cliquez sur le bouton de navigation pour ajouter un nouvel objet de service pour HTTP dans la boîte de dialogue Browse Original Service (Parcourir le service d'origine).

a) Sélectionnez **Add (Ajouter) > Service Object (Objet de service)**.

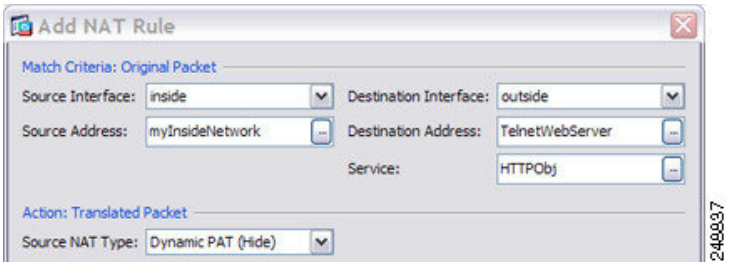
b) Définissez le protocole et le port, puis cliquez sur **OK**.



c) Choisissez le nouvel objet de service en double-cliquant dessus. Cliquez sur **OK** pour revenir à la configuration de la NAT.



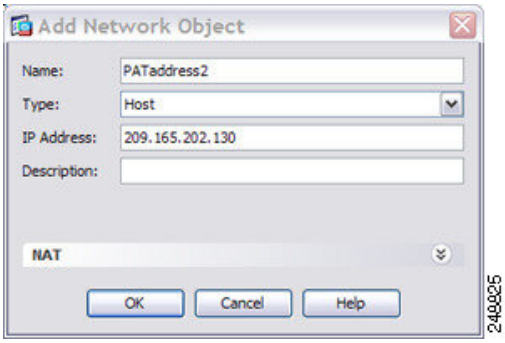
Étape 15 Définissez NAT Type (Type de NAT) sur **Dynamic PAT (Hide) (PAT dynamique [Masquer])** :



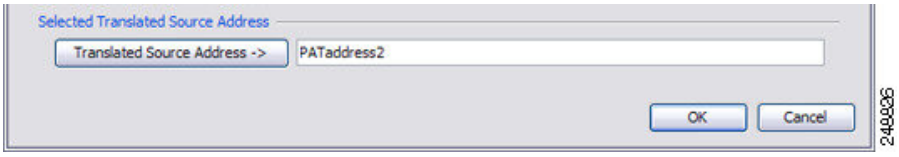
Étape 16 Pour Translated Source Address (Adresse source traduite), cliquez sur le bouton de navigation pour ajouter un nouvel objet réseau pour l'adresse PAT dans la boîte de dialogue Browse Translated Source Address (Parcourir l'adresse source traduite).

a) Sélectionnez **Add (Ajouter) > Network Object (Objet réseau)**

b) Définissez l'adresse PAT, puis cliquez sur **OK**.

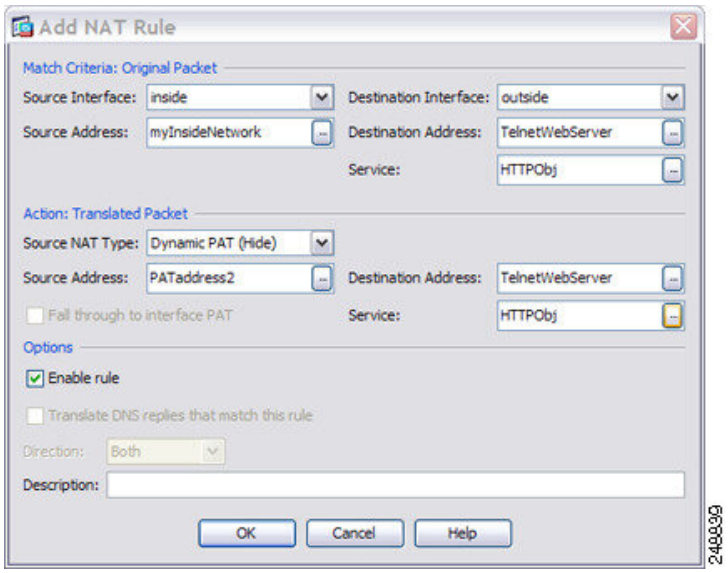


c) Choisissez le nouvel objet réseau en double- cliquant dessus. Cliquez sur **OK** pour revenir à la configuration de la NAT.



Étape 17 Pour Translated Destination Address (Adresse de destination traduite), saisissez le nom indiqué dans Original Destination Address (Adresse de destination d'origine) (TelnetWebServer) ou cliquez sur le bouton de navigation pour la sélectionner.

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.



Étape 18 Cliquez sur **OK** pour ajouter la règle à la table NAT.

Étape 19 Cliquez sur **Apply** (Appliquer).

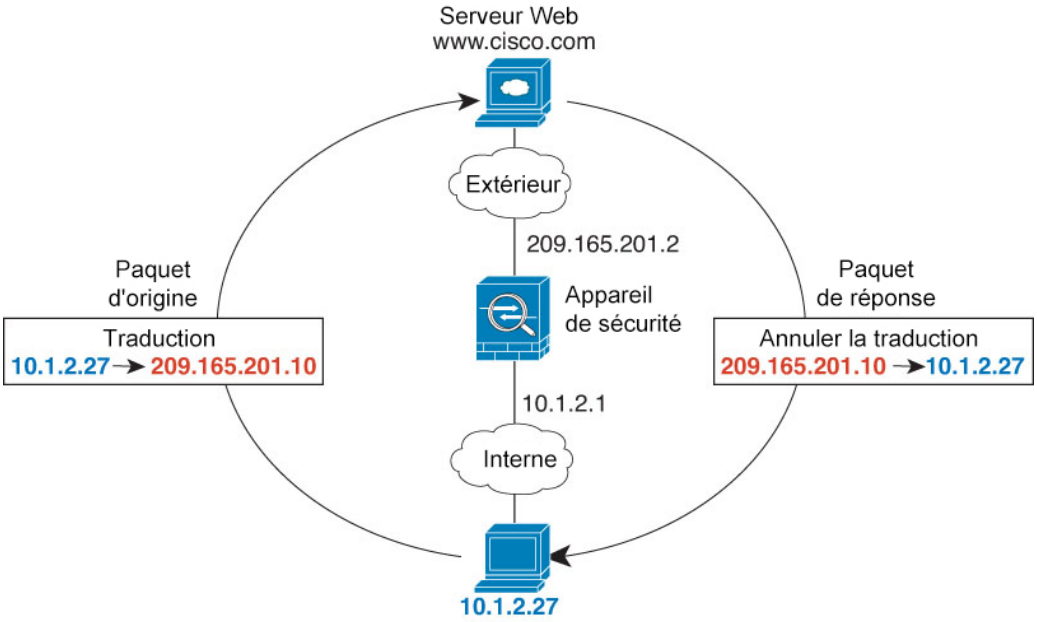
NAT en mode routé et transparent

Vous pouvez configurer la NAT en mode de pare-feu routé et transparent. Les sections suivantes décrivent l'utilisation typique de chaque mode de pare-feu.

NAT en mode routé

La figure suivante montre un exemple de NAT typique en mode routé, avec un réseau privé à l'intérieur.

Illustration 24 : 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'ASA reçoit le paquet, car l'ASA effectue un ARP mandataire pour réclamer le paquet.
3. L'ASA 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 en mode transparent ou dans un groupe de pont

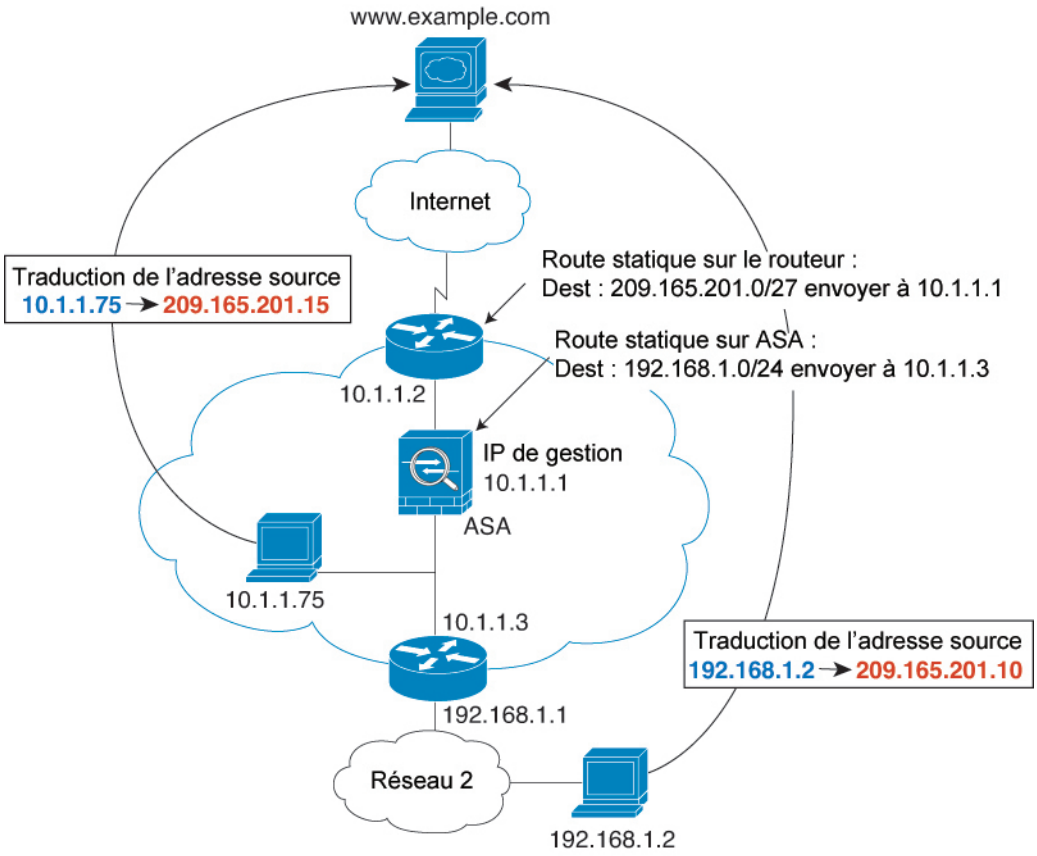
L'utilisation de la NAT en mode transparent élimine le besoin pour les routeurs en amont ou en aval d'effectuer la NAT pour leurs réseaux. Il peut remplir une fonction similaire dans un groupe de ponts en mode routé.

La NAT en mode transparent, ou en mode routé entre les membres d'un même groupe de ponts, comporte les exigences et les limites suivantes :

- Vous ne pouvez pas configurer l'interface PAT lorsque l'adresse mappée est une interface de membre d'un groupe de ponts, car aucune adresse IP n'est associée à l'interface.
- L'inspection ARP n'est pas prise en charge. De plus, si, pour une raison quelconque, un hôte de l'un des côtés de l'ASA envoie une requête ARP à un hôte de l'autre côté de l'ASA et que l'adresse réelle de l'hôte initiateur est mappée à une adresse différente sur le même sous-réseau, l'adresse réelle reste visible dans la requête ARP.
- La traduction entre des réseaux IPv4 et IPv6 n'est pas prise en charge. La traduction entre deux réseaux IPv6 ou entre deux réseaux IPv4 est prise en charge.

La figure suivante montre un scénario NAT typique en mode transparent, avec le même réseau sur les interfaces interne et externe. Le pare-feu transparent dans ce scénario effectue le service NAT, de sorte que le routeur en amont n'a pas à effectuer de NAT.

Illustration 25 : Exemple NAT : mode transparent



1. Lorsque l'hôte interne en 10.1.1.75 envoie un paquet à un serveur Web, l'adresse source réelle du paquet, 10.1.1.75, est remplacée par une adresse mappée, 209.165.201.15.
2. Lorsque le serveur répond, il envoie la réponse à l'adresse mappée, 209.165.201.15, et l'ASA reçoit le paquet, car le routeur en amont inclut ce réseau mappé dans une voie de routage statique dirigée vers l'adresse IP de gestion ASA.
3. L'ASA annule ensuite la traduction de l'adresse mappée, 209.165.201.15, vers l'adresse réelle, 10.1.1.75. Comme l'adresse réelle est directement connectée, l'ASA l'envoie directement à l'hôte.
4. Pour l'hôte 192.168.1.2, le même processus se produit, sauf pour le trafic de retour, l'ASA recherche la route dans sa table de routage et envoie le paquet au routeur en aval à l'adresse 10.1.1.3 en fonction de la route statique ASA pour 192.168.1.0/24.

Routage des paquets NAT

L'ASA doit être la destination de tous les paquets envoyés à l'adresse mappée. L'ASA doit également déterminer l'interface de sortie de tous les paquets qu'il reçoit et qui sont destinés aux adresses mappées. Cette section décrit comment l'ASA gère l'acceptation et la livraison des paquets avec la NAT.

Adresses mappées et routage

Lorsque vous traduisez l'adresse réelle en adresse mappée, l'adresse mappée que vous choisissez détermine comment configurer le routage, le cas échéant, pour l'adresse mappée.

Consultez les lignes directrices supplémentaires concernant les adresses IP mappées dans Lignes directrices supplémentaires pour la NAT, à la page 129.

Les rubriques suivantes expliquent les types d'adresses mappées.

Adresses sur le même réseau que l'interface mappée

Si vous utilisez des adresses sur le même réseau que l'interface mappée, l'ASA utilise 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 l'ASA 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.

Remarque Si vous configurez l'interface mappée sur n'importe quelle interface et que vous spécifiez une adresse mappée sur le même réseau que l'une des interfaces mappées, si une requête ARP pour cette adresse mappée arrive sur une interface *différente*, vous devez configurer manuellement une entrée ARP pour ce réseau sur l'interface d'entrée, en précisant son adresse MAC. En règle générale, si vous spécifiez une interface pour l'interface mappée, vous utilisez un réseau unique pour les adresses mappées, cette situation ne se produit donc pas. Sélectionnez **Configuration** > **Device Management** > **Advanced** > **ARP** > **ARP Static Table** (Périphériques > Gestion des périphériques > Avancé > ARP > Tableau statique ARP) pour configurer ARP.

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 ASA.

Sinon, pour le mode routé, vous pouvez configurer une voie de routage statique sur ASA pour les adresses mappées en utilisant n'importe quelle adresse IP du réseau de destination comme passerelle, puis redistribuer la voie de routage en utilisant votre protocole de routage. Par exemple, si vous utilisez la NAT pour le réseau interne (10.1.1.0/24) et que vous utilisez l'adresse IP mappée 209.165.201.5, vous pouvez configurer une voie de routage statique pour 209.165.201.5 255.255.255.255 (adresse de l'hôte) vers le périphérique 10.165.201.5. Passerelle 1.99 qui peut être redistribuée.

```
route inside 209.165.201.5 255.255.255.255 10.1.1.99
```

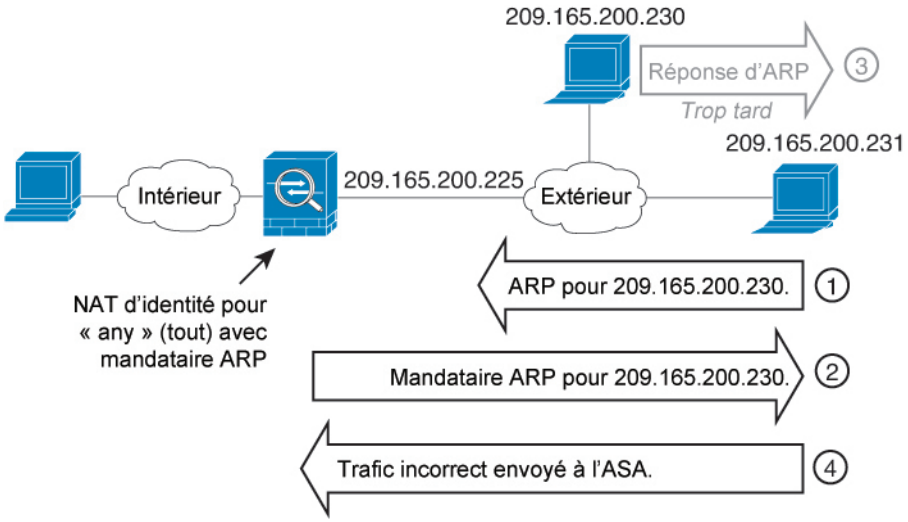
Pour le mode transparent, si l'hôte réel est connecté directement, configurez la route statique sur le routeur en amont pour pointer vers ASA : spécifiez l'adresse IP du groupe de ponts. Pour les hôtes distants en mode transparent, dans la voie de routage statique sur le routeur en amont, vous pouvez également spécifier l'adresse IP du routeur en aval.

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.

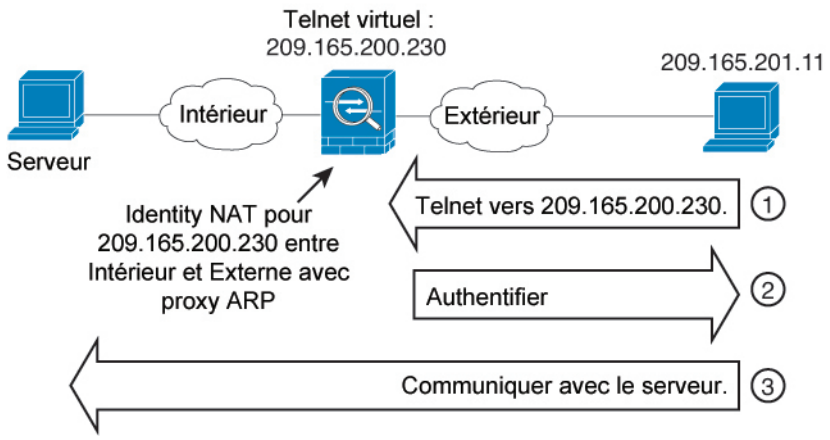
Normalement, pour la NAT d'identité, la technique proxy ARP n'est pas requise et peut même, dans certains cas, entraîner des problèmes de connectivité. Par exemple, si vous configurez une règle NAT d'identité large pour « n'importe quelle » adresse IP, laisser le mandataire ARP activé peut entraîner 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'ASA répondra alors à la requête ARP par un serveur mandataire pour l'adresse, même si le paquet n'est pas réellement destiné à ASA. (Notez que ce problème se produit même si vous avez une règle twice NAT (NAT en double) ; 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 de l'ASA est reçue avant la réponse effective ARP de l'hôte, le trafic sera envoyé par erreur vers ASA.

Illustration 26 : Problèmes de mandataire ARP avec la NAT d'identité



Dans de rares cas, vous avez besoin d'un ARP mandataire pour la NAT d'identité; par exemple pour le Telnet virtuel. Lors de l'utilisation de l'AAA pour l'accès au réseau, un hôte doit s'authentifier auprès de l'ASA à l'aide d'un service tel que Telnet avant que tout autre trafic ne puisse être transmis. Vous pouvez configurer un serveur Telnet virtuel sur l'ASA pour fournir les informations de connexion nécessaires. Lorsque vous accédez à l'adresse Telnet virtuelle depuis l'extérieur, vous devez configurer une règle NAT d'identité pour l'adresse spécifiquement pour la fonctionnalité ARP du proxy. En raison des processus internes de Telnet virtuel, le mandataire ARP permet à l'ASA de conserver le trafic destiné à l'adresse Telnet virtuelle au lieu d'envoyer ce dernier vers l'interface source conformément à la règle NAT. (Voir la figure suivante.)

Illustration 27 : ARP mandataire et Telnet virtuel



Exigences de routage en mode transparent pour les réseaux distants

Lorsque vous utilisez la NAT en mode transparent, certains types de trafic nécessitent des routes statiques. Consultez le guide de configuration des opérations générales pour en savoir plus.

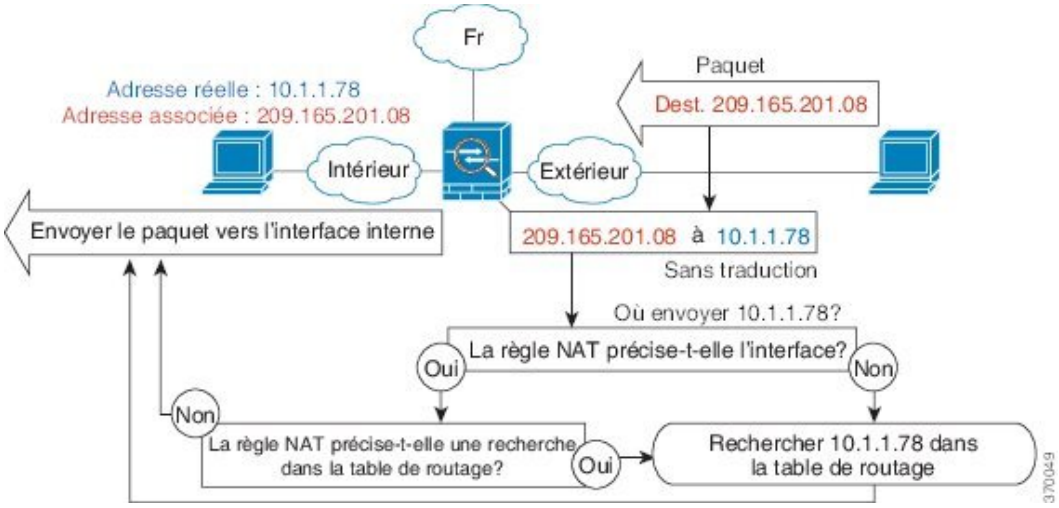
Détermination de l'interface de sortie

Lorsque vous utilisez la NAT et que l'ASA reçoit du trafic pour une adresse mappée, l'ASA détraduit l'adresse de destination en fonction de la règle NAT, puis il envoie le paquet vers l'adresse réelle. L'ASA détermine l'interface de sortie pour le paquet comme suit :

- Interfaces de groupe de ponts en mode transparent ou en mode routé : l'ASA détermine l'interface de sortie pour l'adresse réelle à l'aide de la règle NAT ; vous devez préciser les interfaces de membre du groupe de ponts source et de destination dans le cadre de la règle NAT.
- Interfaces standard en mode routé : l'ASA détermine l'interface de sortie de l'une des manières suivantes :
  - Vous configurez l'interface dans la règle NAT : l'ASA utilise la règle NAT pour déterminer l'interface de sortie. (de la version 8.3(1) à la version 8.4(1)) La seule exception concerne la NAT d'identité, qui utilise toujours une recherche de routage, quelle que soit la configuration de la NAT. (8.4(2) et versions ultérieures) Pour la NAT d'identité, le comportement par défaut est d'utiliser la configuration NAT. Cependant, vous avez la possibilité d'utiliser à la place une recherche de routage. Dans certains scénarios, un remplacement de recherche de routage est requis.
  - Vous ne configurez pas l'interface dans la règle NAT : l'ASA utilise une recherche de routage pour déterminer l'interface de sortie.

La figure suivante montre la méthode de sélection de l'interface de sortie en mode routé. Dans presque tous les cas, une recherche de routage est équivalente à l'interface de règle NAT, mais dans certaines configurations, les deux méthodes peuvent différer.

Illustration 28 : Sélection de l'interface de sortie en mode routé avec NAT



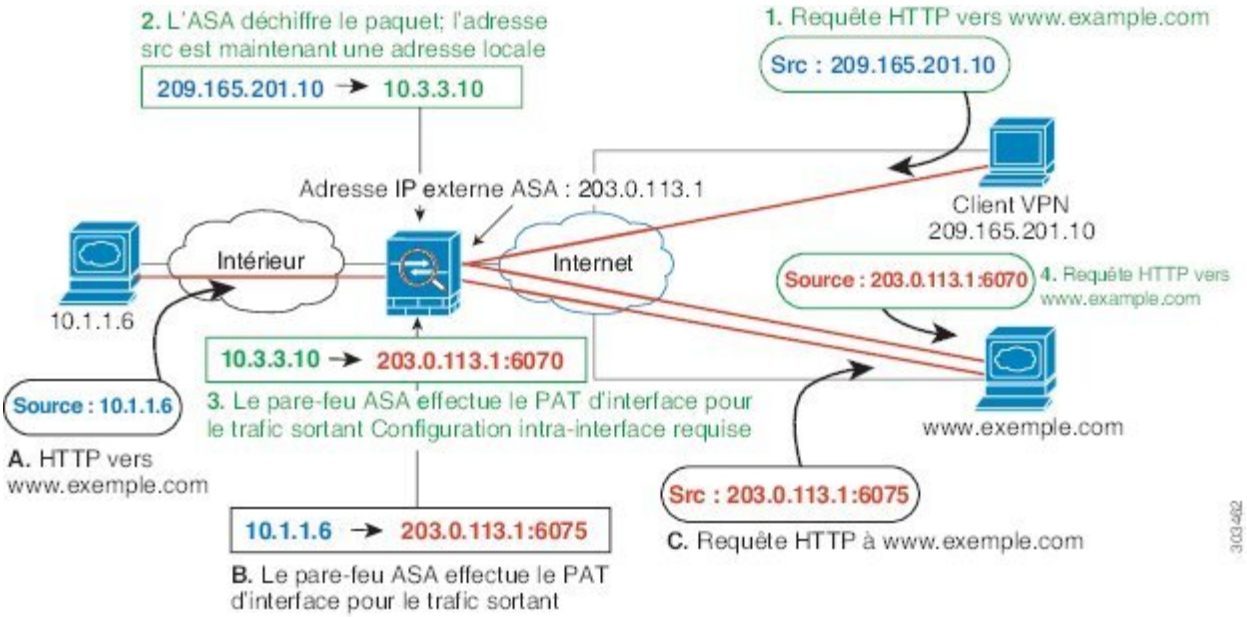
NAT pour VPN

Les rubriques suivantes expliquent l'utilisation de la NAT avec les différents types de VPN.

NAT et VPN d'accès à distance

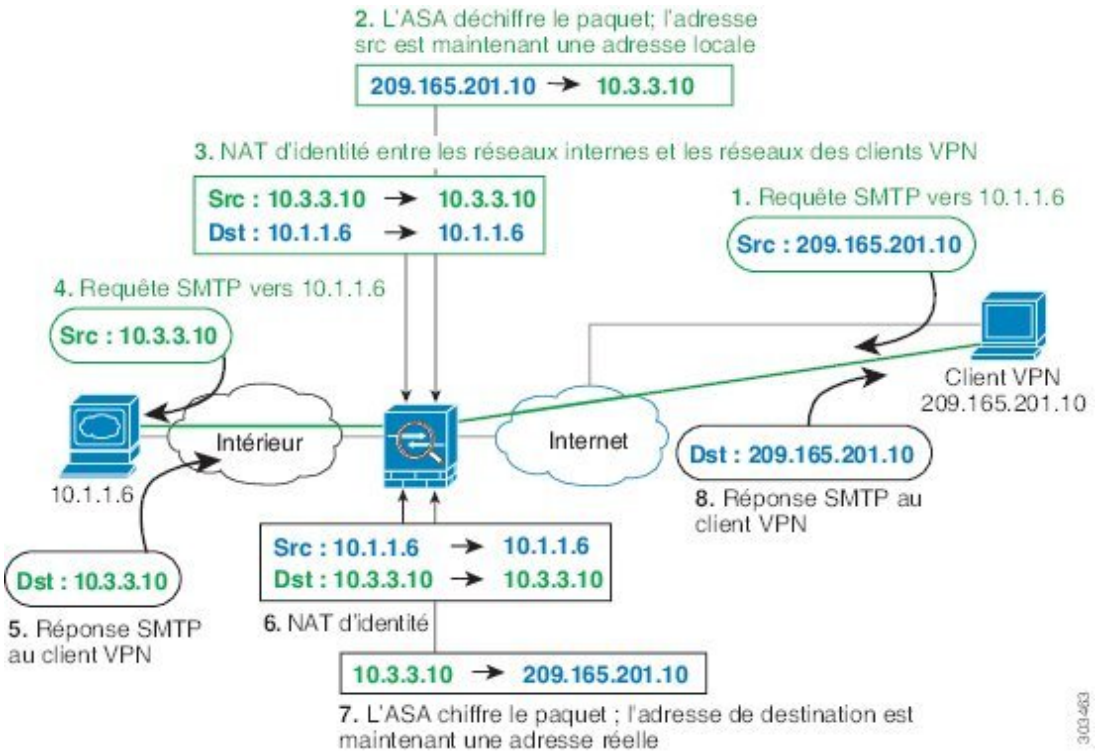
La figure suivante montre un serveur interne (10.1.1.6) et un client VPN (209.165.201.10) qui accèdent à Internet. Sauf si vous configurez la tunnellisation fractionnée pour le client VPN (où seul le trafic spécifié passe par le tunnel VPN), le trafic VPN lié à Internet doit également passer par l'ASA. Lorsque le trafic VPN entre dans l'ASA, l'ASA déchiffre le paquet; le paquet obtenu comprend l'adresse locale du client VPN (10.3.3.10) comme source. Pour les réseaux internes et de clients VPN, 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. Pour permettre au trafic VPN de quitter la même interface par laquelle il est entré, vous devez également activer la communication intra-interface (également connue sous le nom de mise en réseau en épingle à cheveux).

Illustration 29 : PAT d'interface pour le trafic VPN lié à Internet (intra-interface)



La figure suivante montre un client VPN qui souhaite accéder à un serveur de messagerie interne. Comme l'ASA s'attend à ce que le trafic entre le réseau interne et tout réseau externe corresponde à la règle PAT de l'interface que vous avez configurée pour l'accès Internet, le trafic du client VPN (10.3.3.10) vers le serveur SMTP (10.1.1.6) sera abandonné en raison d'un échec de chemin inverse : le trafic de 10.3.3.10 à 10.1.1.6 ne correspond pas à une règle NAT, mais le trafic de retour de 10.1.1.6 à 10.3.3.10 *doit* correspondre à la règle PAT de l'interface pour le trafic sortant. Comme les flux avant et inverse ne correspondent pas, l'ASA abandonne le paquet lorsqu'il est reçu. Pour éviter cette défaillance, vous devez exempter le trafic interne vers client VPN de la règle PAT d'interface en utilisant une règle NAT d'identité entre ces réseaux. La NAT d'identité traduit simplement une adresse en la même adresse.

Illustration 30 : NAT d'identité pour les clients VPN



Consultez l'exemple de configuration NAT suivant pour le réseau ci-dessus :

```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface

! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

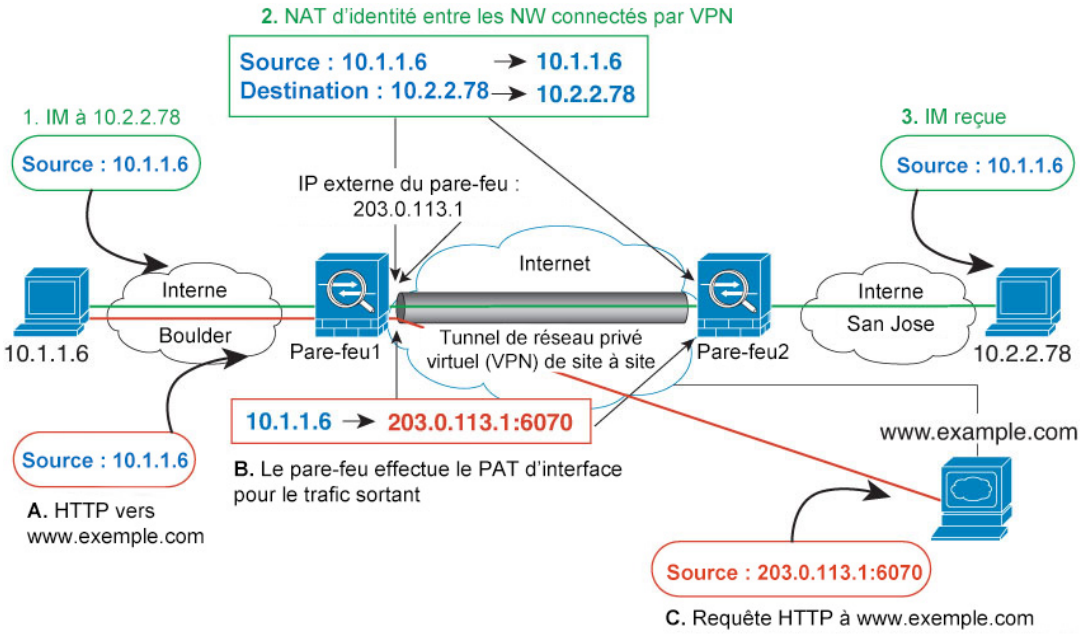
! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static inside_nw inside_nw destination static vpn_local vpn_local
```

NAT et VPN de site à site

La figure suivante montre un tunnel de site à site connectant les bureaux de Bouder et de San Jose. Pour le trafic que vous souhaitez diriger vers Internet (par exemple, de l'hôte 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 l'hôte 10.1.1.6 à Boulder vers l'hôte 10.2.2.78 à San Jose), vous ne

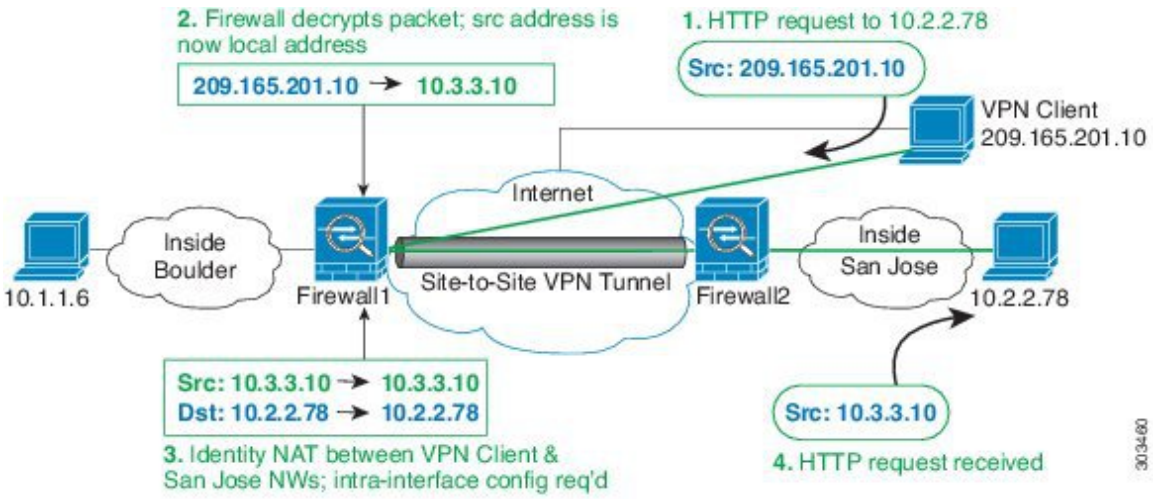
souhaitez pas effectuer la NAT; vous devez exclure ce trafic en créant une règle NAT d'identité. La NAT d'identité traduit simplement une adresse en la même adresse.

Illustration 31 : PAT d'interface et NAT d'identité pour le VPN de site à site



La figure suivante montre un client VPN connecté à Pare-feu1 (Boulder), avec une requête Telnet pour un serveur (10.2.2.78) accessible par un tunnel de site à site entre Pare-feu1 et Pare-feu2 (San Jose). Comme il s'agit d'une connexion en épingle à cheveux, vous devez activer la communication intra-interface, qui est également requise pour le trafic à destination d'Internet par tunnellisation non divisée en provenance du client VPN. Vous devez également configurer la NAT d'identité entre le client VPN et les réseaux de Boulder et San Jose, comme vous le feriez entre n'importe quel réseau connecté par VPN pour exempter ce trafic des règles de la NAT sortante.

Illustration 32 : Accès du client VPN au VPN de site à site



Consultez l'exemple de configuration NAT suivant pour Firewall1 (Boulder) pour le deuxième exemple :

```
! Enable hairpin for VPN client traffic:
same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface

! Identify inside Boulder network, & perform object interface PAT when going to Internet:
object network boulder_inside
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

! Identify inside San Jose network for use in twice NAT rule:
object network sanjose_inside
subnet 10.2.2.0 255.255.255.0

! Use twice NAT to pass traffic between the Boulder network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside
destination static vpn_local vpn_local

! Use twice NAT to pass traffic between the Boulder network and San Jose without
! address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside
destination static sanjose_inside sanjose_inside

! Use twice NAT to pass traffic between the VPN client and San Jose without
! address translation (identity NAT):
nat (outside,outside) source static vpn_local vpn_local
destination static sanjose_inside sanjose_inside
```

Consultez l'exemple de configuration NAT suivant pour Firewall2 (San Jose) :

```
! Identify inside San Jose network, & perform object interface PAT when going to Internet:
object network sanjose_inside
subnet 10.2.2.0 255.255.255.0
nat (inside,outside) dynamic interface

! Identify inside Boulder network for use in twice NAT rule:
object network boulder_inside
subnet 10.1.1.0 255.255.255.0

! Identify local VPN network for use in twice NAT rule:
object network vpn_local
subnet 10.3.3.0 255.255.255.0

! Use twice NAT to pass traffic between the San Jose network and Boulder without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside
destination static boulder_inside boulder_inside

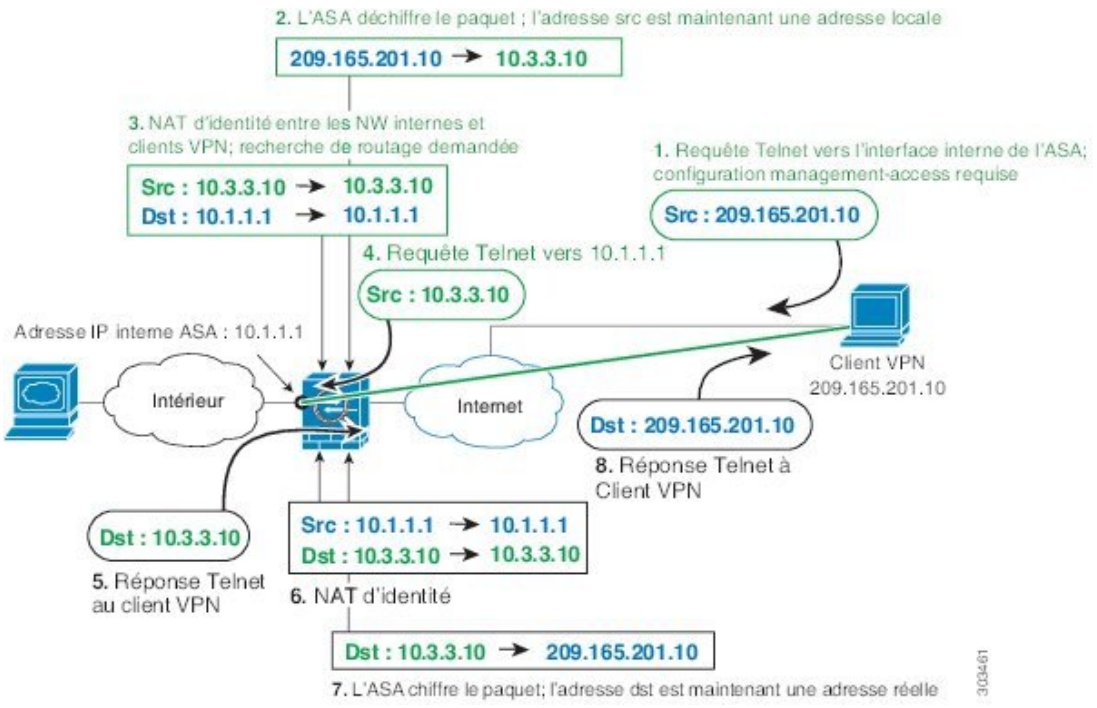
! Use twice NAT to pass traffic between the San Jose network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside
destination static vpn_local vpn_local
```

Accès à la gestion de la NAT et du VPN

Lorsque vous utilisez le VPN, vous pouvez autoriser l'accès de gestion à une interface autre que celle à partir de laquelle vous avez accédé à l'ASA. Par exemple, si vous saisissez l'ASA à partir de l'interface externe, cette fonctionnalité vous permet de vous connecter à l'interface interne à l'aide d'ASDM, SSH, Telnet ou SNMP; ou vous pouvez envoyer un message Ping à l'interface interne.

La figure suivante montre un client VPN qui établit une session Telnet avec l'interface interne de l'ASA. Lorsque vous utilisez une interface d'accès de gestion et que vous configurez la NAT d'identité selon NAT et VPN d'accès à distance, à la page 227 ou NAT et VPN de site à site, à la page 229, vous devez configurer la NAT avec l'option de recherche de routage. Sans recherche de routage, l'ASA envoie le trafic hors de l'interface spécifiée dans la commande NAT, indépendamment de ce que dit la table de routage; dans l'exemple ci-dessous, l'interface de sortie est l'interface interne. Vous ne souhaitez pas que l'ASA envoie le trafic de gestion au réseau interne; il ne reviendra jamais à l'adresse IP de l'interface interne. L'option recherche de routage permet à l'ASA d'envoyer le trafic directement à l'adresse IP de l'interface interne plutôt qu'au réseau interne. Pour le trafic du client VPN vers un hôte du réseau interne, l'option de recherche de routage aboutira toujours à l'interface de sortie correcte (interne), de sorte que le flux de trafic normal n'est pas affecté. Consultez la section Détermination de l'interface de sortie, à la page 226 pour plus d'informations sur l'option de recherche de routage.

Illustration 33 : Accès à la gestion du VPN



Consultez l'exemple de configuration NAT suivant pour le réseau ci-dessus :

```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

! Enable management access on inside ifc:
management-access inside

! Identify local VPN network, & perform object interface PAT when going to Internet:
```

```
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface

! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT), w/route-lookup:
nat (outside,inside) source static vpn_local vpn_local
destination static inside_nw inside_nw route-lookup
```

Dépannage de la NAT et du VPN

Consultez les outils de surveillance suivants pour résoudre les problèmes de NAT avec le VPN :

- Packet tracer : lorsqu'il est utilisé correctement, Packet Tracer indique les règles NAT auxquelles un paquet correspond.
- **show nat detail** : affiche le nombre d'accès et le trafic non traduit pour une règle NAT donnée.
- **show conn all** : permet d'afficher les connexions actives, y compris le trafic vers et à partir du boîtier.

Pour vous familiariser avec une configuration non fonctionnelle par rapport à une configuration fonctionnelle, vous pouvez effectuer les étapes suivantes :

1. Configurez le VPN sans NAT d'identité.
2. Entrez **show nat detail** et **show conn all**.
3. Ajoutez la configuration NAT d'identité.
4. Répétez **show nat detail** et **show conn all**.

Traduction des 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 twice NAT (NAT en double), 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 twice NAT (NAT en double) lorsque vous spécifiez une destination, la création de deux règles network object NAT (NAT objet de réseau) 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

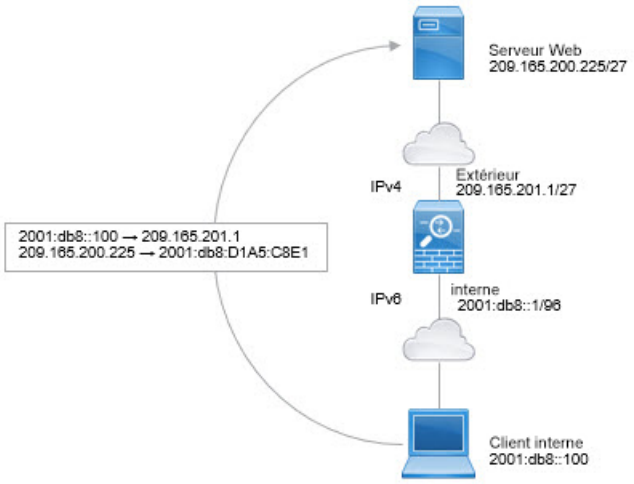
Lorsque le trafic passe d'un réseau IPv6 vers un réseau uniquement IPv4, vous devez convertir l'adresse IPv6 en IPv4 et renvoyer le trafic d'IPv4 à IPv6. Vous devez définir deux ensembles d'adresses, un ensemble d'adresses IPv4 pour lier les adresses IPv6 dans le réseau IPv4 et un ensemble d'adresses 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 twice NAT (NAT en double), 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 twice NAT (NAT en double) lorsque vous spécifiez une destination, la création de deux règles network object NAT (NAT objet de réseau) 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 twice NAT (NAT en double).



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

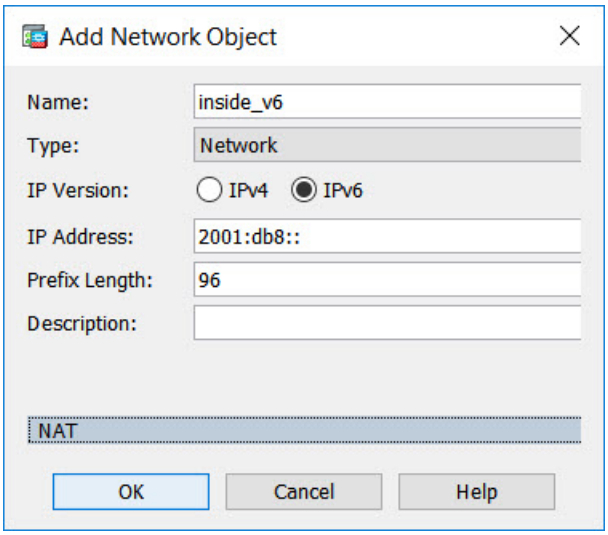
Étape 1 Créez un objet réseau pour le réseau IPv6 interne.

a) Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Network Objects/Groups (Objets/groupes de services réseau)**.

b) Cliquez sur **Add (Ajouter)** > **Network Object** (Objet réseau).

c) Configurez un objet avec les propriétés suivantes :

- **Name** (Nom) : par exemple, inside_v6.
- **Type** : sélectionnez **Network** (Réseau).
- **IP Version** (Version IP) : sélectionnez IPv6.
- **IP Address** (Adresse IP) : saisissez 2001:db8::
- **Prefix Length** (Longueur du préfixe) : saisissez 96.



d) Cliquez sur **OK**.

Étape 2 Créez la règle NAT Twice pour traduire le réseau IPv6 en IPv4 et inversement.

a) Choisissez **Configuration** > **Firewall** > **NAT Rules** > **(Configuration Pare-feu Règles NAT)**.

b) Cliquez sur **Add (Ajouter)** > **Add NAT Rule Before "Network Object" NAT Rules (Ajouter une règle NAT avant les règles NAT « Network Object »)**.

c) Configurez les options **Match Criteria: Original Packet** (Critères de correspondance : Paquet d'origine) suivantes :

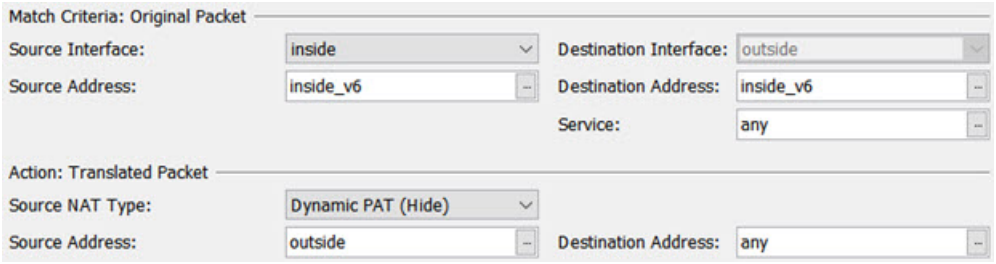
- **Source Interface** (Interface source) : sélectionnez inside (interne).
- **Destination Interface** (Interface de destination) : sélectionnez outside (externe).
- **Source Address** (Adresse source) : sélectionnez l'objet réseau inside_v6.
- **Destination Address** (Adresse de destination) : sélectionnez l'objet réseau inside_v6.
- **Service** : conservez la valeur par défaut, n'importe quel.

d) Configurez les options **Match Criteria: Translated Packet** (Critères de correspondance : Paquet traduit) suivantes :

- **Source NAT Type** (Type de NAT source) : Dynamic PAT (Hide) (PAT dynamique [masquer]).
- **Source Address** (Adresse source) : sélectionnez l'interface outside.
- **Destination Address** (Adresse de destination) : sélectionnez any.

Laissez les autres options à leurs valeurs par défaut.

La boîte de dialogue doit ressembler à ce qui suit :

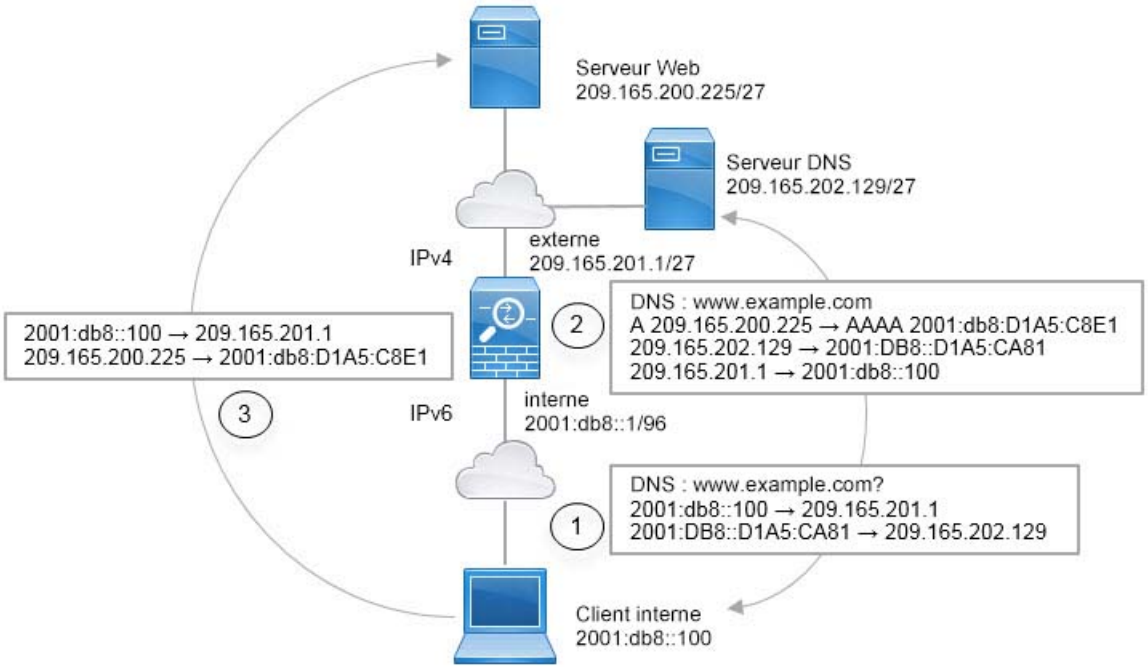


e) Cliquez sur **OK**.

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 vers 2001:DB8::D1A5:CA81
   - 209.165.201.1 vers 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 est l'équivalent IPv6 de 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 Choisissez **Configuration** > **Firewall** > **NAT Rules** > **(Configuration Pare-feu Règles NAT)**.

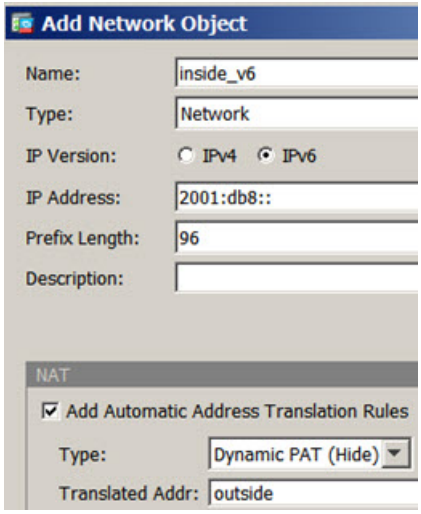
Étape 2 Configurez la règle PAT dynamique NAT64 pour le réseau IPv6 interne.

a) Choisissez **Add** > **Network Object NAT Rule** > **(Ajouter Règle NAT d'objet réseau)**.

b) Configurez les propriétés de base de l'objet :
   - **Name** (Nom) : par exemple, **inside_v6**.
   - **Type** : sélectionnez **Network** (Réseau).
   - **IP Version** (Version IP) : sélectionnez **IPv6**.
   - **IP Address** (Adresse IP) **: saisissez 2001:db8::**
   - **Prefix Length** (Longueur du préfixe) : saisissez **96**.

c) Sélectionnez **Dynamic** (Dynamique) ou **Dynamic PAT (Hide)** (PAT dynamique [masquer]) pour NAT Type (Type de NAT).

d) Pour **Translated Address** (Adresse traduite), cliquez sur le bouton de navigation et sélectionnez l'interface « outside ».



e) Cliquez sur le bouton **Advanced** (Avancé) et configurez les options suivantes :

- **Source Interface** (Interface source) : sélectionnez inside (interne).
- **Destination Interface** (Interface de destination) : l'interface « externe » doit déjà être sélectionnée.

f) Cliquez sur **OK** pour enregistrer les paramètres avancés.

g) Cliquez sur **OK** pour ajouter la règle de NAT.

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.

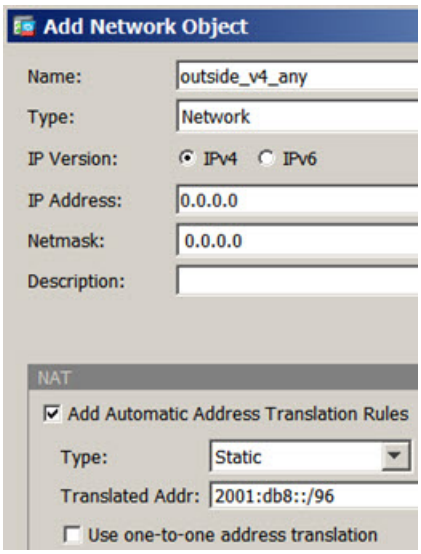
a) Choisissez **Add** > **Network Object NAT Rule** > **(Ajouter Règle NAT d'objet réseau)**.

b) Configurez les propriétés de base de l'objet :

- **Name** (Nom) : par exemple, **outside_v4_any**.
- **Type** : sélectionnez **Network** (Réseau).
- **IP Version** (Version IP) : sélectionnez **IPv4**.
- **IP Address** (Adresse IP) : saisissez **0.0.0.0**.
- **Netmask** (Masque de réseau) : saisissez **0.0.0.0**.

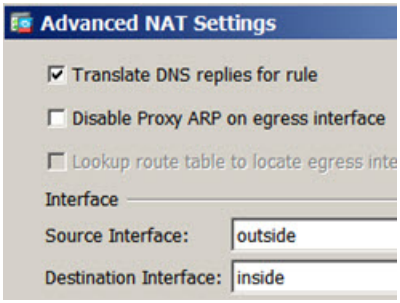
c) Configurez les propriétés NAT :

- **NAT Type** (Type de NAT) : sélectionnez **Static** (Statique).
- **Translated Address** (Adresse traduite) : saisissez **2001:db8::/96**.



d) Cliquez sur le bouton **Advanced** (Avancé) et configurez les options suivantes :

- **Translate DNS Replies for Rule** (Traduire les réponses DNS pour la règle) : sélectionnez cette option.
- **Source Interface** (Interface source) : sélectionnez « outside » (externe).
- **Destination Interface** (Interface de destination) : sélectionnez « inside » (interne).



e) Cliquez sur **OK** pour enregistrer les paramètres avancés.

f) Cliquez sur **OK** pour ajouter la règle de NAT.

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

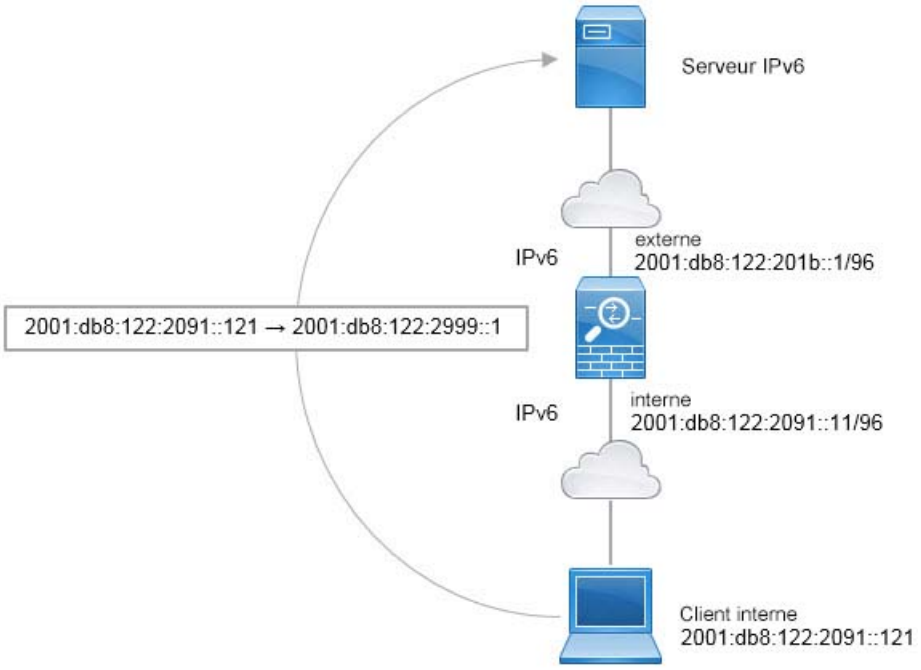
Lorsque vous passe z d'un réseau IPv6 à un autre réseau IPv6, vous pouvez traduire les adresses en adresses IPv6 différentes sur le réseau externe. Nous vous recommandons d'utiliser la NAT statique. Bien que vous

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 network object NAT (NAT objet de réseau). Toutefois, si vous ne souhaitez pas autoriser le trafic de retour, vous pouvez rendre la règle NAT statique unidirectionnelle en utilisant uniquement twice NAT (NAT en double).

Exemple de NAT66 : traduction statique entre réseaux

Vous pouvez configurer une traduction statique entre des regroupements d'adresses IPv6 en utilisant network object NAT (NAT objet de réseau). 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.



Procédure

Étape 1 Choisissez **Configuration** > **Firewall** > **NAT Rules** > **(Configuration** > **Pare-feu** > **Règles NAT)**.

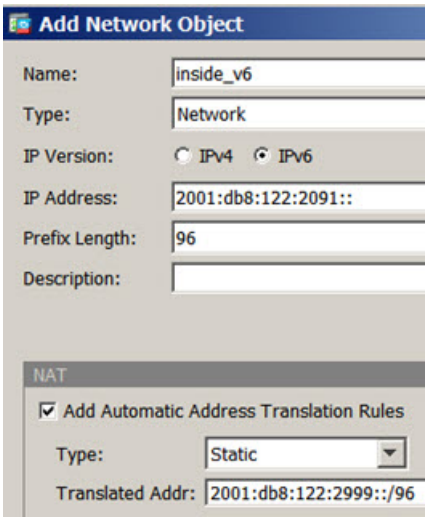
Étape 2 Configurez la règle NAT statique pour le réseau IPv6 interne.

a) Choisissez **Add** > **Network Object NAT Rule** > **(Ajouter** > **Règle NAT d'objet réseau)**.

b) Configurez les propriétés de base de l'objet :

- **Name** (Nom) : par exemple, **inside_v6**.
- **Type** : sélectionnez **Network** (Réseau).
- **IP Version** (Version IP) : sélectionnez **IPv6**.
- **IP Address** (Adresse IP) : saisissez **2001:db8:122:2091::**.
- **Prefix Length** (Longueur du préfixe) : saisissez **96**.

c) Sélectionnez **Static** (Statique) pour le type de NAT.
d) Pour **Translated Address** (Adresse traduite), saisissez **2001:db8:122:2999::/96**.



e) Cliquez sur le bouton **Advanced** (Avancé) et configurez les options suivantes :
   - **Source Interface** (Interface source) : sélectionnez inside (interne).
   - **Destination Interface** (Interface de destination) : sélectionnez outside (externe).

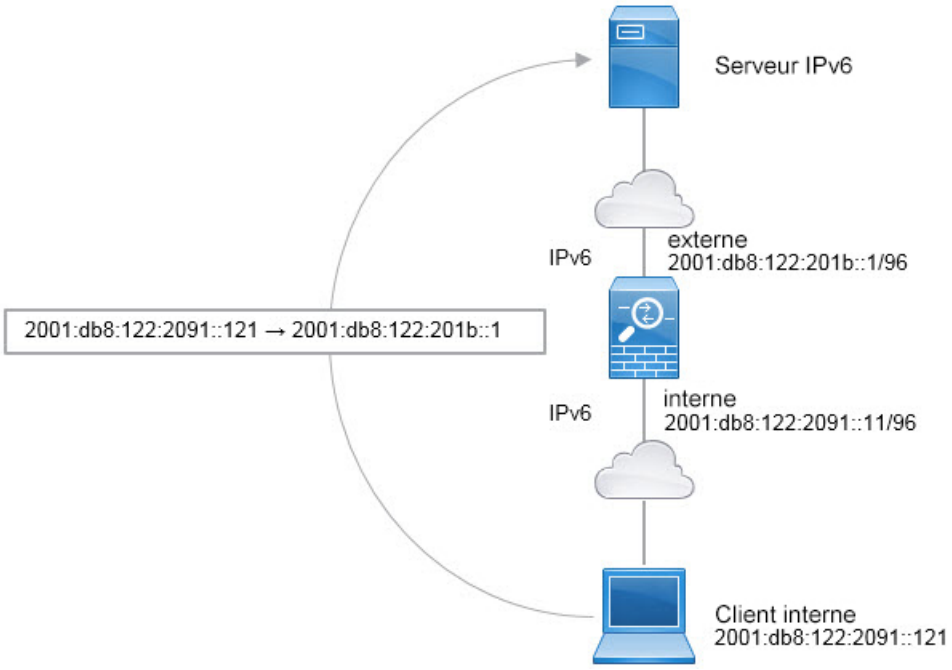
f) Cliquez sur **OK** pour enregistrer les paramètres avancés.
g) Cliquez sur **OK** pour ajouter la règle NAT.

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.

Lorsque vous configurez une règle PAT d'interface pour NAT66, toutes les adresses globales configurées sur cette interface sont utilisées pour le mappage PAT. Les adresses link-local ou site-local pour l'interface ne sont pas utilisées pour la PAT.



Procédure

Étape 1 Choisissez **Configuration** > **Firewall** > **NAT Rules** > **(Configuration Pare-feu Règles NAT)**.

Étape 2 Configurez la règle PAT dynamique pour le réseau IPv6 interne.

a) Choisissez **Add** > **Network Object NAT Rule** > **(Ajouter Règle NAT d'objet réseau)**.

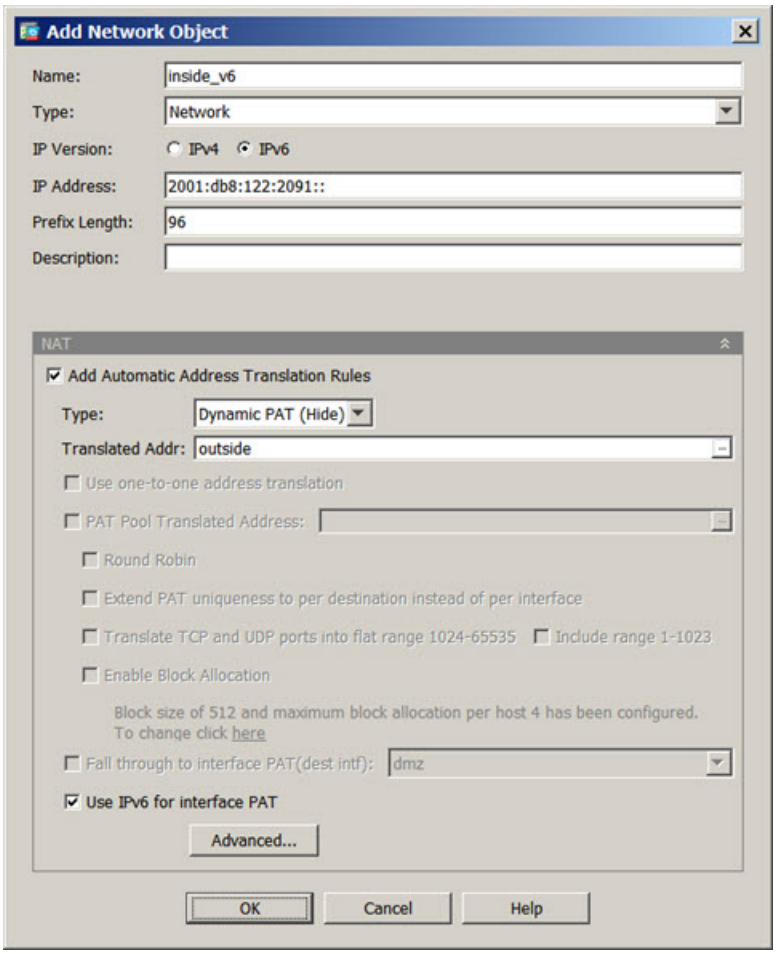
b) Configurez les propriétés de base de l'objet :

- **Name** (Nom) : par exemple, **inside_v6**.
- **Type** : sélectionnez **Network** (Réseau).
- **IP Version** (Version IP) : sélectionnez **IPv6**.
- **IP Address** (Adresse IP) : saisissez **2001:db8:122:2091::**.
- **Prefix Length** (Longueur du préfixe) : saisissez **96**.

c) Sélectionnez **Dynamic** (Dynamique) ou **Dynamic PAT (Hide)** (PAT dynamique [masquer]) pour NAT Type (Type de NAT).

d) Pour **Translated Address** (Adresse traduite), cliquez sur le bouton de navigation et sélectionnez l'interface « outside ».

e) Sélectionnez l'option **Use IPv6 for Interface PAT** (Utiliser IPv6 pour la PAT d'interface).



f) Cliquez sur le bouton **Advanced** (Avancé) et configurez les options suivantes :

- **Source Interface** (Interface source) : sélectionnez inside (interne).
- **Destination Interface** (Interface de destination) : l'interface « externe » doit déjà être sélectionnée.

g) Cliquez sur **OK** pour enregistrer les paramètres avancés.

h) Cliquez sur **OK** pour ajouter la règle NAT.

Avec cette règle, tout trafic du sous-réseau 2001:db8:122:2091::/96 sur l'interface interne à destination de l'interface externe reçoit une traduction PAT NAT66 vers l'une des adresses globales IPv6 configurées pour l'interface externe.

Réécriture des requêtes et des réponses DNS à l'aide de la NAT

Vous devrez peut-être configurer l'ASA 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, NAT66, 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 twice NAT (NAT en double), 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.
- Vous devez activer l'inspection des applications DNS avec la réécriture DNS NAT activée pour que les règles NAT réécrivent les requêtes et les réponses DNS. Par défaut, l'inspection DNS avec la réécriture DNS NAT est appliquée de manière globale. Vous n'avez donc probablement pas besoin de modifier la configuration de l'inspection.
- 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).

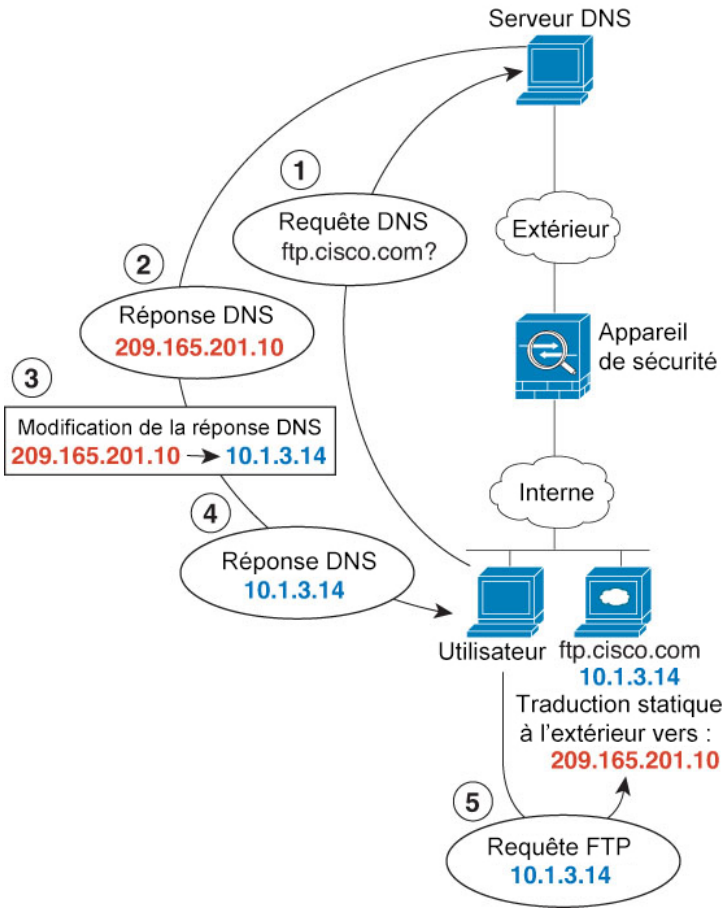
Les rubriques suivantes présentent des exemples de réécriture DNS dans les règles NAT.

Modification de la réponse 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 10.1.3.14. 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.

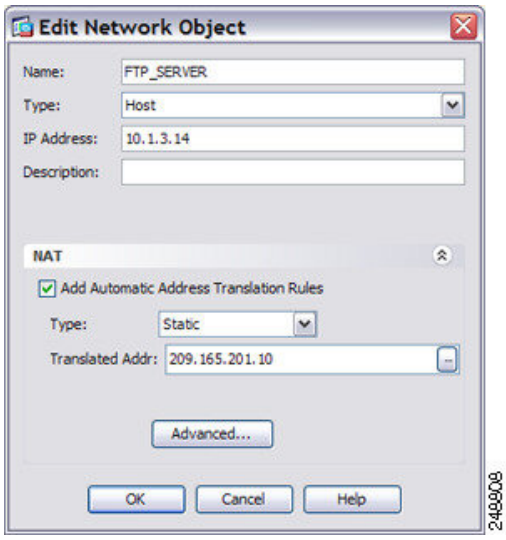


Procédure

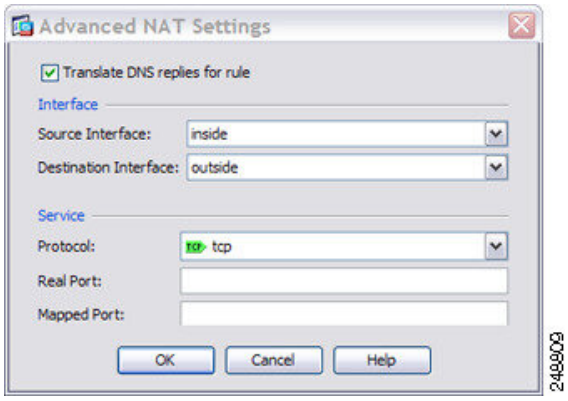
Étape 1 Choisissez **Configuration** > **Firewall** > **(Pare-feu)** > **NAT**.

Étape 2 Choisissez **Add** > **Network Object NAT Rule** > **(Ajouter Règle NAT d'objet réseau)**.

Étape 3 Nommez le nouvel objet réseau, définissez l'adresse du serveur FTP, activez la NAT statique et saisissez l'adresse traduite.



Étape 4 Cliquez sur **Advanced** (Avancé) et configurez les interfaces réelles et mappées et la modification DNS.



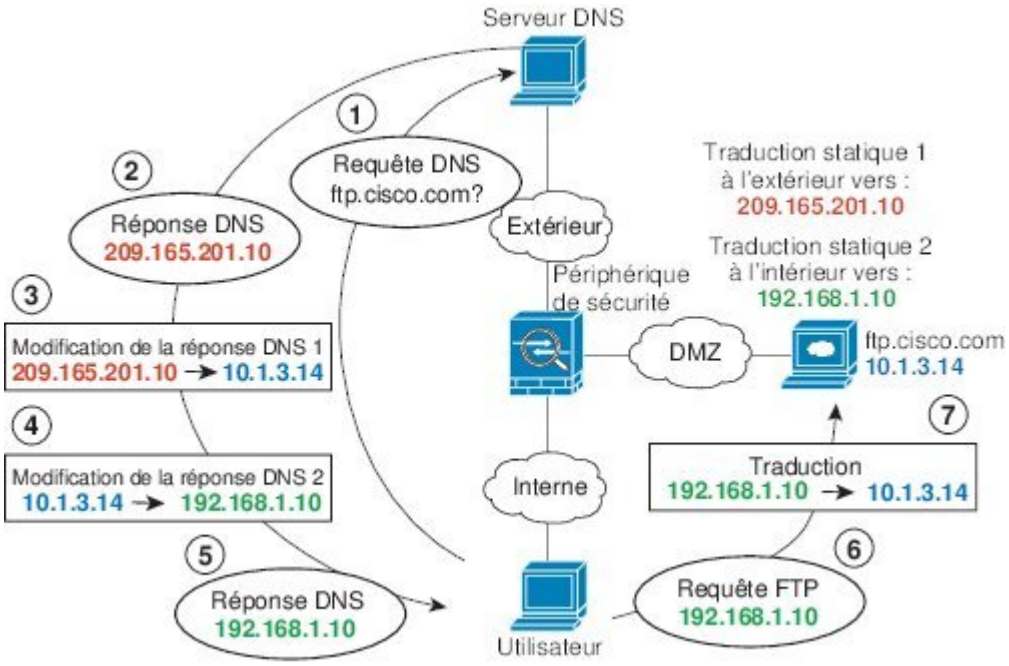
Étape 5 Cliquez sur **OK** pour revenir à la boîte de dialogue Edit Network Object (modifier l'objet de réseau), cliquez de nouveau sur **OK**, puis cliquez sur **Apply** (Appliquer).

Modification de la réponse DNS, serveur DNS, hôte et serveur sur des réseaux séparés

La figure suivante montre un utilisateur du réseau interne demandant l'adresse IP pour ftp.cisco.com, qui se trouve sur le réseau DMZ, à partir d'un serveur DNS externe. Le serveur DNS répond avec l'adresse mappée (209.165.201.10) selon la règle statique entre l'extérieur et DMZ, même si l'utilisateur ne se trouve pas sur le réseau DMZ. L'ASA traduit l'adresse dans la réponse DNS en 10.1.3.14.

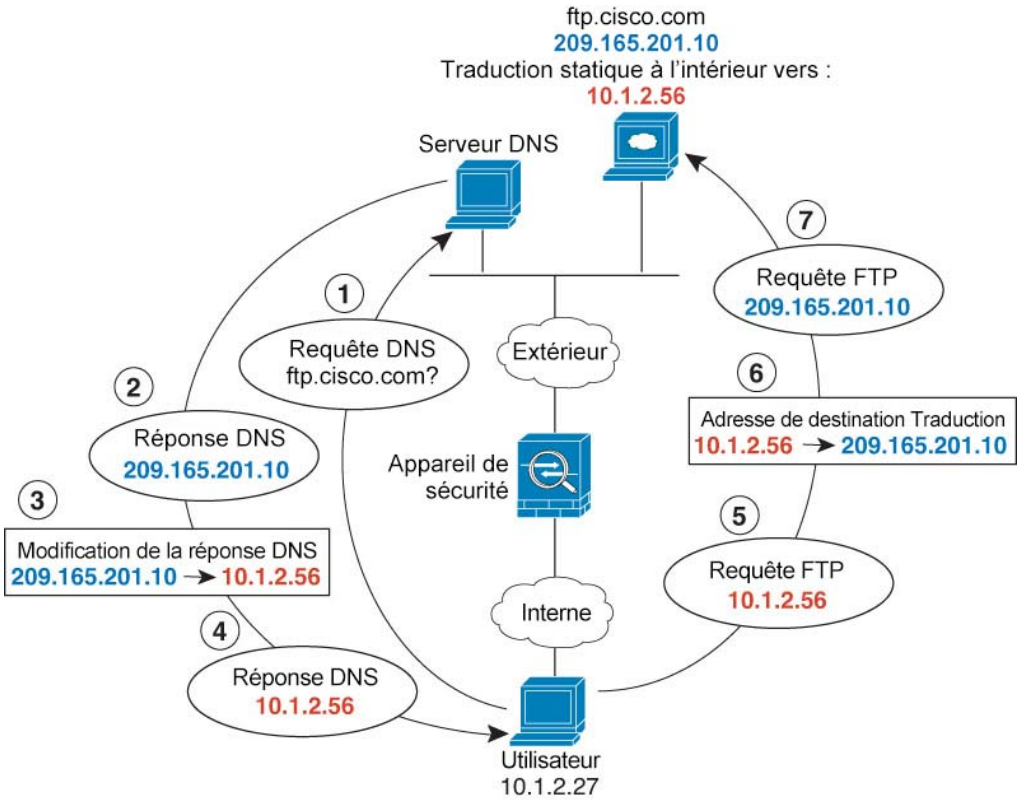
Si l'utilisateur doit accéder à ftp.cisco.com en utilisant l'adresse réelle, aucune autre configuration n'est requise. S'il y a également une règle statique entre l'intérieur et DMZ, vous devez également activer la modification de la réponse DNS sur cette règle. La réponse DNS sera ensuite modifiée deux fois. Dans ce cas, l'ASA traduit à nouveau l'adresse dans la réponse DNS en 192.168.1.10 selon la règle statique entre l'intérieur et DMZ.

Illustration 34 : Modification de la réponse DNS, serveur DNS, hôte et serveur sur des réseaux séparés



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, 209.165.201.10. 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.

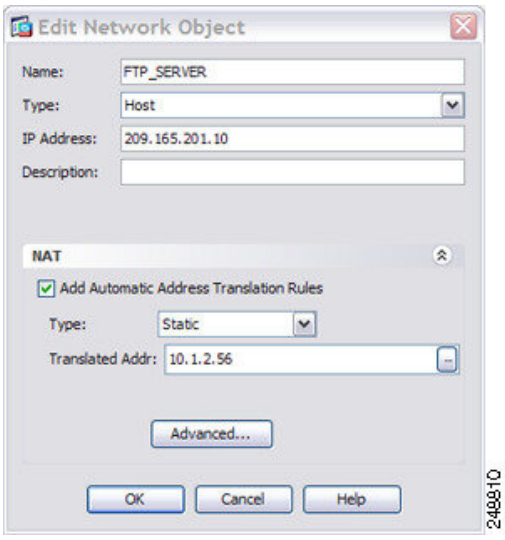


Procédure

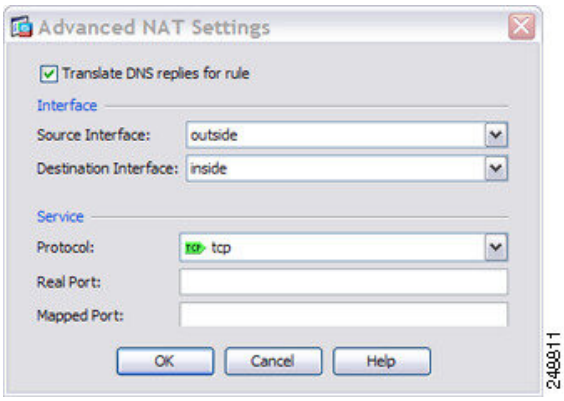
Étape 1 Choisissez **Configuration** > **Firewall** > **(Pare-feu)** > **NAT**.

Étape 2 Choisissez **Add** > **Network Object NAT Rule** > **(Ajouter Règle NAT d'objet réseau)**.

Étape 3 Nommez le nouvel objet réseau, définissez l'adresse du serveur FTP, activez la NAT statique et saisissez l'adresse traduite.



Étape 4 Cliquez sur **Advanced** (Avancé) et configurez les interfaces réelles et mappées et la modification DNS.

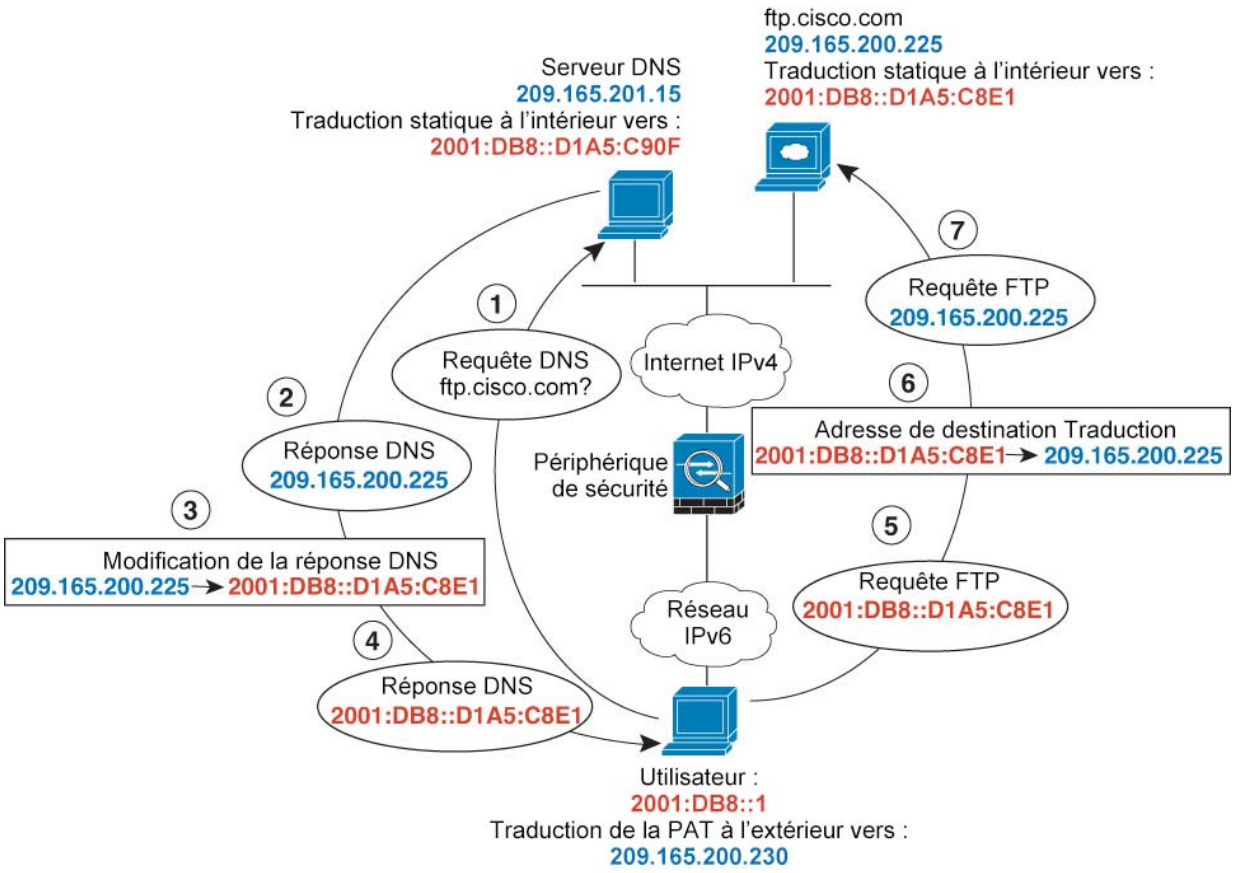


Étape 5 Cliquez sur **OK** pour revenir à la boîte de dialogue Edit Network Object (modifier l'objet de réseau), cliquez de nouveau sur **OK**, puis cliquez sur **Apply** (Appliquer).

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.



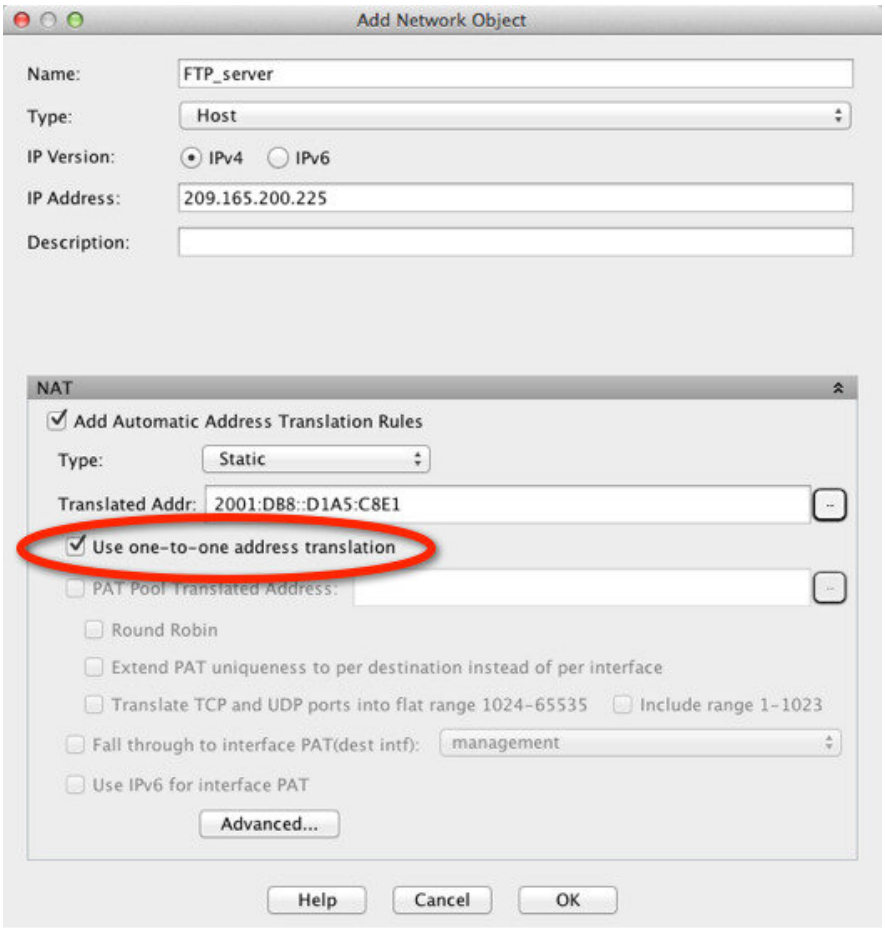
Procédure

Étape 1 Choisissez **Configuration** > **Firewall** > **(Pare-feu)** > **NAT**.

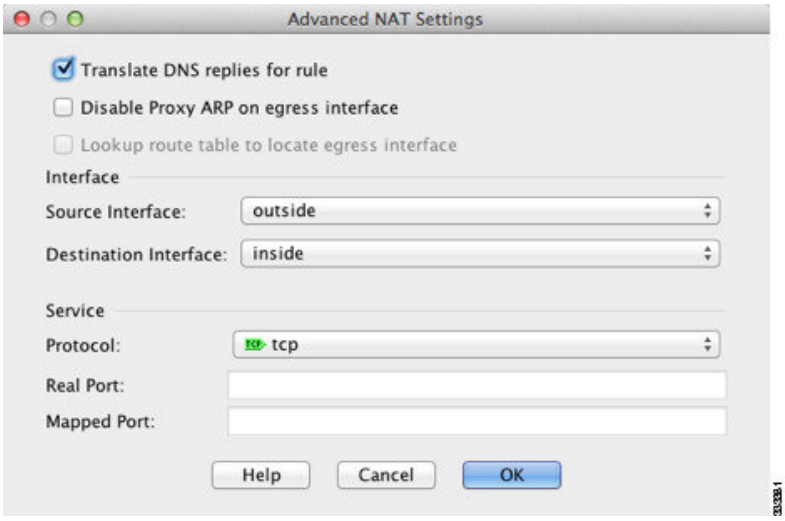
Étape 2 Configurez la règle NAT statique avec modification DNS pour le serveur FTP.

a) Choisissez **Add > Network Object NAT Rule** (Ajouter > Règle NAT d'objet réseau).

b) Nommez le nouvel objet réseau, définissez l'adresse du serveur FTP, activez la NAT statique et saisissez l'adresse traduite. Comme il s'agit d'une traduction un à un pour NAT46, sélectionnez **Use one-to-one address translation** (Utiliser la traduction d'adresse un à un).



c) Cliquez sur **Advanced** (Avancé) et configurez les interfaces réelles et mappées et la modification DNS.

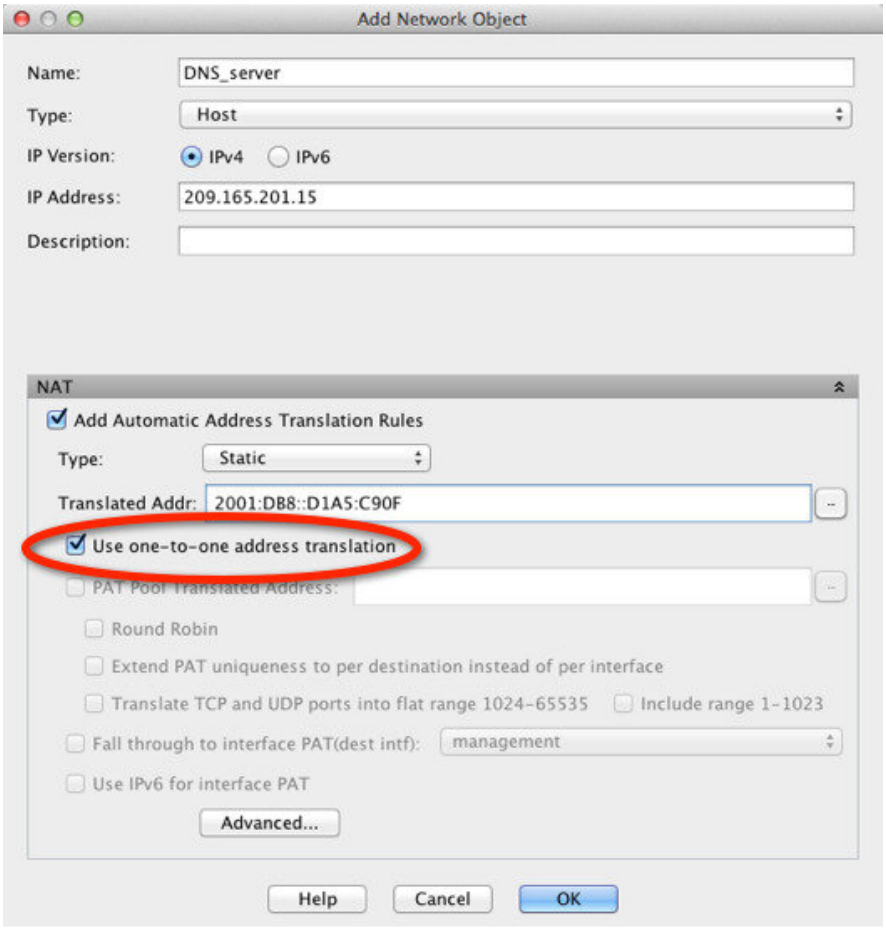


d) Cliquez sur **OK** pour revenir à la boîte de dialogue Network Object, et cliquez de nouveau sur **OK** pour enregistrer la règle.

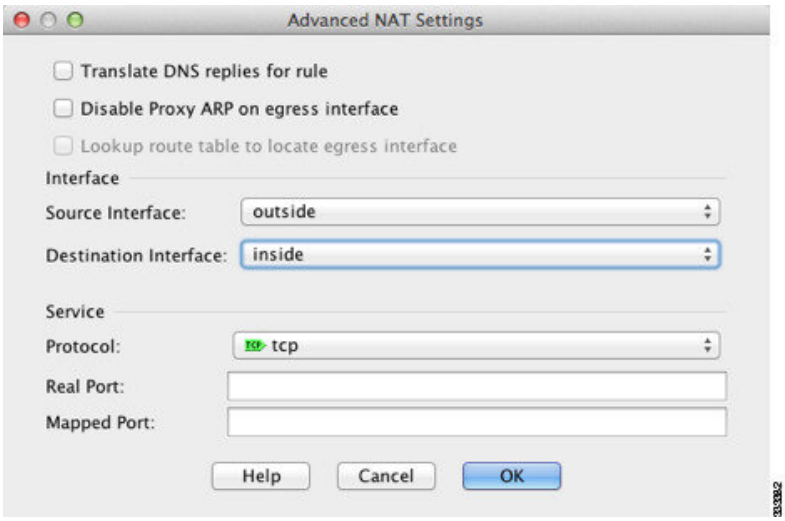
Étape 3 Configurez la NAT statique pour le serveur DNS.

a) Choisissez **Add > Network Object NAT Rule** (Ajouter > Règle NAT d'objet réseau).

b) Nommez le nouvel objet réseau, définissez l'adresse du serveur DNS, activez la NAT statique et saisissez l'adresse traduite. Comme il s'agit d'une traduction un à un pour NAT46, sélectionnez **Use one-to-one address translation** (Utiliser la traduction d'adresse un à un).



c) Cliquez sur **Advanced** (Avancé) pour configurer les interfaces réelles et mappées.



d) Cliquez sur **OK** pour revenir à la boîte de dialogue Network Object, et cliquez de nouveau sur **OK** pour enregistrer la règle.

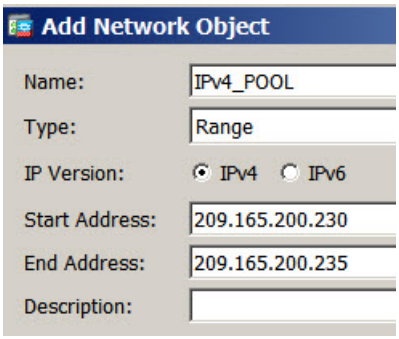
Étape 4 Configurez le PAT pour le réseau IPv6 interne.

a) Choisissez **Add > Network Object NAT Rule** (Ajouter > Règle NAT d'objet réseau).

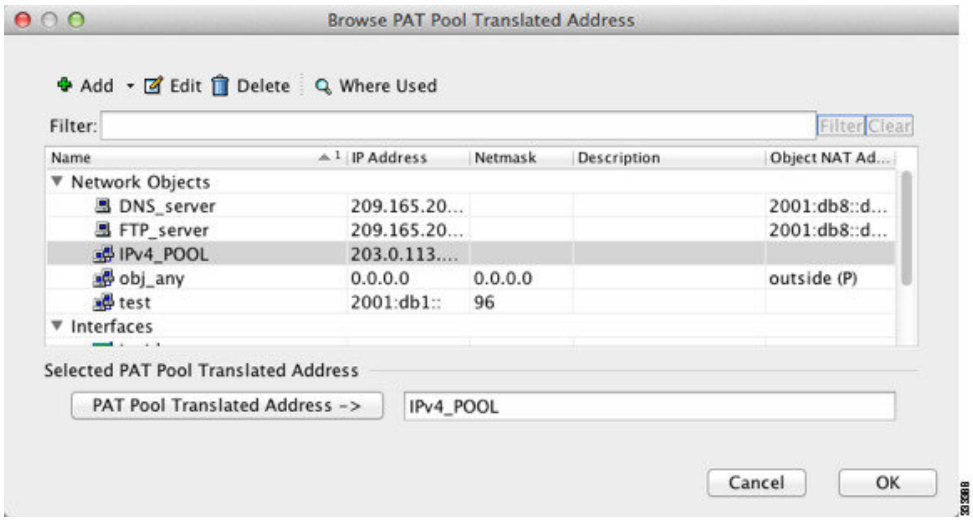
b) Nommez le nouvel objet réseau, définissez l'adresse réseau IPv6 et sélectionnez **Dynamic** NAT.

c) Sélectionnez **PAT Pool Translated Address (Adresses traduites du pool PAT)**, et cliquez sur le bouton **...** (Parcourir) pour créer l'objet de pool PAT.

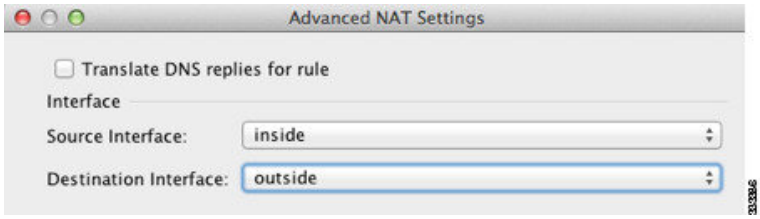
d) Dans la boîte de dialogue Browse PAT Pool Translated Address (Parcourir les adresses traduites du pool PAT), sélectionnez **Add (Ajouter) > Network Object (Objet réseau)**. Nommez le nouvel objet, saisissez la plage d'adresses pour l'ensemble PAT, puis cliquez sur **OK**.



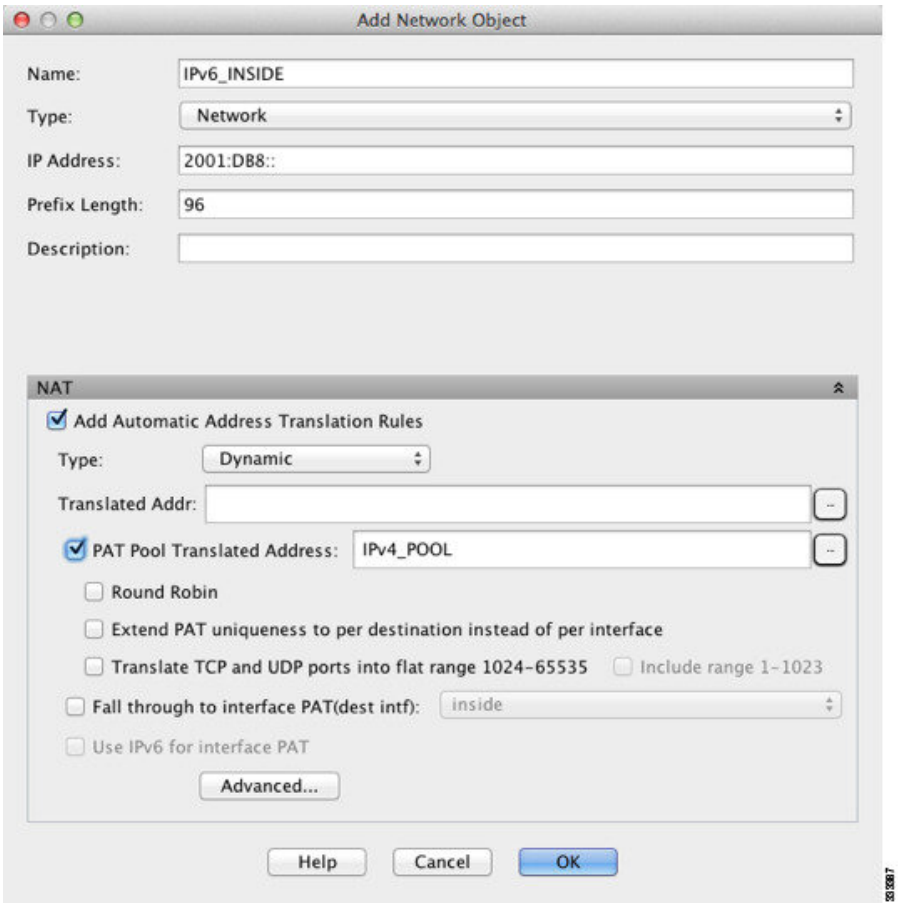
e) Dans la boîte de dialogue Browse PAT Pool Translated Address (Parcourir les adresses traduites du pool PAT), double-cliquez sur l'objet de pool PAT que vous avez créé pour le sélectionner et cliquez sur **OK**.



f) Cliquez sur **Advanced** (Avancé) pour configurer les interfaces réelles et mappées.



g) Cliquez sur **OK** pour revenir à la boîte de dialogue Network Object (Objet réseau).

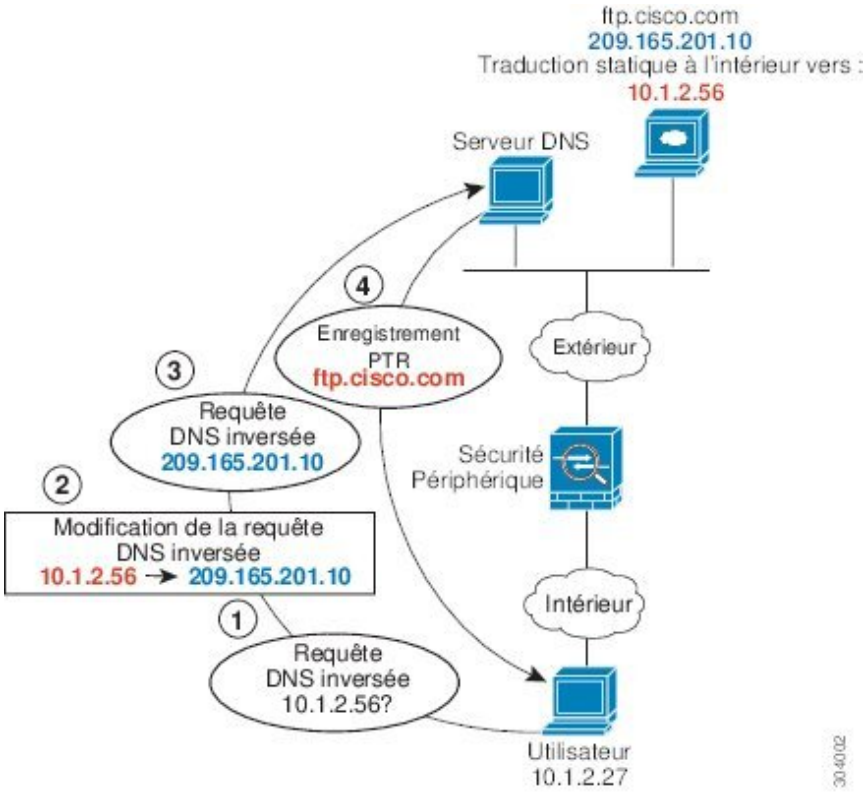


Étape 5 Cliquez sur **OK**, puis sur **Apply**(appliquer).

Modification PTR, serveur DNS sur le réseau hôte

La figure suivante montre un serveur FTP et un serveur DNS à l'extérieur. L'ASA dispose d'une traduction statique pour le serveur externe. Dans ce cas, lorsqu'un utilisateur interne effectue une recherche DNS inversée pour 10.1.2.56, l'ASA modifie la requête DNS inversée avec l'adresse réelle, et le serveur DNS répond avec le nom du serveur, ftp.cisco.com.

Illustration 35 : Modification PTR, serveur DNS sur le réseau hôte





CHAPITRE 10

Mappage de l'adresse et du port (MAP)

Le mappage de l'adresse et du port (MAP) est une fonctionnalité de niveau opérateur permettant de traduire les adresses IPv4 en IPv6, afin que le trafic puisse être envoyé sur le réseau IPv6 du fournisseur de services avant d'être retraduit en IPv4 à la périphérie du fournisseur de services.

- Mappage de l'adresse et du port (MAP), à la page 259
- Lignes directrices pour le mappage de l'adresse et du port (MAP), à la page 260
- Configurer les domaines MAP-T, à la page 262
- Surveillance MAP, à la page 263
- Historique de MAP, à la page 264

Mappage de l'adresse et du port (MAP)

Le mappage de l'adresse et du port (MAP) est principalement une fonctionnalité utilisée dans les réseaux des fournisseurs de services (SP). Le fournisseur de services peut exploiter un réseau IPv6 uniquement, le domaine MAP, tout en prenant en charge les clients IPv4 uniquement et leur besoin de communiquer avec des sites IPv4 uniquement sur l'Internet public. La carte est définie dans RFC7597, RFC7598 et RFC7599.

Pour le fournisseur de services, dans le domaine MAP, l'avantage de MAP sur NAT46 est que la substitution d'une adresse IPv6 à l'adresse IPv4 de l'abonné (et retour à IPv4 à la périphérie du réseau du fournisseur) est sans état. Cela offre une plus grande efficacité dans le réseau SP par rapport à NAT46.

Il existe deux techniques MAP, la traduction MAP (MAP-T) et l'encapsulation MAP (MAP-E). L'ASA prend en charge MAP-T; MAP-E n'est pas pris en charge.

Traduction du mappage de l'adresse et du port (MAP-T)

Avec MAP-T, l'adresse IPv4 de l'abonné est d'abord traduite en adresse IPv4 publique du fournisseur de services (SP), qui peut être un mappage d'adresse un à un, ou un mappage vers un préfixe ou une adresse partagée. Ensuite, cette adresse IPv4 est traduite en adresse IPv6 dans le domaine MAP, et le paquet est transmis sur le réseau IPv6 du fournisseur. À la périphérie du réseau, le relais de frontière du fournisseur de services est responsable de traduire l'adresse IPv6 en adresse IPv4 du fournisseur de services avant d'acheminer le paquet vers le réseau IPv4 public. L'ordre inverse est effectué pour le trafic provenant du réseau IPv4 public vers l'abonné.

Illustration 36 : Réseau MAP-T



En utilisant MAP-T, vous pouvez faire passer le réseau du fournisseur de services vers une architecture IPv6 uniquement, tout en permettant aux abonnés de continuer à utiliser IPv4 et de communiquer avec des réseaux Internet IPv4 uniquement ou d'autres sites situés à l'extérieur du réseau du fournisseur de services.

MAP-T se comporte comme une traduction NAT64, mais au lieu d'utiliser une adresse IPv6 avec une adresse IPv4 intégrée, il utilise un schéma d'encodage qui intègre également le numéro de port. Ainsi, MAP-T permet de restreindre la plage de ports utilisée par les périphériques.

Un système MAP-T comprend les éléments suivants :

- **Périphérique Customer Edge (CE)** : le CE est une passerelle domestique (routeur sans fil, modem câblé avec routeur, etc.). Le CE fournit une traduction IPv4/IPv6 ainsi qu'un transfert IPv6 natif. Il comporte une interface côté WAN adressée en IPv6 et orientée vers le fournisseur, ainsi qu'une ou plusieurs interfaces côté LAN utilisant un adressage IPv4 privé. Vous devez configurer un ou plusieurs domaines MAP que le CE utilisera pour traduire les paquets IPv4 en IPv6 et vice-versa.
- **Périphérique de relais de frontière (BR)** : vous devez installer l'ASA en tant que relais de frontière. Le BR est un composant côté fournisseur à la périphérie du domaine MAP qui prend en charge la traduction IPv4/IPv6. Le BR a au moins une interface compatible avec IPv6 et une interface IPv4 connectée au réseau IPv4. Vous devez configurer un ou plusieurs domaines MAP que le BR utilisera pour traduire les paquets IPv4 en IPv6 et vice-versa. Vous devez configurer les CE et le BR avec les mêmes règles de domaine MAP.
- **Domaine MAP** : un domaine MAP est un mécanisme permettant de regrouper un ensemble de périphériques MAP-T CE avec un ensemble de périphériques MAP-T BR. Un domaine est un ensemble de paramètres partagés entre les périphériques BR et CE affectés au domaine. Vous configurez le même domaine avec les mêmes paramètres sur chacun des périphériques BR et CE.

Lignes directrices pour le mappage de l'adresse et du port (MAP)

Directives sur le mode pare-feu

Vous pouvez configurer MAP en mode routé uniquement. Le mode transparent n'est pas pris en charge.

Directives supplémentaires

- L'ASA ne s'implique pas dans le transfert de paquets en mode maillé. Ainsi, vous ne pouvez pas configurer de règles de mappage de transfert (FMR) dans un domaine MAP.
- MAP ne prend pas en charge le trafic VPN tunnelisé, de multidiffusion ou Anycast.

- Vous ne pouvez pas utiliser à la fois la NAT et le mappage sur une connexion donnée. Assurez-vous que vos règles de NAT et de MAP ne se chevauchent pas. Vous obtiendrez des résultats inattendus si vous avez des règles qui se chevauchent.
- Les inspections suivantes ne prennent pas en charge la traduction MAP. Les paquets soumis à ces inspections ne sont pas traduits.
  - CTIQBE
  - DCERPC
  - Diameter
  - Résolution de nom sur WINS
  - GTP
  - H.323 et H.225 et H.245 et RAS
  - ILS (LDAP)
  - Messagerie instantanée
  - Options IP (RFC 791, 2113)
  - IPSec Pass Through
  - LISP
  - M3UA
  - MGCP
  - MMP
  - NetBIOS
  - PPTP
  - Gestion des comptes RADIUS
  - RSH
  - RTSP
  - SIP
  - SKINNY
  - SMTP et ESMTP
  - SNMP
  - SQL*Net
  - STUN
  - Sun RPC
  - TFTP
  - WAAS

- XDMCP
- FTP actif

Configurer les domaines MAP-T

Pour configurer MAP-T, vous créez un ou plusieurs domaines. Lorsque vous configurez MAP-T sur les périphériques client Edge (CE) et de relais frontière (BR), veillez à utiliser les mêmes paramètres pour chaque périphérique qui participera à chaque domaine.

Vous pouvez configurer jusqu'à 25 domaines MAP-T. En mode contexte multiple, vous pouvez configurer jusqu'à 25 domaines par contexte.

Procédure

Étape 1 Choisissez **Configuration Device Setup (Configuration du périphérique)** > **CGNAT Map (Carte CGNAT)**.

Étape 2 Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour créer un nouveau domaine MAP.
- Sélectionnez un domaine MAP et cliquez sur **Edit** (Modifier) pour modifier le domaine.

Si vous n'avez plus besoin du domaine, sélectionnez-le et cliquez sur **Delete** (Supprimer).

Étape 3 Dans **MAP Domain Name** (Nom du domaine MAP), saisissez un nom pour le domaine. Le nom est une chaîne alphanumérique pouvant comporter jusqu'à 48 caractères. Le nom peut également inclure les caractères spéciaux suivants : point (.), barre oblique (/) et deux-points (:).

Étape 4 Cliquez sur l'onglet **Default Mapping Rule** (Règle de mappage par défaut) et configurez **Rule IPV6 Prefix** (Préfixe IPV6 de la règle) et **Rule IPv6 Prefix Length** (Longueur du préfixe IPv6 de la règle) pour la règle.

Précisez un préfixe IPv6 à utiliser pour intégrer les adresses de destination IPv4 selon la RFC 6052. La longueur du préfixe doit normalement être de 64, mais les valeurs autorisées sont 32, 40, 48, 56, 64 ou 96. Tous les bits de fin après l'adresse IPv4 intégrée sont définis à 0. Par exemple, 2001:DB8:CAFE:CAFE::/64.

Le périphérique de relais de frontière (BR) utilise cette règle pour traduire toutes les adresses IPv4 en dehors du domaine MAP en une adresse IPv6 qui fonctionne dans le domaine MAP.

Étape 5 Cliquez sur l'onglet **Basic Mapping Rule** (Règle de mappage de base), puis configurez les préfixes d'adresse IP et les paramètres de port de la règle de mappage de base.

Le périphérique Customer Edge (CE) utilise la règle de mappage de base pour déterminer son adressage IPv4 dédié ou son affectation d'adresses et d'ensembles de ports partagés. Le périphérique CE traduit d'abord l'adresse IPv4 du système en une adresse IPv4 et un port dans le préfixe et la plage de ports du pool (à l'aide de NAT44), puis MAP traduit la nouvelle adresse IPv4 en une adresse IPv6 dans le pool défini par le préfixe IPv6 de la règle. Le paquet est ensuite prêt à être transmis sur le réseau IPv6 uniquement du fournisseur de services vers un périphérique de relais frontière (BR).

Configurez les options suivantes :

- **Rule IPV4 Prefix** (Préfixe IPV4 de la règle), **Rule IPv4 Subnet Mask** (Masque de sous-réseau IPv4 de la règle) : le préfixe IPv4 définit le pool d'adresses IPv4 pour le périphérique Customer Edge (CE).

Le périphérique CE traduit d'abord son adresse IPv4 en une adresse (et un numéro de port) dans le pool défini par le préfixe IPv4. MAP traduit ensuite cette nouvelle adresse en adresse IPv6 en utilisant le préfixe dans la règle de mappage par défaut.

Précisez une adresse réseau et un masque de sous-réseau, par exemple, 192.168.3.0 255.255.255.0. Vous ne pouvez pas utiliser le même préfixe IPv4 dans différents domaines MAP.

- **Rule IPV6 Prefix** (Préfixe IPV6 de la règle), **Rule IPv6 Prefix Length** (Longueur du préfixe IPv6 de la règle) : le préfixe IPv6 définit le pool d'adresses pour l'adresse IPv6 du périphérique CE. MAP traduit les paquets IPv6 en IPv4 uniquement si les paquets ont une adresse de destination avec ce préfixe et une adresse source avec le préfixe IPv6 défini dans la règle de mappage par défaut et se trouve dans la plage de ports correcte. Tous les paquets IPv6 envoyés au périphérique CE à partir d'autres adresses sont simplement traités comme du trafic IPv6 sans traduction MAP. Les paquets des pools de source/destination MAP, mais avec des ports hors plage, sont simplement abandonnés.

  Précisez un préfixe IPv6 et une longueur de préfixe, qui est normalement 64, mais ne peut pas être inférieure à 8. Vous ne pouvez pas utiliser le même préfixe IPv6 dans différents domaines MAP. Par exemple : 2001:DB8:FFFF:F000::/64.

- **Share Ratio** (Ratio de partage) : spécifiez le nombre de ports qui doivent se trouver dans le pool. Le nombre doit être une puissance de 2, de 1 à 65536, comme 1, 2, 4, 8, etc.

- **Start Port** (Port de début) : premier port dans le pool de ports pour l'adresse traduite. Le port que vous spécifiez doit être une puissance de 2, de 1 à 32 768, par exemple 1, 2, 4, 8, etc. Si vous souhaitez exclure les ports bien connus, commencez à 1024 ou plus.

Étape 6 Cliquez sur **OK**.

Surveillance MAP

Les rubriques suivantes expliquent comment surveiller la configuration et l'activité du MAP.

Vérification de la configuration du domaine MAP

Vous pouvez afficher les domaines de mappage et leur état pour vérifier que la configuration est correcte.

Sélectionnez **Monitoring (Surveillance)** > **Properties (Propriétés)**, puis sélectionnez **MAP Domains** (Domaines MAP) dans la table des matières. Les informations comprennent la configuration MAP et affichent le résultat de la commande **show map-domain**. Si la configuration d'un domaine n'est pas encore terminée, cela est indiqué. Un domaine incomplètement configuré n'est pas actif. Vous pouvez saisir un nom de carte et cliquer sur **Filter** (filtre) pour afficher les informations d'un seul domaine.

```
MAP Domain 1
  Default Mapping Rule
    IPv6 prefix 2001:db8:cafe:cafe::/64
  Basic Mapping Rule
    IPv6 prefix 2001:cafe:cafe:1::/64
    IPv4 prefix 192.168.3.0 255.255.255.0
    share ratio 16
    start port 1024
    PSID length 4
    PSID offset 6
```

```
    Rule EA-bit length 12

MAP Domain 2
  Default Mapping Rule
    IPv6 prefix 2001:db8:1234:1234::/64

Warning: map-domain 2 configuration is incomplete and not in effect.
```

Surveillance des messages Syslog

Si vous activez le syslog vous pouvez surveiller le comportement de MAP avec les messages desyslog suivants :

- 305018 : Traduction MAP du *nom de l'interface : adresse IP source/port source-adresse IP de destination/port de destination* vers *nom de l'interface : adresse IP source traduite/port source traduit-adresse IP de destination traduite/port de destination traduit*

  Une nouvelle traduction MAP a été effectuée. Le message affiche la source et la destination d'origine et traduites.

- 305019 : le nœud MAP à l'adresse IP/au port indiqués présente un encodage incohérent de l'ID d'ensemble de ports

  Un paquet a une adresse qui correspond aux règles de mappage de base MAP, ce qui signifie qu'il est destiné à être traduit, mais l'ID d'ensemble de port codé dans l'adresse est incohérent par RFC7599. Cela signifie probablement qu'il y a une défaillance logicielle sur le nœud MAP d'où provient ce paquet.

- 305020 : le nœud MAP avec l'adresse IP *adresse IP* n'est pas autorisé à utiliser le port *port*

  Un paquet a une adresse qui correspond aux règles de mappage de base MAP, ce qui signifie qu'il est destiné à être traduit, mais le port associé ne fait pas partie de la plage allouée à cette adresse. Cela signifie probablement qu'il y a une erreur de configuration sur le nœud MAP d'où provient ce paquet.

Historique de MAP

Nom de la caractéristique	Versions de plateforme	Description
Mappage de l'adresse et de la traduction du port (MAP-T)	9.13(1)	Le mappage de l'adresse et du port (MAP) est principalement une fonctionnalité utilisée dans les réseaux des fournisseurs de services (SP). Le fournisseur de services peut exploiter un réseau IPv6 uniquement, le domaine MAP, tout en prenant en charge les clients IPv4 uniquement et leur besoin de communiquer avec des sites IPv4 uniquement sur l'Internet public. La carte est définie dans RFC7597, RFC7598 et RFC7599. Nous avons introduit ou modifié les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **CGNAT Map (Mappage CGNAT)**, **Monitoring (Supervision)** > **Properties (Propriétés)** > **MAP Domains (Domaines MAP)**.



PARTIE IV

Politiques de service et inspection des applications

- Politique de service, à la page 267
- Premiers pas avec l'inspection du protocole de la couche application, à la page 285
- Inspection des protocoles Internet de base, à la page 305
- Inspection des protocoles vocaux et vidéo, à la page 343
- Inspection des réseaux mobiles, à la page 367



CHAPITRE 11

Politique de service

Les politiques de service offrent un moyen cohérent et flexible de configurer les fonctionnalités de l'ASA. Par exemple, vous pouvez utiliser une politique de service pour créer une configuration de délai d'expiration qui est spécifique à une application TCP particulière, par opposition à une configuration qui s'applique à toutes les applications TCP. Une politique de service comprend plusieurs actions ou règles appliquées à une interface ou appliquées globalement.

- À propos des politiques de service, à la page 267
- Lignes directrices pour les politiques de service, à la page 273
- Par défaut pour les politiques de service, à la page 275
- Configurer les politiques de service, à la page 276
- Historique des politiques de service, à la page 283

À propos des politiques de service

Les rubriques suivantes décrivent le fonctionnement des politiques de service.

Les composants d'une politique de service

Les politiques de service permettent d'appliquer des services avancés au trafic que vous autorisez. Tout trafic autorisé par les règles d'accès peut faire l'objet de politiques de service et donc recevoir un traitement spécial, comme être redirigé vers un module de service ou faire l'objet d'une inspection d'application.

Vous pouvez avoir les types de politiques de service suivants :

- Une politique globale qui s'applique à toutes les interfaces.
- Une politique de service appliquée par interface. La politique peut être un ensemble de cartes pour le trafic passant par le périphérique et le trafic de gestion dirigé vers l'interface de l'ASA plutôt que de passer par elle.

Chaque politique de service est composée des éléments suivants :

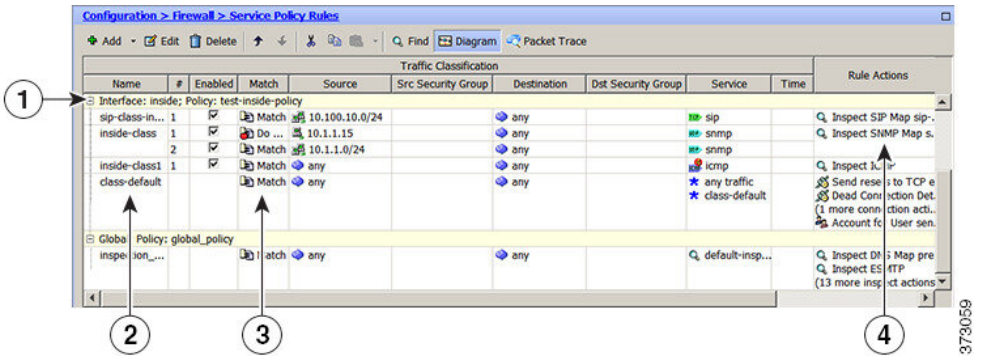
1. La liste des politiques de service, qui est l'ensemble ordonné de règles, et est nommée dans la commande **service-policy**. Dans ASDM, la liste des politiques est représentée sous forme de dossier sur la page des règles de politique de service.

2. Des règles, chaque règle étant une commande **class** dans la liste des politiques de service et les commandes associées à la commande **class**. Dans ASDM, chaque règle est affichée sur une ligne distincte, et le nom de la règle est le nom de la carte.

   La commande **class** définit les critères de correspondance de trafic pour la règle.

   Les commandes associées à la carte, telles que **inspect**, **set connection timeout**, etc., définissent les services et les contraintes à appliquer au trafic correspondant. Notez que les commandes d'inspection peuvent pointer vers des listes des politiques d'inspection, qui définissent les actions à appliquer au trafic inspecté. Gardez à l'esprit que les listes des politiques d'inspection ne sont pas la même chose que les listes des politiques de service.

L'exemple suivant compare la façon dont les politiques de service s'affichent dans l'interface de ligne de commande avec la façon dont elles s'affichent dans ASDM. Notez qu'il n'y a pas de mappage un à un entre les appels de figure et les lignes dans l'interface de ligne de commande.



L'interface de ligne de commande suivante est générée par les règles affichées dans la figure ci-dessus.

```
: Access lists used in class maps.
: In ASDM, these map to call-out 3, from the Match to the Time fields.
access-list inside_mpc line 1 extended permit tcp 10.100.10.0 255.255.255.0 any eq sip
access-list inside_mpc_1 line 1 extended deny udp host 10.1.1.15 any eq snmp
access-list inside_mpc_1 line 2 extended permit udp 10.1.1.0 255.255.255.0 any eq snmp
access-list inside_mpc_2 line 1 extended permit icmp any any
: SNMP map for SNMP inspection. Denies all but v3.
: In ASDM, this maps to call-out 4, rule actions, for the class-inside policy.
snmp-map snmp-v3only
  deny version 1
  deny version 2
  deny version 2c
: Inspection policy map to define SIP behavior.
: The sip-high inspection policy map must be referred to by an inspect sip command
: in the service policy map.
: In ASDM, this maps to call-out 4, rule actions, for the sip-class-inside policy.
policy-map type inspect sip sip-high
  parameters
    rtp-conformance enforce-payloadtype
    no traffic-non-sip
    software-version action mask log
    uri-non-sip action mask log
    state-checking action drop-connection log
    max-forwards-validation action drop log
    strict-header-validation action drop log
: Class map to define traffic matching for the inside-class rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class
```

```
  match access-list inside_mpc_1
: Class map to define traffic matching for the sip-class-inside rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map sip-class-inside
  match access-list inside_mpc
: Class map to define traffic matching for the inside-class1 rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class1
  match access-list inside_mpc_2
: Policy map that actually defines the service policy rule set named test-inside-policy.
: In ASDM, this corresponds to the folder at call-out 1.
policy-map test-inside-policy
: First rule in test-inside-policy, named sip-class-inside. Inspects SIP traffic.
: The sip-class-inside rule applies the sip-high inspection policy map to SIP inspection.
: In ASDM, each rule corresponds to call-out 2.
  class sip-class-inside
    inspect sip sip-high
: Second rule, inside-class. Applies SNMP inspection using an SNMP map.
  class inside-class
    inspect snmp snmp-v3only
: Third rule, inside-class1. Applies ICMP inspection.
  class inside-class1
    inspect icmp
: Fourth rule, class-default. Applies connection settings and enables user statistics.
  class class-default
    set connection timeout embryonic 0:00:30 half-closed 0:10:00 idle 1:00:00
reset dcd 0:15:00 5
    user-statistics accounting
: The service-policy command applies the policy map rule set to the inside interface.
: This command activates the policies.
service-policy test-inside-policy interface inside
```

Fonctionnalités configurées avec les politiques de service

Le tableau suivant répertorie les fonctionnalités que vous configurez à l'aide des politiques de service.

Tableau 8 : Fonctionnalités configurées avec les politiques de service

Fonctionnalités	Pour le trafic de transit?	Pour le trafic de gestion?	Voir :
inspection des applications (plusieurs types)	**Tous** sauf la comptabilité RADIUS	**Comptabilité RADIUS** uniquement	• Premiers pas avec l'inspection du protocole de la couche application, à la page 285. • Inspection des protocoles Internet de base, à la page 305. • Inspection des protocoles vocaux et vidéo, à la page 343. • Inspection des réseaux mobiles, à la page 367.
Filtrage de journalisation des événements sécurisés NetFlow	**Oui**	**Oui**	Consultez le guide de mise en œuvre de NetFlow.
Régulation d'entrée et de sortie QoS	**Oui**	Non	Qualité de service, à la page 441.

Fonctionnalités	Pour le trafic de transit?	Pour le trafic de gestion?	Voir :
File d'attente prioritaire standard QoS	**Oui**	Non	Qualité de service, à la page 441.
Limites et délais d'expiration de connexion TCP et UDP et répartition aléatoire du numéro de séquence TCP	**Oui**	**Oui**	Paramètres de connexion, à la page 411.
normalisationTCP	**Oui**	Non	Paramètres de connexion, à la page 411.
contournement de l'état du TCP	**Oui**	Non	Paramètres de connexion, à la page 411.
Statistiques d'utilisateurs pour le pare-feu d'identité	**Oui**	**Oui**	Consultez la commande **user-statistics** dans la référence de commande.

Sens d'application de la fonctionnalité

Les actions sont appliquées au trafic de manière bidirectionnelle ou unidirectionnelle, selon la fonctionnalité. Pour les fonctionnalités appliquées de manière bidirectionnelle, tout le trafic qui entre ou sort de l'interface à laquelle vous appliquez la liste des politiques est affecté si le trafic correspond à la carte de trafic dans les deux sens.

Remarque Lorsque vous utilisez une politique globale, toutes les fonctionnalités sont unidirectionnelles; les fonctionnalités qui sont normalement bidirectionnelles lorsqu'elles sont appliquées à une seule interface ne s'appliquent qu'au trafic entrant de chaque interface lorsqu'elles sont appliquées globalement. Comme la politique est appliquée à toutes les interfaces, la politique sera appliquée dans les deux sens, de sorte que la bidirectionnalité dans ce cas est redondante.

Pour les fonctionnalités appliquées de manière unidirectionnelle, par exemple la file d'attente de priorité QoS, seul le trafic qui entre (ou quitte, selon la fonctionnalité) l'interface à laquelle vous appliquez la liste des politiques est affecté. Consultez le tableau suivant pour connaître le sens d'application de chaque fonctionnalité.

Tableau 9 : Sens d'application sur une interface unique

Fonctionnalités	Sens d'application sur une interface unique	Sens d'application global
Inspection des applications (plusieurs types)	Bidirectionnel	Entrée
Filtrage NetFlow Secure Event Logging	S. O.	Entrée
Régulation du trafic entrant QoS	Entrée	Entrée
Régulation du trafic sortant QoS	Sortie	Sortie
File d'attente prioritaire standard QoS	Sortie	Sortie

Fonctionnalités	Sens d'application sur une interface unique	Sens d'application global
Limites et délais d'expiration de connexion TCP et UDP et répartition aléatoire du numéro de séquence TCP	Bidirectionnel	Entrée
normalisationTCP	Bidirectionnel	Entrée
contournement de l'état du TCP	Bidirectionnel	Entrée
Statistiques d'utilisateurs pour le pare-feu d'identité	Bidirectionnel	Entrée

Correspondance des fonctionnalités dans une politique de service

Un paquet correspond aux règles de classe de trafic d'une politique de service pour pour une interface donnée selon les règles suivantes :

1. Un paquet ne peut correspondre qu'à une seule règle de classe de trafic pour chaque type de fonctionnalité.
2. Lorsque le paquet correspond à une règle de trafic pour un type de fonctionnalité, l'ASA ne tente pas de le mettre en correspondance avec les règles de trafic ultérieures pour ce type de fonctionnalité.
3. Si le paquet correspond à une règle de trafic ultérieure pour un type de fonctionnalité différent, l'ASA applique également les actions pour la règle de trafic ultérieure, si elle est prise en charge. Consultez Incompatibilité de certaines actions de fonctionnalité, à la page 272 pour obtenir plus d'informations sur les combinaisons non prises en charge.



Remarque L'inspection d'application comprend plusieurs types d'inspection, et la plupart s'excluent mutuellement. Pour les inspections qui peuvent être combinées, chaque inspection est considérée comme une fonctionnalité distincte.

Exemples de mise en correspondance de paquets

Par exemple :

- Si un paquet correspond à une règle de trafic pour les limites de connexion, ainsi qu'à une règle de trafic pour une inspection d'application, les deux actions sont appliquées.
- Si un paquet correspond à une règle de trafic pour l'inspection HTTP, mais correspond également à une autre règle de trafic qui inclut l'inspection HTTP, les actions de la deuxième règle de trafic ne sont pas appliquées.
- Si un paquet correspond à une règle de trafic pour l'inspection HTTP, mais correspond également à une autre règle de trafic qui comprend l'inspection FTP, les actions de la deuxième règle de trafic ne sont pas appliquées, car les inspections HTTP et FTP ne peuvent pas être combinées.
- Si un paquet correspond à une règle de trafic pour l'inspection HTTP, mais correspond également à une autre règle de trafic qui inclut l'inspection IPv6, les deux actions sont appliquées, car l'inspection IPv6 peut être combinée avec tout autre type d'inspection.

Ordre dans lequel plusieurs actions de fonctionnalité sont appliquées

L'ordre dans lequel les différents types d'actions d'une politique de service sont exécutés est indépendant de l'ordre dans lequel ils apparaissent dans le tableau de la politique.

Les actions sont effectuées dans l'ordre suivant :

1. régulation d'entrée QoS
2. Normalisation TCP, limites et délais d'expiration de connexion TCP et UDP, randomisation du numéro de séquence TCP et contournement de l'état TCP.

Remarque Lorsque l'ASA effectue un service de proxy (comme AAA) ou qu'il modifie la charge utile TCP (comme l'inspection FTP), le normaliseur TCP agit en mode double, où il est appliqué avant et après le service de modification du proxy ou de la charge utile.

3. Inspections d'application qui peuvent être combinées avec d'autres inspections :
   1. IPv6
   2. Options IP
   3. WAAS
4. Inspections d'application qui ne peuvent pas être combinées avec d'autres inspections. Consultez Incompatibilité de certaines actions de fonctionnalité, à la page 272 pour de plus amples renseignements.
5. Régulation de sortie QoS
6. File d'attente prioritaire standard QoS

Remarque Le filtrage de la journalisation des événements sécurisés NetFlow et les statistiques d'utilisateur pour le pare-feu d'identité sont indépendants de l'ordre.

Incompatibilité de certaines actions de fonctionnalité

Certaines fonctionnalités ne sont pas compatibles entre elles pour le même trafic. La liste suivante peut ne pas inclure toutes les incompatibilités ; pour en savoir plus sur la compatibilité de chaque fonctionnalité, consultez le chapitre ou la section correspondant à la fonctionnalité :

- Vous ne pouvez pas configurer la mise en file d'attente prioritaire QoS et la régulation QoS pour le même ensemble de trafic.
- La plupart des inspections ne doivent pas être combinées avec une autre inspection, donc l'ASA n'applique qu'une seule inspection si vous configurez plusieurs inspections pour le même trafic. Les exceptions sont répertoriées dans Ordre dans lequel plusieurs actions de fonctionnalité sont appliquées, à la page 272.

Remarque La classe de trafic d'inspection par défaut, qui est utilisée dans la politique globale par défaut, est un raccourci d'interface de ligne de commande spécial pour faire correspondre les ports par défaut pour toutes les inspections. Lorsqu'elle est utilisée dans une liste des politiques, cette carte de trafic garantit que l'inspection correcte est appliquée à chaque paquet, en fonction du port de destination du trafic. Par exemple, lorsque le trafic UDP pour le port 69 atteint l'ASA, l'ASA applique l'inspection TFTP; lorsque le trafic TCP pour le port 21 arrive, l'ASA applique l'inspection FTP. Ainsi, dans ce cas uniquement, vous pouvez configurer plusieurs inspections pour la même carte de trafic. Normalement, l'ASA n'utilise pas le numéro de port pour déterminer quelle inspection appliquer, ce qui vous donne ainsi la possibilité d'appliquer des inspections à des ports non standard, par exemple.

Mise en correspondance des fonctionnalités pour plusieurs politiques de service

Pour le trafic TCP et UDP (et ICMP lorsque vous activez l'inspection ICMP dynamique), les politiques de service fonctionnent sur les flux de trafic, et pas seulement sur les paquets individuels. Si le trafic fait partie d'une connexion existante qui correspond à une fonctionnalité dans une politique sur une interface, ce flux de trafic ne peut pas également correspondre à la même fonctionnalité dans une politique sur une autre interface; seule la première politique est utilisée.

Par exemple, si le trafic HTTP correspond à une politique sur l'interface interne pour inspecter le trafic HTTP, et que vous disposez d'une politique distincte sur l'interface externe pour l'inspection HTTP, ce trafic n'est pas également inspecté à la sortie de l'interface externe. De même, le trafic de retour pour cette connexion ne sera pas inspecté par la politique d'entrée de l'interface externe ni par la politique de sortie de l'interface interne.

Pour le trafic qui n'est pas traité comme un flux, par exemple ICMP lorsque vous n'activez pas l'inspection ICMP avec état, le trafic de retour peut correspondre à une liste des politiques différente sur l'interface de retour.

Lignes directrices pour les politiques de service

Lignes directrices relatives à l'inspection

Il existe une rubrique distincte qui fournit des lignes directrices détaillées sur les politiques de service d'inspection des applications. Consultez Lignes directrices relatives à l'inspection des applications, à la page 287.

Directives IPv6

Prend en charge IPv6 pour les fonctionnalités suivantes :

- Inspection d'application pour plusieurs protocoles, mais pas tous. Pour de plus amples renseignements, consultez la section Lignes directrices relatives à l'inspection des applications, à la page 287.
- Filtrage NetFlow Secure Event Logging
- Contournement de l'état du SCTP

- Limites et délais d'expiration de connexion TCP et UDP et répartition aléatoire du numéro de séquence TCP
- normalisationTCP
- contournement de l'état du TCP
- Statistiques d'utilisateurs pour le pare-feu d'identité

Lignes directrices relatives aux cartes de trafic (classes de trafic)

Le nombre maximal de cartes de trafic (classes de trafic) de tous les types est de 255 en mode unique ou par contexte en mode multiple. Les cartes de trafic comprennent les types suivants :

- Classes de trafic de couche 3/4 (pour le trafic de transit et le trafic de gestion).
- Cartes de trafic d'inspection
- Cartes de trafic d'expressions régulières
- Commandes **match** utilisées directement sous une liste des politiques d'inspection

Cette limite inclut également les cartes de trafics par défaut de tous les types, ce qui limite les cartes de trafics configurées par l'utilisateur à environ 235.

Lignes directrices relatives aux politiques de service

- Les politiques de service d'interface sur les interfaces d'entrée prévalent sur la politique de service globale pour une fonctionnalité donnée. Par exemple, si vous avez une politique globale avec inspection FTP et une politique d'interface avec normalisation TCP, l'inspection FTP et la normalisation TCP sont appliquées à l'interface. Toutefois, si vous avez une politique globale avec inspection FTP et une politique d'interface d'entrée avec inspection FTP, seule l'inspection FTP de la politique d'interface d'entrée est appliquée à cette interface. Si aucune politique d'entrée ou globale ne met en œuvre une fonctionnalité, une politique de service d'interface sur l'interface de sortie qui spécifie la fonctionnalité est appliquée.
- Vous ne pouvez appliquer qu'une seule politique globale. Par exemple, vous ne pouvez pas créer une politique globale qui inclut l'ensemble de fonctionnalités 1 et une politique globale distincte qui inclut l'ensemble de fonctionnalités 2. Toutes les fonctionnalités doivent être incluses dans une seule politique.
- Lorsque vous apportez des modifications à la configuration de la politique de service, toutes les *nouvelles* connexions utilisent la nouvelle politique de service. Les connexions existantes continuent d'utiliser la politique qui était configurée au moment de l'établissement de la connexion. La sortie pour la commande **show** n'inclura pas de données sur les anciennes connexions.

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

  Pour vous assurer que toutes les connexions utilisent la nouvelle politique, vous devez déconnecter les connexions actuelles afin qu'elles puissent se reconnecter à l'aide de la nouvelle politique. Utilisez les commandes **clear conn** ou **clear local-host**.

Par défaut pour les politiques de service

Les rubriques suivantes décrivent les paramètres par défaut des politiques de service et le cadre de politique modulaire.

Configuration de la politique de service par défaut

Par défaut, la configuration comprend une politique qui correspond à tout le trafic d'inspection d'application par défaut et applique certaines inspections au trafic sur toutes les interfaces (politique globale). Toutes les inspections ne sont pas activées par défaut. Vous ne pouvez appliquer qu'une seule politique globale, donc si vous souhaitez modifier la politique globale, vous devez soit modifier la politique par défaut, soit la désactiver et en appliquer une nouvelle. (Une politique d'interface remplace la politique globale pour une fonctionnalité particulière.)

La politique par défaut inclut les inspections d'application suivantes :

- DNS
- FTP
- H323 (H225)
- H323 (RAS)
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny (SCCP)
- SunRPC
- SIP
- NetBios
- TFTP
- Options d'adresse IP

Cartes de trafics par défaut (classes de trafic)

La configuration comprend une carte de trafic de couche 3/4 par défaut (classe de trafic) que l'ASA utilise dans la politique globale par défaut appelée Default Inspection Traffic; il correspond au trafic d'inspection par défaut. Cette carte, qui est utilisée dans la politique globale par défaut, est un raccourci spécial pour faire correspondre les ports par défaut pour toutes les inspections.

Lorsqu'elle est utilisée dans une politique, cette carte garantit que l'inspection correcte est appliquée à chaque paquet, en fonction du port de destination du trafic. Par exemple, lorsque le trafic UDP pour le port 69 atteint l'ASA, l'ASA applique l'inspection TFTP; lorsque le trafic TCP pour le port 21 arrive, l'ASA applique

l'inspection FTP. Ainsi, dans ce cas uniquement, vous pouvez configurer plusieurs inspections pour la même carte de trafic. Normalement, l'ASA n'utilise pas le numéro de port pour déterminer quelle inspection appliquer, vous donnant ainsi la flexibilité d'appliquer des inspections à des ports non standard, par exemple.

Une autre carte de trafic qui existe dans la configuration par défaut est appelée class-default, et elle correspond à tout le trafic. Cette carte de trafic apparaît à la fin de toutes les listes des politiques de couche 3/4 et indique essentiellement à l'ASA de n'effectuer aucune action sur tout autre trafic. Si vous utilisez la classe par défaut (la classe Tout trafic dans ASDM), utilisez-la à des fins plus larges comme l'activation de l'aléatoire des séquences TCP, du décrément des TTL ou toute autre modification d'attribut facultatif. Ne l'utilisez pas pour l'inspection, car cela pourrait perturber le trafic. Certaines fonctionnalités sont uniquement disponibles pour class-default.

Configurer les politiques de service

La configuration d'une politique de service consiste à ajouter une ou plusieurs règles de politique de service par interface ou pour la politique globale. ASDM utilise un assistant pour vous guider dans le processus de création d'une politique de service. Pour chaque règle, vous identifiez les éléments suivants :

1. L'interface à laquelle vous souhaitez appliquer la règle ou la politique globale.
2. Le trafic auquel vous souhaitez appliquer les actions. Vous pouvez identifier le trafic des couches 3 et 4.
3. Les actions à appliquer à la classe de trafic. Vous pouvez appliquer plusieurs actions non incompatibles pour chaque classede trafic.

Après avoir créé une politique, vous pouvez ajouter des règles et déplacer, modifier ou supprimer des règles ou des politiques. Les rubriques suivantes expliquent comment configurer les politiques de service.

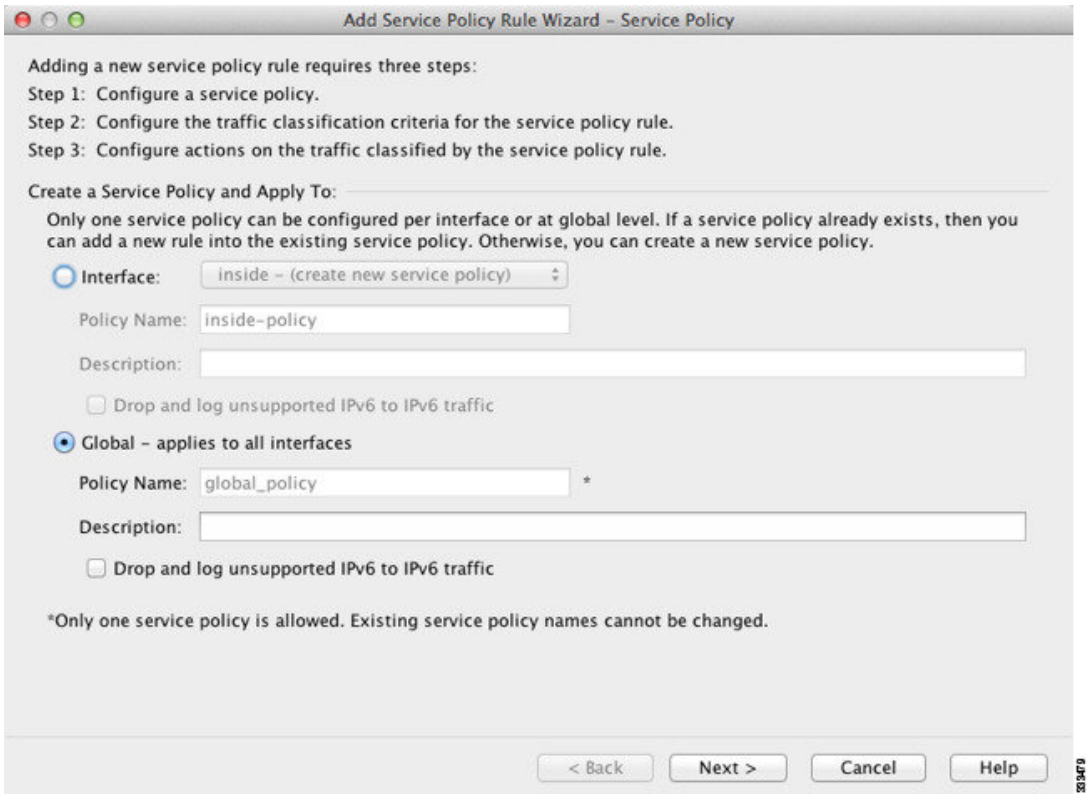
Ajouter une règle de politique de service pour le trafic de transit

Pour ajouter une règle de politique de service pour le trafic de transit, utilisez l'assistant Ajouter une règle de politique de service. Vous serez invité à choisir la portée de la politique, pour une interface spécifique ou globale :

- Les politiques de service d'interface prévalent sur la politique de service globale pour une fonctionnalité donnée. Par exemple, si vous avez une politique globale avec inspection FTP et une politique d'interface avec des limites de connexion TCP, l'inspection FTP et les limites de connexion TCP sont appliquées à l'interface. Toutefois, si vous avez une politique globale avec inspection FTP et une politique d'interface avec inspection FTP, seule l'inspection FTP de la politique d'interface est appliquée à cette interface.
- Les politiques de service globales fournissent des services par défaut à toutes les interfaces. Sauf s'ils sont remplacés par une politique spécifique à l'interface, les services globaux sont appliqués. Par défaut, il existe une politique globale qui comprend une règle de politique de service pour l'inspection d'application par défaut. Vous pouvez ajouter une règle à la politique globale à l'aide de l'assistant.

Procédure

Étape 1 Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**, puis cliquez sur **Add (Ajouter)** ou **Add** > **Add Service Policy Rule (Ajouter une règle de politique de service)**.



Étape 2 Dans la zone Créer une politique de service et l'appliquer à :

a) Choisissez si la politique s'applique à une **interface** spécifique ou **globale** à toutes les interfaces.
b) Si vous sélectionnez Interface, choisissez le nom de l'interface. Si l'interface a déjà une politique, vous ajoutez une règle à la politique existante.
c) Si l'interface n'a pas encore de politique de service, saisissez le nom de la nouvelle politique.
d) (Facultatif) Saisissez une description pour la politique.
e) (Facultatif) Cochez l'option **Drop and log unsupported IPv6 to IPv6 traffic** (Abandonner et journaliser le trafic IPv6 à IPv6 non pris en charge) pour générer un journal système (767001) pour le trafic IPv6 abandonné par les inspections d'application qui ne prennent pas en charge le trafic IPv6. Par défaut, les journaux système ne sont pas générés.
f) Cliquez sur **Next** (suivant).

Étape 3 Sur la page Traffic Classification Criteria (Critères de classification du trafic), choisissez l'une des options suivantes pour préciser le trafic auquel appliquer les actions de politique et cliquez sur **Next** (Suivant).

- **Créez une nouvelle classe de trafic.** Saisissez un nom et une description facultative.

  Déterminez le trafic à l'aide de l'un des critères suivants :

  - **Trafic d'inspection par défaut** : la classe correspond aux ports TCP et UDP par défaut utilisés par toutes les applications que l'ASA peut inspecter. Lorsque vous cliquez sur **Next** (Suivant), les services et les ports définis par cette classe s'affichent.

    Cette option, qui est utilisée dans la politique globale par défaut, est un raccourci spécial qui, lorsqu'elle est utilisée dans une règle, garantit que l'inspection correcte est appliquée à chaque paquet, en fonction du port de destination du trafic. Pour en savoir plus, consultez Cartes de trafics par défaut (classes de trafic), à la page 275.

Consultez Inspections par défaut et limites de la NAT, à la page 289 pour obtenir la liste des ports par défaut. L'ASA comprend une politique globale par défaut qui correspond au trafic d'inspection par défaut et applique les inspections courantes au trafic sur toutes les interfaces. Toutes les applications dont les ports sont inclus dans la classe Default Inspection Traffic (Trafic d'inspection par défaut) ne sont pas activées par défaut dans la liste des politiques.

Vous pouvez spécifier une classe Source and Destination IP Address (Adresse IP source et de destination) (qui utilise une ACL) avec la classe Default Inspection Traffic (Trafic d'inspection par défaut) pour restreindre le trafic correspondant. Comme la classe Default Inspection Traffic (Trafic d'inspection par défaut) spécifie les ports et les protocoles à mettre en correspondance, tous les ports et protocoles dans l'ACL sont ignorés.

- **Adresses IP source et de destination (utilise l'ACL)** : la classe correspond au trafic spécifié par une liste de contrôle d'accès étendue. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à saisir les attributs de l'entrée de contrôle d'accès et l'assistant crée l'ACL. Vous pouvez également sélectionner une liste de contrôle d'accès existante.

  Lors de la définition de l'ACE, l'option Match (Correspondance) crée une règle selon laquelle les actions sont appliquées au trafic qui correspond aux adresses. L'option Do Not Match (aucune correspondance) exempte le trafic de l'application des actions précisées. Par exemple, vous souhaitez mettre en correspondance tout le trafic dans 10.1.1.0/24 et y appliquer des limites de connexion, à l'exception de 10.1.1.25. Dans ce cas, créez deux règles, une pour 10.1.1.0/24 en utilisant l'option Match (Correspondance) et l'autre pour 10.1.1.25 à l'aide de l'option Do Not Match (aucune correspondance). Assurez-vous d'organiser les règles de sorte que la règle Do Not Match (aucune correspondance) soit au-dessus de la règle Match (Correspondance), sinon 10.1.1.25 correspondra d'abord à la règle Match (Correspondance).

  Remarque
  Lorsque vous créez une nouvelle classe de trafic de ce type, vous ne pouvez spécifier qu'une seule entrée de contrôle d'accès (ACE) au départ. Une fois que vous avez terminé d'ajouter la règle, vous pouvez ajouter des ACE supplémentaires en ajoutant une nouvelle règle à la même interface ou à la politique globale, puis en spécifiant **Add rule to existing traffic class (Ajouter une règle à la classe de trafic** existante) (voir ci-dessous).

- **Groupe de tunnels** : la classe correspond au trafic d'un groupe de tunnels (profil de connexion) auquel vous souhaitez appliquer la QoS. Vous pouvez également spécifier une autre option de correspondance de trafic pour affiner la correspondance de trafic, à l'exclusion de Any Traffic (Tout trafic), Source and Destination IP Address (Adresse IP source et de destination) (utilise une ACL) ou Default Inspection Traffic (Trafic d'inspection par défaut).

  Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à sélectionner le groupe de tunnels (vous pouvez en créer un nouveau si nécessaire). Pour contrôler chaque flux, cochez **Match flow destination IP address** (Faire correspondre l'adresse IP de destination du flux). Tout le trafic acheminé vers une adresse de destination IP unique est considéré comme un flux.

- **TCP or UDP or SCTP Destination Port** (Port de destination TCP, UDP ou SCTP) : la classe correspond à un port unique ou à une plage contiguë de ports. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à choisir le protocole et à saisir le numéro de port; cliquez sur **...** pour en choisir un déjà défini dans ASDM.

  Astuces
  Pour les applications qui utilisent plusieurs ports non contigus, utilisez Source and Destination IP Address (Adresse IP source et de destination) (utilise une ACL) pour faire correspondre chaque port.

- **Plage RTP** : la carte de trafic correspond au trafic RTP. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à saisir une plage de ports RTP comprise entre 2 000 et 65 534. Le nombre maximal de ports dans la plage est de 16 383.
- **IP DiffServ CodePoints (DSCP)** : la carte correspond à jusqu'à huit valeurs DSCP dans l'en-tête IP. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à sélectionner ou à saisir les valeurs souhaitées (déplacez-les dans la liste Correspondance sur DSCP).
- **Précédence IP** : la carte de trafic correspond à jusqu'à quatre valeurs de priorité, représentées par l'octet TOS dans l'en-tête IP. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à saisir les valeurs.
- **Tout trafic** : correspond à tout le trafic.

- **Ajouter une règle à la carte de trafic existante**. Si vous avez déjà une règle de politique de service sur la même interface ou si vous en ajoutez à la politique de service globale, cette option vous permet d'ajouter une ACE à une ACL existante. Vous pouvez ajouter une ACE à n'importe quelle liste de contrôle d'accès que vous avez créée précédemment lorsque vous avez choisi l'option d'adresse IP source et de destination (utilise l'ACL) pour une règle de politique de service sur cette interface. Pour cette classe de trafic, vous ne pouvez avoir qu'un seul ensemble d'actions de règles, même si vous ajoutez plusieurs ACE. Vous pouvez ajouter plusieurs ACE à la même classe de trafic en répérant l'ensemble de cette procédure. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à saisir les attributs de l'entrée de contrôle d'accès.
- **Utilisez une classe de trafic existante.** Si vous avez créé une classe de trafic utilisée par une règle sur une interface différente, vous pouvez réutiliser la définition de classe de trafic pour cette règle. Notez que si vous modifiez la classe de trafic pour une règle, la modification est transmise par toutes les règles qui utilisent cette classe de trafic. Si votre configuration comprend des commandes **class-map** que vous avez saisies au niveau de l'interface de ligne de commande, ces noms de carte de trafic sont également disponibles (bien que pour afficher la définition de la carte de trafic, vous devez créer la règle).
- **Utilisez la classe class-default, comme classe de trafic**. Cette option utilise la classe class-default, qui correspond à tout le trafic. La carte class-default est créée automatiquement par l'ASA et placée à la fin de la politique. Si vous ne lui appliquez aucune action, elle est toujours créée par l'ASA, mais pour des besoins internes uniquement. Vous pouvez appliquer des actions à cette carte, si vous le souhaitez, ce qui peut être plus pratique que de créer une nouvelle carte de trafic qui correspond à tout le trafic. Vous ne pouvez créer qu'une seule règle pour cette politique de service en utilisant la carte class-default, car chaque carte de trafic ne peut être associée qu'à une seule règle par politique de service.

Étape 4 Si vous avez sélectionné un critère de correspondance de trafic qui nécessite une configuration supplémentaire, saisissez les paramètres souhaités et cliquez sur **Next** (Suivant).

Étape 5 Sur la page Actions de règle, configurez une ou plusieurs actions de règle. Consultez Fonctionnalités configurées avec les politiques de service, à la page 269 pour obtenir une liste des fonctionnalités et des actions que vous pouvez appliquer, avec des pointeurs vers des détails supplémentaires.

Étape 6 Cliquez sur **Terminer**.

Ajouter une règle de politique de service pour le trafic de gestion

Pour ajouter une règle de politique de service pour le trafic dirigé vers l'ASA à des fins de gestion, utilisez l'assistant Add Service Policy Rule (Ajouter une règle de politique de service). Vous serez invité à choisir la portée de la politique, pour une interface spécifique ou globale :

- Les politiques de service d'interface prévalent sur la politique de service globale pour une fonctionnalité donnée. Par exemple, si vous avez une politique globale avec inspection de comptabilité RADIUS et une politique d'interface avec limites de connexion, la comptabilité RADIUS et les limites de connexion sont appliquées à l'interface. Toutefois, si vous avez une politique globale avec la comptabilité RADIUS et une politique d'interface avec la comptabilité RADIUS, seule la comptabilité RADIUS de la politique d'interface est appliquée à cette interface.
- Les politiques de service globales fournissent des services par défaut à toutes les interfaces. Sauf s'ils sont remplacés par une politique spécifique à l'interface, les services globaux sont appliqués. Par défaut, il existe une politique globale qui comprend une règle de politique de service pour l'inspection d'application par défaut. Vous pouvez ajouter une règle à la politique globale à l'aide de l'assistant.

Procédure

Étape 1 Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**, puis cliquez sur **Add (Ajouter)** ou **Add** > **Add Management Service Policy Rule (Ajouter une règle de politique de service de gestion)**.

Étape 2 Dans la zone Créer une politique de service et l'appliquer à :

a) Choisissez si la politique s'applique à une **interface** spécifique ou **globalement** à toutes les interfaces.
b) Si vous sélectionnez Interface, choisissez le nom de l'interface. Si l'interface a déjà une politique, vous ajoutez une règle à la politique existante.
c) Si l'interface n'a pas encore de politique de service, saisissez le nom de la nouvelle politique.
d) (Facultatif) Saisissez une description pour la politique.
e) Cliquez sur **Next** (suivant).

Étape 3 Sur la page Traffic Classification Criteria (Critères de classification du trafic), choisissez l'une des options suivantes pour préciser le trafic auquel appliquer les actions de politique et cliquez sur **Next** (Suivant).

- **Créez une nouvelle classe de trafic.** Saisissez un nom et une description facultative.

  Déterminez le trafic à l'aide de l'un des critères suivants :

  - **Adresses IP source et de destination (utilise l'ACL)** : la classe correspond au trafic spécifié par une liste de contrôle d'accès étendue. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à saisir les attributs de l'entrée de contrôle d'accès et l'assistant crée l'ACL. Vous pouvez également sélectionner une liste de contrôle d'accès existante.

    Lors de la définition de l'ACE, l'option Match (Correspondance) crée une règle selon laquelle les actions sont appliquées au trafic qui correspond aux adresses. L'option Do Not Match (aucune correspondance) exempte le trafic de l'application des actions précisées. Par exemple, vous souhaitez mettre en correspondance tout le trafic dans 10.1.1.0/24 et y appliquer des limites de connexion, à l'exception de 10.1.1.25. Dans ce cas, créez deux règles, une pour 10.1.1.0/24 en utilisant l'option Match (Correspondance) et l'autre pour 10.1.1.25 à l'aide de l'option Do Not Match (aucune correspondance). Assurez-vous d'organiser les règles de sorte que la règle Do Not Match (aucune

correspondance) soit au-dessus de la règle Match (Correspondance), sinon 10.1.1.25 correspondra d'abord à la règle Match (Correspondance).

- **TCP or UDP or SCTP Destination Port** (Port de destination TCP, UDP ou SCTP) : la classe correspond à un port unique ou à une plage contiguë de ports. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à choisir le protocole et à saisir le numéro de port; cliquez sur **...** pour en choisir un déjà défini dans ASDM.

  Astuces
  Pour les applications qui utilisent plusieurs ports non contigus, utilisez Source and Destination IP Address (Adresse IP source et de destination) (utilise une ACL) pour faire correspondre chaque port.

- **Ajoutez une règle à la classe de trafic existante**. Si vous avez déjà une règle de politique de service sur la même interface ou si vous en ajoutez à la politique de service globale, cette option vous permet d'ajouter une ACE à une ACL existante. Vous pouvez ajouter une ACE à n'importe quelle liste de contrôle d'accès que vous avez créée précédemment lorsque vous avez choisi l'option d'adresse IP source et de destination (utilise l'ACL) pour une règle de politique de service sur cette interface. Pour cette classe de trafic, vous ne pouvez avoir qu'un seul ensemble d'actions de règles, même si vous ajoutez plusieurs ACE. Vous pouvez ajouter plusieurs ACE à la même classe de trafic en répérant l'ensemble de cette procédure. Lorsque vous cliquez sur **Next** (Suivant), vous êtes invité à saisir les attributs de l'entrée de contrôle d'accès.

- **Utilisez une classe de trafic existante.** Si vous avez créé une classe de trafic utilisée par une règle sur une interface différente, vous pouvez réutiliser la définition de classe de trafic pour cette règle. Notez que si vous modifiez la classe de trafic pour une règle, la modification est transmise par toutes les règles qui utilisent cette classe de trafic. Si votre configuration comprend des commandes **class-map** que vous avez saisies au niveau de l'interface de ligne de commande, ces noms de classe de trafic sont également disponibles (bien que pour afficher la définition de la classe de trafic, vous devez créer la règle).

Étape 4 Si vous avez sélectionné un critère de correspondance de trafic qui nécessite une configuration supplémentaire, saisissez les paramètres souhaités et cliquez sur **Next** (Suivant).

Étape 5 Sur la page Actions de règle, configurez une ou plusieurs actions de règle.

- Pour configurer l'inspection de comptabilité RADIUS, choisissez une liste d'inspection dans la liste déroulante RADIUS Accounting Map (Liste de comptabilité RADIUS) ou cliquez sur **Configure** (Configurer) pour ajouter une liste. Consultez Fonctionnalités configurées avec les politiques de service, à la page 269 pour de plus amples renseignements.
- Pour configurer les paramètres de connexion, consultez Configurer les paramètres de connexion pour des classes de trafic spécifiques (tous les services), à la page 429.

Étape 6 Cliquez sur **Terminer**.

Gérer l'ordre des règles de politique de service

L'ordre des règles de politique de service sur une interface ou dans la politique globale affecte la façon dont les actions sont appliquées au trafic. Consultez les lignes directrices suivantes sur la façon dont un paquet correspond aux règles d'une politique de service :

- Un paquet ne peut correspondre qu'à une seule règle dans une politique de service pour chaque type de fonctionnalité.
- Lorsque le paquet correspond à une règle qui comprend des actions pour un type de fonctionnalité, l'ASA ne tente pas de le mettre en correspondance avec les règles ultérieures, y compris ce type de fonctionnalité.
- Si le paquet correspond à une règle ultérieure pour un type de fonctionnalité différent, l'ASA applique également les actions pour la règle ultérieure.

Par exemple, si un paquet correspond à une règle pour les limites de connexion et correspond également à une règle pour l'inspection des applications, les deux actions découlant d'une règle sont appliquées.

Si un paquet correspond à une règle d'inspection d'application, mais correspond également à une autre règle qui inclut l'inspection d'application, les actions de la deuxième règle ne sont pas appliquées.

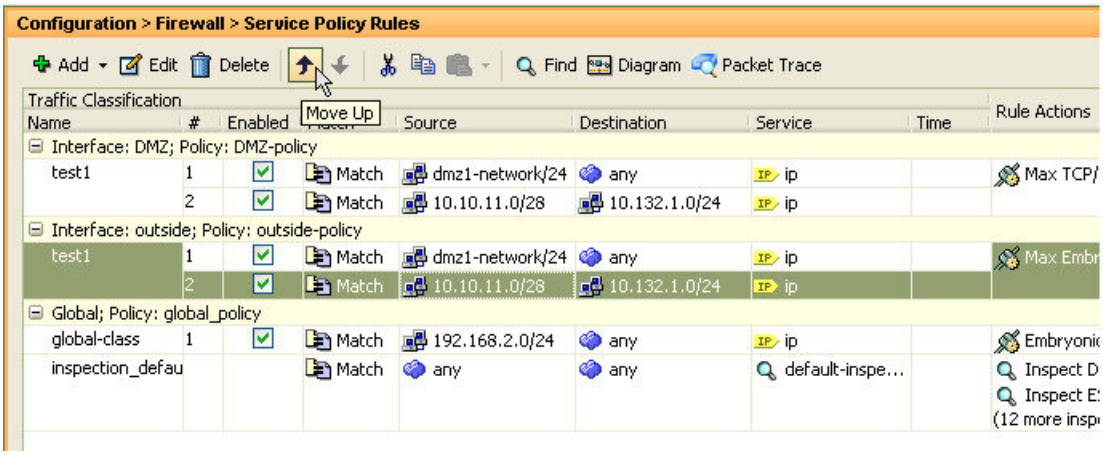
Si votre règle comprend une liste de contrôle d'accès avec plusieurs ACE, l'ordre des ACE affecte également le flux de paquets. L'ASA teste le paquet par rapport à chaque ACE dans l'ordre dans lequel les entrées sont répertoriées. Une fois qu'une correspondance est trouvée, aucune autre Ace n'est vérifiée. Par exemple, si vous créez une entrée ACE au début d'une liste de contrôle d'accès qui autorise explicitement tout le trafic, aucune autre instruction n'est jamais vérifiée.

Pour modifier l'ordre des règles ou des ACE dans une règle, procédez comme suit :

Procédure

Étape 1 Dans le volet **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**, choisissez la règle ou l'ACE que vous souhaitez déplacer vers le haut ou vers le bas.

Étape 2 Cliquez sur le bouton **Move Up** (Déplacer vers le haut) ou **Move Down** (Déplacer vers le bas).



Remarque
Si vous réorganisez les ACE dans une liste de contrôle d'accès utilisée dans plusieurs politiques de service, la modification est transmise dans toutes les politiques de service.

Étape 3 Lorsque vous avez terminé de réorganiser vos règles ou vos règles ACE, cliquez sur **Apply** (Appliquer).

Historique des politiques de service

Nom de la caractéristique	Versions	Description
Cadre de politique modulaire	7.0(1)	Le cadre de politique modulaire a été lancé.
carte de trafic de gestion à utiliser avec le trafic de comptabilité RADIUS	7.2(1)	La carte de trafic de gestion a été introduite pour une utilisation avec le trafic de comptabilité RADIUS. Les commandes suivantes ont été introduites : **class-map type management**, et **inspect radius-accounting**.
listes des politiques d'inspection	7.2(1)	La liste des politiques d'inspection a été introduite. La commande suivante a été introduite : **class-map type inspect**.
Expressions régulières et listes des politiques	7.2(1)	Les expressions régulières et les listes des politiques ont été introduites pour être utilisées dans les listes des politiques d'inspection. Les commandes suivantes ont été introduites : **class-map type regex**, **regex**, **match regex**.
match any pour les listes des politiques d'inspection	8.0(2)	Le mot-clé **match any** a été introduit pour une utilisation avec des listes des politiques d'inspection : le trafic peut correspondre à un ou plusieurs critères pour correspondre à la carte de trafic. Auparavant, uniquement **match all** était disponible.



CHAPITRE 12

Premiers pas avec l'inspection du protocole de la couche application

Les rubriques suivantes décrivent comment configurer l'inspection du protocole de couche d'application.

- Inspection des protocoles de la couche applicative, à la page 285
- Configurer l'inspection du protocole de couche d'application, à la page 293
- Configurer les expressions régulières, à la page 297
- Surveillance des politiques d'inspection, à la page 302
- Historique de l'inspection des applications, à la page 303

Inspection des protocoles de la couche applicative

Des plateformes d'inspection sont nécessaires pour les services qui intègrent des renseignements d'adressage IP dans le paquet de données des utilisateurs ou qui ouvrent des canaux secondaires sur des ports attribués de manière dynamique. Ces protocoles obligent l'ASA à effectuer une inspection approfondie des paquets au lieu de transmettre le paquet par le chemin rapide. Par conséquent, les moteurs d'inspection peuvent avoir une incidence sur le débit global. Plusieurs moteurs d'inspection courants sont activés sur l'ASA par défaut, mais vous devrez peut-être en activer d'autres en fonction de votre réseau.

Les rubriques suivantes expliquent l'inspection des applications plus en détail.

Quand utiliser l'inspection du protocole d'application

Lorsqu'un utilisateur établit une connexion, l'ASA vérifie le paquet par rapport aux ACL, crée une traduction d'adresses et crée une entrée pour la session dans le chemin rapide, afin que d'autres paquets puissent contourner les vérifications chronophages. Cependant, le chemin rapide repose sur des numéros de port prévisibles et n'effectue pas de traduction d'adresses dans un paquet.

De nombreux protocoles ouvrent des ports TCP ou UDP secondaires. La session initiale sur un port bien connu est utilisée pour négocier les numéros de port attribués dynamiquement.

D'autres applications intègrent une adresse IP dans le paquet qui doit correspondre à l'adresse source normalement traduite lorsqu'elle passe par l'ASA.

Si vous utilisez des applications comme celles-ci, vous devez activer l'inspection des applications.

Lorsque vous activez l'inspection des applications pour un service qui intègre les adresses IP, l'ASA traduit les adresses intégrées et met à jour la somme de contrôle ou les autres champs affectés par la traduction.

Lorsque vous activez l'inspection des applications pour un service qui utilise des ports affectés dynamiquement, l'ASA surveille les sessions pour identifier les affectations de ports dynamiques et permet l'échange de données sur ces ports pour la durée de la session spécifique.

Listes des politiques d'inspection

Vous pouvez configurer des actions spéciales pour de nombreuses inspection d'application à l'aide d'une *liste des politiques d'inspection*. Ces listes sont facultatives : vous pouvez activer l'inspection pour un protocole qui prend en charge les listes des politiques d'inspection sans configurer de liste. Ces listes sont nécessaires uniquement si vous souhaitez autre chose que les actions d'inspection par défaut.

Une liste des politiques d'inspection comprend un ou plusieurs des éléments suivants. Les options exactes disponibles pour une liste des politiques d'inspection dépendent de l'application.

- Critères de correspondance du trafic : vous faites correspondre le trafic d'application à des critères spécifiques à l'application, tels qu'une chaîne d'URL, pour laquelle vous activez ensuite les actions.

  Pour certains critères de correspondance de trafic, vous utilisez des expressions régulières pour faire correspondre le texte à l'intérieur d'un paquet. Assurez-vous de créer et de tester les expressions régulières avant de configurer la liste des politiques, qu'elles soient uniques ou regroupées dans une carte de trafic d'expression régulière.

- Carte de trafic d'inspection : certaines listes des politiques d'inspection vous permettent d'utiliser une carte de trafic d'inspection pour inclure plusieurs critères de correspondance de trafic. Vous identifiez ensuite la carte de trafic d'inspection dans la liste des politiques d'inspection et activez les actions pour la carte dans son ensemble. La différence entre la création d'une carte de trafic et la définition de la correspondance de trafic directement dans la liste des politiques d'inspection est que vous pouvez créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafic. Cependant, vous ne pouvez pas définir différentes actions pour différentes correspondances.

- Paramètres : les paramètres affectent le comportement du moteur d'inspection.

Pour plus d'informations, consultez les rubriques suivantes.

Remplacement d'une liste des politiques d'inspection en cours d'utilisation

Si une inspection est activée avec une liste des politiques dans une politique de service, le remplacement de la liste des politiques est un processus en deux étapes. Vous devez d'abord supprimer l'inspection de la politique de service et appliquer les modifications. Ensuite, vous le rajoutez, sélectionnez le nouveau nom de liste des politiques et appliquez à nouveau les modifications.

Comment plusieurs classes de trafic sont gérées

Vous pouvez spécifier plusieurs mappages de classes d'inspection ou correspondances directes dans la carte de politique d'inspection.

Si un paquet correspond à plusieurs classes différentes ou correspondances directes, l'ordre dans lequel l'ASA applique les actions est déterminé par les règles ASA internes, et non par l'ordre dans lequel elles sont ajoutées à la carte des politiques d'inspection. Les règles internes sont déterminées par le type d'application et la progression logique de l'analyse d'un paquet, et ne sont pas configurables par l'utilisateur. Par exemple, pour le trafic HTTP, l'analyse d'un champ méthode de requête précède l'analyse du champ Longueur de l'hôte d'en-tête ; une action pour le champ méthode de requête se produit avant l'action pour le champ Longueur de l'hôte d'en-tête.

Si une action abandonne un paquet, aucune autre action n'est effectuée dans la liste des politiques d'inspection. Par exemple, si la première action est de réinitialiser la connexion, elle ne correspondra jamais à d'autres critères de correspondance. Si la première action consiste à journaliser le paquet, une deuxième action, telle que la réinitialisation de la connexion, peut se produire.

Si un paquet correspond à plusieurs critères de correspondance qui sont identiques, ils sont mis en correspondance dans l'ordre dans lequel ils apparaissent dans la liste des politiques.

Une carte de trafic est déterminée comme étant du même type qu'une autre carte de trafic ou une correspondance directe en fonction de l'option de correspondance de priorité la plus basse dans la carte de trafic (la priorité est basée sur les règles internes). Si une carte de trafic a le même type d'option de correspondance de priorité la plus basse qu'une autre carte de trafic, les cartes de trafic sont mises en correspondance en fonction de l'ordre dans lequel elles sont ajoutées à la liste des politiques. Si la correspondance de priorité la plus basse pour chaque mappage de carte est différente, la carte de trafic avec l'option de correspondance de priorité la plus élevée est mise en correspondance en premier.

Lignes directrices relatives à l'inspection des applications

Basculement

Les informations d'état pour les sessions multimédias qui nécessitent une inspection ne sont pas transmises sur la liaison d'état pour le basculement dynamique. Les exceptions sont GTP, M3UA et SIP, qui sont répliquées sur la liaison d'état. Vous devez configurer la vérification stricte de l'état du processus de serveur d'applications (ASP) dans l'inspection M3UA pour obtenir un basculement dynamique.

Mise en grappes

Les inspections suivantes ne sont pas prises en charge dans le regroupement :

- CTIQBE
- H323, H225 et RAS
- Intercommunication IPsec
- MGCP
- MMP
- RTSP
- SCCP (Skinny)
- WAAS

IPv6

Prend en charge IPv6 pour les inspections suivantes :

- Diamètre
- DNS sur UDP
- FTP
- GTP

- HTTP
- ICMP
- Intercommunication IPsec
- IPv6
- M3UA
- SCCP (Skinny)
- SCTP
- SIP
- SMTP
- VXLAN

Prend en charge NAT64 pour les inspections suivantes :

- DNS sur UDP
- FTP
- HTTP
- ICMP
- SCTP

Directives supplémentaires

- Certains moteurs d'inspection ne prennent pas en charge la PAT, la NAT, la NAT externe ou la NAT entre les mêmes interfaces de sécurité. Pour plus d'informations sur la prise en charge de la NAT, consultez Inspections par défaut et limites de la NAT, à la page 289.
- Pour toutes les inspections d'application, l'ASA limite le nombre de connexions de données actives simultanées à 200 connexions. Par exemple, si un client FTP ouvre plusieurs connexions secondaires, le moteur d'inspection FTP n'autorise que 200 connexions actives et la connexion 201 est abandonnée et l'appliance de sécurité adaptative génère un message d'erreur du système.
- Les protocoles inspectés sont soumis à un suivi avancé de l'état TCP, et l'état TCP de ces connexions n'est pas automatiquement répliqué. Pendant que ces connexions sont répliquées sur l'unité de secours, il y a une tentative au mieux pour rétablir un état TCP.
- Si le système détermine qu'une connexion TCP nécessite une inspection, le système efface toutes les options TCP, à l'exception des options MSS et de réception sélective (SACK) sur les paquets avant de les inspecter. Les autres options sont effacées même si vous les autorisez dans une liste TCP appliquée aux connexions.
- Le trafic TCP/UDP dirigé vers l'ASA (vers une interface) est inspecté par défaut. Cependant, le trafic ICMP dirigé vers une interface n'est jamais inspecté, même si vous activez l'inspection ICMP. Ainsi, un ping (requête d'écho) à une interface peut échouer dans des circonstances spécifiques, comme lorsque la demande d'écho provient d'une source que l'ASA peut atteindre par une route de sauvegarde par défaut.

Valeurs par défaut pour l'inspection des applications

Les rubriques suivantes expliquent les opérations par défaut pour l'inspection des applications.

Inspections par défaut et limites de la NAT

Par défaut, la configuration comprend une politique qui correspond à tout le trafic d'inspection d'application par défaut et applique l'inspection au trafic sur toutes les interfaces (politique globale). Le trafic d'inspection des applications par défaut comprend le trafic vers les ports par défaut pour chaque protocole. Vous ne pouvez appliquer qu'une seule politique globale. Par conséquent, si vous souhaitez modifier la politique globale, par exemple, pour appliquer une inspection aux ports non standard ou pour ajouter des inspections qui ne sont pas activées par défaut, vous devez modifier la politique par défaut, ou désactivez-le et appliquez-en un nouveau.

Le tableau suivant répertorie toutes les inspections prises en charge, les ports par défaut utilisés dans la carte de trafic par défaut et les moteurs d'inspection qui sont activés par défaut, qui sont en gras. Ce tableau indique également toutes les limites de la NAT. Dans ce tableau :

- Les moteurs d'inspection activés par défaut pour le port par défaut sont en gras.
- L'ASA est conforme aux normes indiquées, mais il n'applique pas la conformité aux paquets inspectés. Par exemple, les commandes FTP sont censées être dans un ordre particulier, mais l'ASA ne fait pas respecter l'ordre.

Tableau 10 : Moteurs d'inspection d'applications pris en charge

Application	Protocole, port par défaut	Limites de la NAT	Normes	Commentaires
CTIQBE	TCP/2748	Pas de PAT étendue. No NAT64. (Mise en grappe) Pas de PAT statique.	—	—
DCERPC	TCP/135	No NAT64.	—	—
Diamètre	TCP/3868 TCP/5868 (pour TCP/TLS) SCTP/3868	Pas de NAT / PAT.	RFC 6733	Nécessite la licence Carrier (exploitant).
DNS sur UDP DNS sur TCP	UDP/53 UDP/443 TCP/53	Aucune prise en charge de NAT n'est disponible pour la résolution de nom par le biais de WINS.	RFC 1123	Vous devez activer l'inspection DNS/TCP dans la liste des politiques d'inspection DNS pour inspecter le DNS sur TCP. UDP/443 est utilisé uniquement pour les sessions DNScrypt de Cisco Umbrella.
FTP	TCP/21	(Mise en grappe) Pas de PAT statique.	RFC 959	—

Application	Protocole, port par défaut	Limites de la NAT	Normes	Commentaires
GTP	UDP/3386 (GTPv0) UDP/2123 (GTPv1+)	Pas de PAT étendue. Pas de NAT.	—	Nécessite la licence Carrier (exploitant).
H.323 H.225 et **RAS**	TCP/1720 UDP/1718 UDP (RAS) 1718-1719	(Mise en grappe) Pas de PAT statique. Pas de PAT étendue. Pas de NAT sur les mêmes interfaces de sécurité. No NAT64.	ITU-T H.323, H.245, H225.0, Q.931, Q.932	—
HTTP	TCP/80	—	RFC 2616	Méfiez-vous des limites de la MTU en supprimant ActiveX et Java. Si la MTU est trop faible pour permettre à la balise Java ou ActiveX d'être incluse dans un paquet, il se peut que le stripping (suppression) ne se produise pas.
ICMP	ICMP	—	—	Le trafic ICMP dirigé vers une interface ASA n’est jamais inspecté.
ERREUR ICMP	ICMP	—	—	—
ILS (LDAP)	TCP/389	Pas de PAT étendue. No NAT64.	—	—
Messagerie instantanée (IM)	Varie selon le client	Pas de PAT étendue. No NAT64.	RFC 3860	—
Options d’adresse IP	RSVP	No NAT64.	RFC 791, RFC 2113	—
Intercommunication IPsec	UDP/500	Pas de PAT No NAT64.	—	—
IPv6	—	No NAT64.	RFC 2460	—
LISP	—	Pas de NAT ou PAT.	—	—
M3UA	SCTP/2905	Pas de NAT ou PAT pour les adresses intégrées.	RFC 4666	Nécessite la licence Carrier (exploitant).

Application	Protocole, port par défaut	Limites de la NAT	Normes	Commentaires
MGCP	UDP/2427, 2727	Pas de PAT étendue. No NAT64. (Mise en grappe) Pas de PAT statique.	RFC 2705bis-05	—
MMP	TCP/5443	Pas de PAT étendue. No NAT64.	—	—
Serveur de noms NetBIOS sur IP	UDP/137, 138 (ports sources)	Pas de PAT étendue. No NAT64.	—	NetBIOS est pris en charge par l'exécution de la NAT des paquets pour le port UDP 138 du service NBNS et le port UDP 138.
PPTP	TCP/1723	No NAT64. (Mise en grappe) Pas de PAT statique.	RFC 2637	—
Gestion des comptes RADIUS	UDP/1646	No NAT64.	RFC 2865	—
RSH	TCP/514	Pas de PAT No NAT64. (Mise en grappe) Pas de PAT statique.	Berkeley UNIX	—
RTSP	TCP/554	Pas de PAT étendue. No NAT64. (Mise en grappe) Pas de PAT statique.	RFC 2326, 2327, 1889	Aucun traitement pour le masquage HTTP.
SCTP	SCTP	—	RFC 4960	Nécessite la licence Carrier (exploitant). Bien que vous puissiez effectuer une NAT d'objet réseau statique sur le trafic SCTP (sans NAT ni PAT dynamique), le moteur d'inspection n'est pas utilisé pour la NAT.

Application	Protocole, port par défaut	Limites de la NAT	Normes	Commentaires
SIP	TCP/5060 UDP/5060	Pas de NAT/PAT sur les interfaces avec des niveaux de sécurité identiques ou inférieurs ou supérieurs. Pas de PAT étendue. Pas de NAT64 ou NAT46. (Mise en grappe) Pas de PAT statique.	RFC 2543	Ne gère pas les configurations de téléphones IP Cisco téléchargées par TFTP dans certaines circonstances.
SKINNY (SCCP)	TCP/2000	Pas de NAT sur les mêmes interfaces de sécurité. Pas de PAT étendue. Pas de NAT64, NAT46 ou NAT66. (Mise en grappe) Pas de PAT statique.	—	Ne gère pas les configurations de téléphones IP Cisco téléchargées par TFTP dans certaines circonstances.
SMTP et **ESMTP**	TCP/25	No NAT64.	RFC 821, 1123	—
SNMP	UDP/161, 162 UDP/4161 sur les plateformes qui exécutent également Secure Firewall eXtensible Operating System (FXOS).	Pas de NAT ou PAT.	RFC 1155, 1157, 1212, 1213, 1215	v.2 RFC 1902-1908; v.3 RFC 2570-2580. Sur les plateformes FXOS, si vous configurez SNMP, cette inspection est activée automatiquement et vous ne pouvez pas la désactiver.
SQL*Net	TCP/1521	Pas de PAT étendue. No NAT64. (Mise en grappe) Pas de PAT statique.	—	v.1 et v.2.
STUN	TCP/3478 UDP/3478	(WebRTC) NAT statique/PAT44 uniquement. (Cisco Spark) NAT/PAT 44 et 64 statiques; et NAT/PAT dynamique.	RFC 5245, 5389	—
Sun RPC	TCP/111 UDP/111	Pas de PAT étendue. No NAT64.	—	—

Application	Protocole, port par défaut	Limites de la NAT	Normes	Commentaires
TFTP	UDP/69	No NAT64. (Mise en grappe) Pas de PAT statique.	RFC 1350	Les adresses IP de charge utile ne sont pas traduites.
WAAS	TCP/1- 65535	Pas de PAT étendue. No NAT64.	—	—
XDMCP	UDP/177	Pas de PAT étendue. No NAT64. (Mise en grappe) Pas de PAT statique.	—	—
VXLAN	UDP/4789	Sans objet	RFC 7348	Réseau local extensible virtuel.

Listes des politiques d'inspection par défaut

Certains types d'inspection utilisent des listes des politiques par défaut masquées. Par exemple, si vous activez l'inspection ESMTP sans préciser de liste, _default_esmtp_map est utilisé.

L'inspection par défaut est décrite dans les sections qui expliquent chaque type d'inspection. Vous pouvez afficher ces listes par défaut à l'aide de la commande **show running-config all policy-map** ; utilisez **Tools (Outils) > Command Line Interface (Interface de ligne de commande)**.

L'inspection DNS est la seule à utiliser une liste par défaut configurée explicitement, preset_dns_map.

Configurer l'inspection du protocole de couche d'application

Vous configurez l'inspection des applications dans les politiques de service.

L'inspection est activée par défaut globalement sur toutes les interfaces pour certaines applications sur leurs ports et protocoles standard. Consultez Inspections par défaut et limites de la NAT, à la page 289 pour obtenir plus d'informations sur les inspections par défaut. Une méthode courante pour personnaliser la configuration d'inspection consiste à personnaliser la politique globale par défaut. Vous pouvez également créer une nouvelle politique de service comme vous le souhaitez, par exemple, une politique spécifique à l'interface.

Avant de commencer

Pour certaines applications, vous pouvez effectuer des actions particulières lorsque vous activez l'inspection en configurant des listes des politiques d'inspection. Le tableau présenté plus loin dans cette procédure indique les protocoles qui prennent en charge les listes des politiques d'inspection et renvoie aux instructions permettant de les configurer. Si vous souhaitez configurer ces fonctionnalités avancées, créez la liste avant de configurer l'inspection.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**.

Étape 2 Ouvrez une règle.

- Pour modifier la politique globale par défaut, sélectionnez la règle « inspection_default » dans le dossier Global, puis cliquez sur **« Edit »** (Modifier).
- Pour créer une nouvelle règle, cliquez sur **Add (Ajouter) > Add Service Policy Rule (Ajouter une règle de politique de service)**. Passez par l'assistant jusqu'à la page Rules (Règles).
- Si vous avez une autre règle d'inspection ou une règle à laquelle vous ajoutez une inspection, sélectionnez-la et cliquez sur **Edit** (Modifier).

Si vous souhaitez faire correspondre des ports non standard, créez une nouvelle règle pour les ports non standard. Consultez Inspections par défaut et limites de la NAT, à la page 289 pour connaître les ports standard de chaque moteur d'inspection.

Vous pouvez combiner plusieurs règles dans la même politique de service si vous le souhaitez, de sorte que vous pouvez créer une règle pour faire correspondre un certain trafic et une autre pour faire correspondre un trafic différent. Toutefois, si le trafic correspond à une règle qui contient une action d'inspection, puis correspond à une autre règle qui a également une action d'inspection, seule la première règle correspondante est utilisée.

Si vous mettez en œuvre l'inspection de comptabilité RADIUS, créez plutôt une règle de politique de service de gestion. Consultez Configurer l'inspection de comptabilité RADIUS, à la page 398.

Étape 3 Sur la page ou l'onglet de l'assistant Rule Actions (Actions de règle), sélectionnez l'onglet Protocol Inspection **(Inspection du protocole)** .

Étape 4 (Pour modifier une politique en cours d'utilisation) Si vous modifiez une politique en cours d'utilisation pour utiliser une liste des politiques d'inspection différente, vous devez désactiver l'inspection, puis la réactiver avec le nouveau nom de liste des politiques d'inspection :

a) Décochez la case du protocole.
b) Cliquez sur **OK** .
c) Cliquez sur **Apply** (Appliquer).
d) Répétez ces étapes pour revenir à l'onglet **Protocol Inspection** (Inspection de protocole).

Étape 5 Sélectionnez le type d'inspection que vous souhaitez appliquer.

Vous pouvez sélectionner plusieurs options dans la classes de trafic d'inspection par défaut uniquement.

Certains moteurs d'inspection vous permettent de contrôler des paramètres supplémentaires lorsque vous appliquez l'inspection au trafic. Cliquez sur (Configure) (**Configurer**) pour le type d'inspection afin de configurer une liste des politiques d'inspection et d'autres options. Vous pouvez choisir une liste des politiques d'inspection existante ou en créer une nouvelle. Vous pouvez prédéfinir des listes des politiques d'inspection à partir de **Configuration > Firewall > Objects > Inspect Maps** (Configuration > Pare-feu > Objets > Listes d'inspection).

Le tableau suivant répertorie les protocoles que vous pouvez inspecter, qu'ils autorisent l'inspection des listes des politiques ou des cartes de trafics d'inspection, et un pointeur vers des informations détaillées sur l'inspection.

Tableau 11 : Protocoles d'inspection

Protocole	Prend en charge les listes des politiques d'inspection	Prend en charge les cartes de trafics d'inspection	Notes
CTIQBE	Non	Non	Consultez Inspection CTIQBE, à la page 343 .
DCERPC	Oui	Oui	Consultez Inspection DCERPC, à la page 305 .
Diamètre	Oui	Oui	Consultez Inspection Diameter, à la page 372. Si vous souhaitez inspecter le trafic Diameter chiffré, choisissez **Enable encrypted traffic inspection** (Activer l'inspection du trafic chiffré) et sélectionnez un proxy TLS (cliquez sur **Manage** (Gérer) pour en créer un si nécessaire).
DNS	Oui	Oui	Consultez Inspection DNS, à la page 308 . Si vous utilisez le filtre de trafic de réseau de zombies, choisissez **Enable DNS snooping** (Activer la surveillance DNS). Nous vous suggérons d'activer la surveillance DNS uniquement sur les interfaces vers lesquelles des demandes DNS externes sont transmises. L'activation de la surveillance DNS sur tout le trafic DNS UDP, y compris celui vers un serveur DNS interne, crée une charge inutile sur l'ASA. Par exemple, si le serveur DNS se trouve sur l'interface externe, vous devez activer l'inspection DNS avec surveillance pour tout le trafic DNS UDP sur l'interface externe.
ESMTP	Oui	Non	Consultez Inspection SMTP et SMTP étendue, à la page 332 .
FTP	Oui	Oui	Consultez Inspection FTP, à la page 312 . Sélectionnez **Use Strict FTP** (Utiliser le protocole FTP strict) pour sélectionner une liste des politiques d'inspection. Le protocole FTP strict augmente la sécurité des réseaux protégés en empêchant les navigateurs Web d'envoyer des commandes intégrées dans les demandes FTP.
GTP	Oui	Non	Consultez Présentation de l'inspection GTP, à la page 367.
H.323 H.225	Oui	Oui	Consultez Inspection H.323, à la page 344 .
H.323 RAS	Oui	Oui	Consultez Inspection H.323, à la page 344 .
HTTP	Oui	Oui	Consultez Inspection HTTP, à la page 317 .

Protocole	Prend en charge les listes des politiques d'inspection	Prend en charge les cartes de trafics d'inspection	Notes
ICMP	Non	Non	Consultez Inspection ICMP, à la page 321 .
Erreur ICMP	Non	Non	Consultez Inspection des erreurs ICMP, à la page 322 .
ILS	Non	Non	Consultez Inspection ILS, à la page 322 .
IM	Oui	Oui	Consultez Inspection de la messagerie instantanée, à la page 323 .
IP-Options	Oui	Non	Consultez Inspection des options IP, à la page 325 .
IPSec Pass Thru	Oui	Non	Consultez Inspection IPsec Pass Through, à la page 327 .
IPv6	Oui	Non	Consultez Inspection IPv6, à la page 328 .
LISP	Oui	Non	Pour des informations détaillées sur la configuration de LISP, y compris l'inspection, consultez le chapitre sur la mise en grappe dans le guide de configuration général.
M3UA	Oui	Non	Consultez Inspection M3UA, à la page 372.
MGCP	Oui	Non	Consultez Inspection MGCP, à la page 349 .
NetBIOS	Oui	Non	Consultez Inspection NetBIOS, à la page 330 .
PPTP	Non	Non	Consultez Inspection PPTP, à la page 331 .
Gestion des comptes RADIUS	Oui	Non	Consultez Aperçu de l'inspection de comptabilité RADIUS, à la page 374. L'inspection de comptabilité RADIUS est disponible pour une politique de service de gestion uniquement. Vous devez sélectionner une liste des politiques pour mettre en œuvre cette inspection.
RSH	Non	Non	Consultez Inspection RSH, à la page 331 .
RTSP	Oui	Non	Consultez Inspection RTSP, à la page 352 .
SCCP (Skinny)	Oui	Non	Consultez Inspection Skinny (SCCP), à la page 360 .
SCTP	Oui	Non	Consultez Inspection de la couche application SCTP, à la page 371 .

Protocole	Prend en charge les listes des politiques d'inspection	Prend en charge les cartes de trafics d'inspection	Notes
SIP	Oui	Oui	Consultez Inspection SIP, à la page 355 . Si vous souhaitez inspecter le trafic SIP chiffré, choisissez **Enable encrypted traffic inspection** (Activer l'inspection du trafic chiffré) et sélectionnez un proxy TLS (cliquez sur **Manage** (Gérer) pour en créer un, le cas échéant).
SNMP	Oui	Non	Consultez Inspection SNMP, à la page 336 .
SQLNET	Non	Non	Consultez Inspection SQL*Net, à la page 337 .
STUN	Non	Non	Consultez Inspection STUN, à la page 363.
SunRPC	Non	Non	Consultez Inspection Sun RPC, à la page 337 . La carte de trafic par défaut comprend le port UDP 111 ; Si vous souhaitez activer l'inspection SUNRPC pour le port TCP 111, vous devez créer une nouvelle carte de trafic qui correspond au port TCP 111, ajouter la carte à la politique, puis appliquer l'inspection SUNRPC à cette carte.
TFTP	Non	Non	Consultez Inspection TFTP, à la page 339 .
WAAS	Non	Non	Active l'analyse TCP de l'option 33. À utiliser lors du déploiement des produits de services d'applications pour zone étendue.
XDMCP	Non	Non	Consultez Inspection XDMCP, à la page 339 .
VXLAN	Non	Non	Consultez Inspection VXLAN, à la page 340 .

Étape 6 Cliquez sur **OK** ou **Finish** (Terminer) pour enregistrer la règle de politique de service.

Configurer les expressions régulières

Les expressions régulières définissent la mise en correspondance de modèles pour les chaînes de texte. Vous pouvez utiliser ces expressions dans certaines listes d'inspection de protocoles pour faire correspondre les paquets en fonction de chaînes telles que les URL ou le contenu de champs d'en-tête particuliers.

Créer une expression régulière

Une expression régulière correspond aux chaînes de texte soit littéralement en tant que chaînes exacte, soit en utilisant des *métacaractères* afin que vous puissiez mettre en correspondance plusieurs variantes d'une

chaîne de texte. Vous pouvez utiliser une expression régulière pour mettre en correspondance le contenu de certains trafics d'application; par exemple, vous pouvez mettre en correspondance une chaîne d'URL dans un paquet HTTP.

Avant de commencer

Consultez la commande **regex** dans la référence de commande pour obtenir des renseignements sur l'incidence sur les performances lors de la mise en correspondance d'une expression régulière et de paquets. En général, la mise en correspondance avec de longues chaînes d'entrée ou la tentative de mise en correspondance d'un grand nombre d'expressions régulières réduira les performances du système.

Remarque En tant qu'optimisation, l'ASA recherche sur l'URL désobfusquée. La désobfuscation compresse plusieurs barres obliques (/) en une seule barre oblique. Pour les chaînes qui utilisent couramment des barres obliques doubles, comme « http:// », veillez à rechercher « http:/ » à la place.

Le tableau suivant répertorie les métacaractères qui ont des significations particulières.

Tableau 12 : Métacaractères d'expressions régulières

Caractères	Description	Remarques
.	Point	Correspond à un caractère unique. Par exemple, **d.g** correspond à dog, dag, dtg et à tout mot qui contient ces caractères, tel que doggonnit.
(*exp*)	Sous-expression	Une sous-expression sépare les caractères des caractères environnants, afin que vous puissiez utiliser d'autres métacaractères sur la sous-expression. Par exemple, **d(o|a)g** correspond à dog et dag, mais **do|ag** correspond à do et ag. Une sous-expression peut également être utilisée avec des quantificateurs de répétition pour différencier les caractères destinés à la répétition. Par exemple, **ab(xy){3}z** correspond à abxyxyxyz.
|	Alternance	Correspond à l'une ou l'autre des expressions qu'il sépare. Par exemple, **dog|cat** correspond à dog ou cat.
?	Point d'interrogation	Un quantificateur qui indique qu'il y a 0 ou 1 de l'expression précédente. Par exemple, **lo?se** correspond à lse ou lose.
*	Astérisque	Un quantificateur qui indique qu'il y a 0, 1 ou n'importe quel nombre de l'expression précédente. Par exemple, **lo*se** correspond à lse, lose, loose, etc.
+	Plus	Un quantificateur qui indique qu'il y a au moins 1 de l'expression précédente. Par exemple, **lo+se** correspond à lose et loose, mais pas à lse.

Caractères	Description	Remarques
{*x*} ou {*x*,}	Quantificateur de répétition minimal	Répétez au moins *x* fois. Par exemple, **ab(xy){2,}z** correspond à abxyxyz, abxyxyxyz, etc.
[*abc*]	Classe de caractères	Correspond à l'un des caractères entre crochets. Par exemple, **[abc]** correspond à a, b ou c.
[^*abc*]	Classe de caractère négative	Correspond à un seul caractère qui n'est pas contenu dans les crochets. Par exemple, **[^abc]** correspond à tout caractère autre que a, b ou c. **[^A-Z]** correspond à tout caractère qui n'est pas une lettre majuscule.
[*a-c*]	Classe de plage de caractères	Correspond à n'importe quel caractère dans la plage. **[a-z]** correspond à n'importe quelle lettre minuscule. Vous pouvez combiner les caractères et les plages : **[abcq-z]** correspond à a, b, c, q, r, s, t, u, v, w, x, y, z, de même que [**a-cq-z]**. Le caractère de tiret (-) est littéral uniquement s'il s'agit du dernier ou du premier caractère entre crochets : **[abc-]** ou **[-abc]**.
""	Guillemets	Préserve les espaces de fin ou de début dans la chaîne. Par exemple, **« test »** conserve l'espace de début lorsqu'il recherche une correspondance.
^	Caret	Spécifie le début d'une ligne.
\	Caractère d'échappement	Lorsqu'il est utilisé avec un metacaractère, correspond à un caractère littéral. Par exemple, **\[** correspond au crochet gauche.
char	Caractères	Lorsque le caractère n'est pas un métacaractère, correspond au caractère littéral.
\r	Retour chariot	Correspond à un retour chariot 0x0d.
\n	Nouvelle ligne	Correspond à une nouvelle ligne 0x0a.
\t	Onglet	Correspond à une tabulation 0x09.
\f	Saut de page	Correspond à un saut de page 0x0c.
\x*NN*	Nombre hexadécimal échappé	Correspond à un caractère ASCII au moyen de l'hexadécimal (exactement deux chiffres).
NNN	Nombre octal échappé	Correspond à un caractère ASCII comme octal (exactement trois chiffres). Par exemple, le caractère 040 représente un espace.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Regular Expressions (Expressions régulières)**.

Étape 2 Dans la zone des expressions régulières, effectuez l'une des opérations suivantes :

- Choisissez **Add** (Ajouter) pour ajouter un nouvel objet. Saisissez un nom et éventuellement, une description.
- Choisissez un objet existant et cliquez sur **Edit** (Modifier).

Étape 3 Saisissez l'expression régulière dans le champ **Value** (Valeur) ou cliquez sur **Build** (Créer) pour obtenir de l'aide pour créer l'expression.

L'expression régulière est limitée à 100 caractères de longueur.

Si vous cliquez sur **Build** (Créer), utilisez le processus suivant pour créer l'expression :

a) Dans la zone Build Snippet (Créer un fragment), créez un composant de l'expression en utilisant les options suivantes. Consultez la zone d'aperçu du fragment de code à la fin de cette section pour voir l'expression que vous créez.

- Commence au début de la ligne (^) : indique que le fragment de code doit commencer au début d'une ligne, en utilisant le métacaractère (^). Veillez à insérer tout fragment de code avec cette option au début de l'expression régulière.
- Spécifier une chaîne de caractères : si vous essayez de faire correspondre une chaîne en particulier, comme un mot ou une expression, saisissez la chaîne.

  S'il y a des métacaractères dans votre chaîne de texte que vous souhaitez utiliser littéralement, choisissez **Escape Special Characters** (Échapper les caractères spéciaux) pour ajouter le caractère d'échappement de barre oblique inverse avant eux. Par exemple, si vous saisissez « example.com », cette option le convertit en « example.com ».

  Si vous souhaitez faire correspondre les majuscules et les minuscules, choisissez **Ignore Case** (Ignorer la casse). Par exemple, « cats » est converti en « [cC][aA][tT][sS] ».

- Préciser le caractère : si vous essayez de mettre en correspondance un type de caractère ou un ensemble de caractères spécifique, plutôt qu'une phrase particulière, sélectionnez cette option et identifiez les caractères à l'aide de ces options :
  - **Négation du caractère** : spécifie ne pas correspondre au caractère que vous identifiez.
  - **Tout caractère (.)** : insère le metacaractère du point (.) pour correspondre à n'importe quel caractère. Par exemple, **d.g** correspond à dog, dag, dtg et à tout mot qui contient ces caractères, tel que doggonnit.
  - **Ensemble de caractères** : insère un ensemble de caractères. Le texte peut correspondre à n'importe quel caractère dans l'ensemble. Par exemple, si vous spécifiez [0-9A-Za-z], ce fragment de code correspondra à tout caractère de A à Z (majuscules ou minuscules) ou à tout chiffre de 0 à 9. L'ensemble [\n\f\r\t] correspond à une nouvelle ligne, à un saut de page, à un retour chariot ou à une tabulation.

- **Caractère spécial** : insère un caractère qui nécessite un échappement, y compris , ?, *, +, |, ., [, (, ou ^. Le caractère d'échappement est la barre oblique inverse , qui est automatiquement saisie lorsque vous choisissez cette option.
- **Caractère d'espacement** : les caractères d'espacement comprennent \n (nouvelle ligne), \f (saut de page), \r (retour chariot) ou \t (tabulation).
- **Nombre octal à trois chiffres** : correspond à un caractère ASCII sous forme octale (jusqu'à trois chiffres). Par exemple, le caractère \040 représente un espace. La barre oblique inverse (\) est saisie automatiquement.
- **Nombre hexadécimal à deux chiffres** : correspond à un caractère ASCII en utilisant l'hexadécimal (exactement deux chiffres). La barre oblique inverse (\) est saisie automatiquement.
- **Caractère précisé** : saisissez un seul caractère.

b) Ajoutez le fragment de code à la zone d'expression régulière en utilisant l'un des boutons suivants. Notez que vous pouvez également taper directement dans l'expression régulière.

- **Ajouter le fragment** : ajoute le fragment à la fin de l'expression régulière.
- **Ajouter le fragment comme variante** : ajoute le fragment de code à la fin de l'expression régulière séparé par une barre verticale (|), qui correspond à l'une ou l'autre des expressions qu'elle sépare. Par exemple, **dog|cat** correspond à dog ou cat.
- **Insérer le fragment au curseur)** : insère le fragment au curseur.

c) Répétez le processus pour ajouter des fragments jusqu'à ce que l'expression soit terminée.

d) (Facultatif) Dans **Occurrences de sélection**, sélectionnez la fréquence à laquelle l'expression ou des parties de celle-ci doivent correspondre au texte pour être considérées comme une correspondance. Sélectionnez du texte dans le champ Expression régulière, cliquez sur l'une des options suivantes, puis cliquez sur **Appliquer à la sélection**. Par exemple, si l'expression régulière est « test me » et que vous sélectionnez « me » et appliquez **Une ou plusieurs fois**, l'expression régulière passe à « test (me)+ ».

- **Zéro ou une fois (?)** : Il y a 0 ou 1 de l'expression précédente. Par exemple, **lo?se** correspond à lse ou lose.
- **Une ou plusieurs fois (+)** : il y a au moins 1 de l'expression précédente. Par exemple, **lo+se** correspond à lose et loose, mais pas à lse.
- **Un nombre quelconque de fois (*)** : il y a 0, 1 ou un nombre quelconque de l'expression précédente. Par exemple, **lo*se** correspond à lse, lose, loose, etc.
- **Au moins :**répétez au moins *x* fois. Par exemple, **ab(xy){2,}z** correspond à abxyxyz, abxyxyxyz, etc.
- **Exactement** : répétez exactement *x* fois. Par exemple, **ab(xy){3}z** correspond à abxyxyxyz.

e) Cliquez sur **Test** (Tester) pour vérifier que votre expression correspondra au texte prévu. Si le test échoue, vous pouvez essayer de le modifier dans la boîte de dialogue de test ou revenir au générateur d'expression. Si vous modifiez l'expression dans la boîte de dialogue de texte et que vous cliquez sur **OK**, les modifications sont enregistrées et répercutées dans le générateur d'expression.

f) Cliquez sur **OK** .

Créer une carte de trafic d'expression régulière

Une carte de trafic d'expression régulière identifie une ou plusieurs expressions régulières. Il s'agit simplement d'un ensemble d'objets d'expression régulière. Vous pouvez utiliser une carte de trafic d'expression régulière dans de nombreux cas pour remplacer un objet d'expression régulière.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Regular Expressions (Expressions régulières)**.

Étape 2 Dans la zone Regular Expressions Classes (Listes d'expressions régulières), effectuez l'une des opérations suivantes :

- Choisissez **Ajouter** (Ajouter) pour ajouter une nouvelle carte de trafic. Saisissez un nom et éventuellement, une description.
- Choisissez une carte de trafic existante et cliquez sur **Edit** (Modifier).

Étape 3 Sélectionnez les expressions que vous souhaitez dans la liste et cliquez sur **Add** (Ajouter). Supprimez tout ce que vous ne souhaitez pas.

Étape 4 Cliquez sur **OK**.

Surveillance des politiques d'inspection

Pour surveiller les politiques de service d'inspection, entrez les commandes suivantes. Sélectionnez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)** pour entrer ces commandes. Consultez la référence de commande sur Cisco.com pour obtenir une syntaxe détaillée et des exemples.

- **show service-policy inspect** *protocol*

  Affiche les statistiques pour les politiques de service d'inspection. Le *protocole* est le protocole de la commande inspect, par exemple **dns**. Cependant, tous les protocoles d'inspection n'affichent pas de statistiques avec cette commande. Par exemple :

```
asa# show service-policy inspect dns

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
asa#
```

- **show conn**

Affiche les connexions actuelles pour le trafic passant par le périphérique. Cette commande dispose d'un large éventail de mots-clés afin que vous puissiez obtenir des informations sur les différents protocoles.

- Commandes supplémentaires pour des protocoles inspectés spécifiques :
  - **show ctiqbe**

    Affiche les renseignements sur les connexions de support attribuées par le moteur d'inspection CTIQBE
  - **show h225**

    Affiche les informations sur les sessions H.225.
  - **show h245**

    Affiche les informations sur les sessions H.245 établies par les terminaux à l'aide du démarrage lent.
  - **show h323 ras**

    Affiche les informations de connexion pour les sessions RAS H.323 établies entre un portier et son terminal H.323.
  - **show mgcp** {**commands** | **sessions**}

    Affiche le nombre de commandes MGCP dans la file d'attente de commandes ou le nombre de sessions MGCP existantes.
  - **show sip**

    Affiche les informations pour les sessions SIP.
  - **show skinny**

    Affiche les informations pour les sessions Skinny (SCCP).
  - **show sunrpc-server active**

    Affiche les passages ouverts pour les services Sun RPC.

Historique de l'inspection des applications

Nom de la caractéristique	Versions	Description
listes des politiques d'inspection	7.2(1)	La liste des politiques d'inspection a été introduite. La commande suivante a été introduite : **class-map type inspect**.
Expressions régulières et listes des politiques	7.2(1)	Les expressions régulières et les listes des politiques ont été introduites pour être utilisées dans les listes des politiques d'inspection. Les commandes suivantes ont été introduites : **class-map type regex**, **regex**, **match regex**.
Correspondance de n'importe quel pour les listes des politiques d'inspection	8.0(2)	Le mot-clé **match any** a été introduit pour une utilisation avec des listes des politiques d'inspection : le trafic peut correspondre à un ou plusieurs critères pour correspondre à la carte de trafic. Auparavant, uniquement **match all** était disponible.



CHAPITRE 13

Inspection des protocoles Internet de base

Les rubriques suivantes expliquent l'inspection des applications pour les protocoles Internet de base. Pour en savoir plus sur la raison pour laquelle vous devez utiliser l'inspection pour certains protocoles et sur les méthodes globales d'application de l'inspection, consultez Premiers pas avec l'inspection du protocole de la couche application, à la page 285.

- Inspection DCERPC, à la page 305
- Inspection DNS, à la page 308
- Inspection FTP, à la page 312
- Inspection HTTP, à la page 317
- Inspection ICMP, à la page 321
- Inspection des erreurs ICMP, à la page 322
- Inspection ILS, à la page 322
- Inspection de la messagerie instantanée, à la page 323
- Inspection des options IP, à la page 325
- Inspection IPsec Pass Through, à la page 327
- Inspection IPv6, à la page 328
- Inspection NetBIOS, à la page 330
- Inspection PPTP, à la page 331
- Inspection RSH, à la page 331
- Inspection SMTP et SMTP étendue, à la page 332
- Inspection SNMP, à la page 336
- Inspection SQL*Net, à la page 337
- Inspection Sun RPC, à la page 337
- Inspection TFTP, à la page 339
- Inspection XDMCP, à la page 339
- Inspection VXLAN, à la page 340
- Historique de l'inspection du protocole Internet de base, à la page 340

Inspection DCERPC

L'inspection DCERPC n'est pas activée dans la politique d'inspection par défaut, vous devez donc l'activer si vous avez besoin de cette inspection. Vous pouvez simplement modifier la politique d'inspection globale par défaut pour ajouter l'inspection DCERPC. Vous pouvez également créer une nouvelle politique de service comme vous le souhaitez, par exemple, une politique spécifique à l'interface.

Les sections suivantes décrivent le moteur d'inspection DCERPC.

Présentation de DCERPC

L'appel de procédure à distance de Microsoft (MSRPC), basé sur DCERPC, est un protocole très utilisé par les applications client et serveur distribuées de Microsoft qui permet aux clients logiciels d'exécuter des programmes sur un serveur à distance.

Cela implique généralement qu'un client interroge un serveur appelé mappeur de terminaux à l'écoute sur un numéro de port bien connu pour obtenir les informations réseau allouées dynamiquement d'un service requis. Le client établit ensuite une connexion secondaire avec l'instance de serveur qui fournit le service. Le périphérique de sécurité autorise le numéro de port et l'adresse réseau appropriés et applique également la NAT, le cas échéant, pour la connexion secondaire.

Le moteur d'inspection DCERPC inspecte la communication TCP native entre l'EPM et le client sur le port TCP 135 bien connu. Les opérations de mappage et de recherche d'EPM sont prises en charge pour les clients. Le client et le serveur peuvent se trouver dans n'importe quelle zone de sécurité. L'adresse IP du serveur intégré et le numéro de port sont reçus à partir des messages de réponse EPM applicables. Étant donné qu'un client peut tenter plusieurs connexions au port de serveur renvoyé par EPM, l'utilisation multiple de passages est autorisée, avec des délais d'expiration configurables.

L'inspection DCE prend en charge les identifiants universels uniques (UUID) et les messages suivants :

- UUID du mappeur de terminal (EPM). Tous les messages EPM sont pris en charge.
- UUID ISystemMapper (non EPM). Les messages pris en charge sont les suivants :
  - RemoteCreateInstance opnum4
  - RemoteGetClassObject opnum3
- UUID d'OxidResolver (non EPM). Le message pris en charge est :
  - ServerAlive2 opnum5
- Tout message qui ne contient pas d'adresse IP ou d'informations de port, car ces messages ne nécessitent pas d'inspection.

Configurer une liste des politiques d'inspection DCERPC

Pour spécifier des paramètres d'inspection DCERPC supplémentaires, créez une liste des politiques d'inspection DCERPC. Vous pouvez ensuite appliquer la liste des politiques d'inspection lorsque vous activez l'inspection DCERPC.

Lors de la définition des critères de correspondance du trafic, vous pouvez soit créer une carte de trafic, soit inclure les instructions de correspondance directement dans la liste des politiques. La différence entre la création d'une carte de trafic et la définition de la correspondance de trafic directement dans la liste des politiques d'inspection est que vous pouvez réutiliser les cartes de trafic. La procédure suivante couvre les listes des politiques d'inspection, mais explique également les critères de correspondance de trafic disponibles dans la carte de trafic. Pour créer une carte de trafic, sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Class Maps (Cartes de trafic)** > **DCERPC (DCERPC**).

Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **DCERPC**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier le niveau de sécurité directement ou cliquer sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Security Level** (Niveau de sécurité) de la boîte de dialogue DCERPC Inspect Map (Liste d'inspection DCERPC), sélectionnez le niveau qui correspond le mieux à la configuration souhaitée.

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection DCERPC.

Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails) et poursuivez la procédure.

Astuces
Le bouton **UUID Filtering** (filtrage UUID) est un raccourci pour configurer le filtrage des messages, qui est expliqué plus loin dans cette procédure.

Étape 5 Configurez les options souhaitées.

- **Pinhole Timeout** (Délai d'expiration du passage) : définit le délai d'expiration du passage. Comme un client peut utiliser les informations de serveur renvoyées par le mappeur de point de terminaison pour plusieurs connexions, la valeur du délai d'expiration est configurable en fonction de l'environnement de l'application client. La plage est comprise entre 0:0:1 et 1193:0:0.
- **Enforce endpoint-mapper service** (Appliquer le service de mappage de point de terminaison) : indique s'il faut appliquer le service de mappage de point de terminaison lors de la liaison afin que seul le trafic de service soit traité.
- **Enable endpoint-mapper service lookup** (Activer la recherche du service de mappage de point de terminaison) : indique s'il faut activer l'opération de recherche du service de mappage de point de terminaison. Vous pouvez également appliquer un délai d'expiration pour la recherche de service. Si vous ne configurez pas de délai d'expiration, le pinhole timeout est utilisé.

Étape 6 (Facultatif) Cliquez sur l'onglet **Inspections** et définissez les actions à entreprendre pour des types de messages particuliers.

Vous pouvez définir les critères de correspondance du trafic en fonction des cartes de trafic DCERPC, en configurant les correspondances directement dans la liste d'inspection, ou les deux.

a) Effectuez l'une des actions suivantes :
   - Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
   - Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez **Single Match** (Correspondance unique) pour définir le critère directement, ou **Multiple Match** (Correspondance multiple), auquel cas vous sélectionnez la carte de trafic DCERPC qui définit les critères.
c) Si vous définissez le critère ici, choisissez le type de correspondance : **Match** (Correspondance) (le trafic doit correspondre au critère) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au critère). Ensuite, sélectionnez l'UUID souhaité :
   - **ms-rpc-epm**: correspond aux messages EPM Microsoft RPC.
   - **ms-rpc-isystemactivator**: correspond aux messages ISystemMapper.
   - **ms-rpc-oxidresolver**: correspond aux messages OxidResolver.

d) Choisissez de réinitialiser ou de journaliser la connexion avec **Reset** (Réinitialiser) ou **Log** (Journaliser). Vous pouvez également activer la journalisation si vous choisissez de réinitialiser la connexion. La réinitialisation de la connexion abandonne le paquet, ferme la connexion et envoie une réinitialisation TCP au serveur ou au client.
e) Cliquez sur **OK** pour ajouter le critère. Répétez le processus au besoin.

Étape 7 Cliquez sur **OK**.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection DCERPC.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection DNS

L'inspection DNS est activée par défaut. Vous ne devez le configurer que si vous souhaitez un traitement autre que celui par défaut. Les sections suivantes décrivent l'inspection des applications DNS.

Valeurs par défaut pour l'inspection DNS

L'inspection DNS est activée par défaut, à l'aide de la carte de trafic d'inspection preset_dns_map :

- La longueur maximale du message DNS est de 512 octets.
- L'inspection DNS sur TCP est désactivée.
- La longueur maximale du message DNS du client est automatiquement définie pour correspondre à l'enregistrement de ressource.

- La protection DNS est activée, de sorte que l'ASA supprime la session DNS associée à une requête DNS dès que la réponse DNS est transmise par l'ASA. L'ASA surveille également l'échange de messages pour s'assurer que l'ID de la réponse DNS correspond à l'ID de la requête DNS.
- La traduction de l'enregistrement DNS en fonction de la configuration NAT est activée.
- L'application du protocole est activée, ce qui permet la vérification du format du message DNS, y compris une longueur de nom de domaine d'au plus 255 caractères, une longueur d'étiquette de 63 caractères, la compression et la vérification des pointeurs en boucle.

Remarque Une utilisation élevée du processeur est susceptible de se produire dans Cisco ASA lorsqu'un grand nombre de paquets est inspecté par seconde. À mesure que le nombre de paquets traités augmente, en particulier lorsque le périphérique approche de son débit ou de sa capacité de connexion maximum, l'utilisation du processeur augmente également. En effet, l'ASA doit effectuer plus d'opérations par seconde, ce qui augmente la consommation des ressources du processeur.

Configurer la liste des politiques d'inspection DNS

Vous pouvez créer une liste des politiques d'inspection DNS pour personnaliser les actions d'inspection DNS si le comportement d'inspection par défaut n'est pas suffisant pour votre réseau.

Vous pouvez éventuellement créer une carte de trafic d'inspection DNS pour définir la classe de trafic pour l'inspection DNS. L'autre option consiste à définir les classes de trafic directement dans la liste des politiques d'inspection DNS. La différence entre la création d'une carte de trafic et la définition de la correspondance de trafic directement dans la liste d'inspection est que vous pouvez créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafic. Bien que cette procédure explique les listes d'inspection, les critères de correspondance utilisés dans les cartes de trafics sont les mêmes que ceux expliqués à l'étape relative à l'onglet **Inspection**. Vous pouvez configurer les cartes de trafics DNS en sélectionnant **Configuration** > **Firewall** > **Objects** > **Class Maps (Cartes de trafic)** > **DNS**, ou en les créant lors de la configuration de la liste d'inspection.

Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **DNS** .

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier le niveau de sécurité directement ou cliquer sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Security Level** (Niveau de sécurité) de la boîte de dialogue DNS Inspect Map (Liste d'inspection DNS), sélectionnez le niveau qui correspond le mieux à la configuration souhaitée. Le niveau par défaut est Low (Bas).

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection DNS.

Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails) et poursuivez la procédure.

Étape 5 Cliquez sur l'onglet **Conformité du protocole** et choisissez les options souhaitées :

- **Enable DNS guard function (Activer la fonction de protection DNS)** : à l'aide de DNS Guard, l'ASA supprime la session DNS associée à une requête DNS dès que la réponse DNS est transmise par l'ASA. L'ASA surveille également l'échange de messages pour s'assurer que l'ID de la réponse DNS correspond à l'ID de la requête DNS.
- **Enable NAT re-write function** (Activer la fonction de réécriture de la NAT) : traduit l'enregistrement DNS en fonction de la configuration NAT.
- **Enable protocol enforcement** (Activer l'application du protocole) : active la vérification du format du message DNS, y compris la longueur du nom de domaine d'au plus 255 caractères, la longueur d'étiquette de 63 caractères, la compression et la vérification des pointeurs en boucle.
- **Randomiser l'identifiant DNS pour la requête DNS**.
- **Activer l'inspection TCP** : active l'inspection du trafic DNS sur TCP. Assurez-vous que le trafic DNS/TCP du port 53 fait partie de la carte de trafic à laquelle vous appliquez l'inspection DNS. La carte de trafic d'inspection par défaut comprend TCP/53.
- **Enforce TSIG resource record to be present in DNS message** (Appliquer la présence de l'enregistrement de ressource TSIG dans le message DNS) : vous pouvez abandonner ou journaliser les paquets non conformes, et éventuellement journaliser les paquets abandonnés.

Étape 6 Cliquez sur l'onglet **Filtering** (Filtrage) et choisissez les options souhaitées.

- Paramètres globaux : choisissez s'il faut abandonner les paquets qui dépassent la longueur maximale spécifiée, qu'ils proviennent du client ou du serveur, de 512 à 65535 octets.
- Paramètres du serveur : **abandon des paquets qui dépassent la longueur maximale spécifiée** et **abandon des paquets envoyés au serveur qui dépassent la longueur indiquée par le RR** : définit la longueur maximale du message DNS du serveur, de 512 à 65 535 octets, ou définit la longueur maximale à la valeur dans l'enregistrement de ressource. Si vous activez les deux paramètres, la valeur la plus basse est utilisée.

- Paramètres du client : **abandon des paquets qui dépassent la longueur maximale spécifiée** et **abandon des paquets envoyés au serveur qui dépassent la longueur indiquée par le RR** : définit la longueur maximale du message DNS du client, de 512 à 65 535 octets, ou définit la longueur maximale à la valeur dans l'enregistrement de ressource. Si vous activez les deux paramètres, la valeur la plus basse est utilisée.

Étape 7 Cliquez sur l'onglet **Mismatch Rate** (Taux de non-concordance) et choisissez d'activer la journalisation lorsque le taux de non-concordance de l'ID DNS dépasse le seuil spécifié. Par exemple, vous pouvez définir un seuil de 30 incompatibilités par 3 secondes.

Étape 8 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

Vous pouvez définir les critères de correspondance du trafic en fonction des cartes de trafic DNS, en configurant les correspondances directement dans la liste d'inspection, ou les deux.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez **Single Match** (Correspondance unique) pour définir le critère directement, ou **Multiple Match** (Correspondance multiple), auquel cas vous sélectionnez la carte de trafic DNS qui définit les critères.

c) Si vous définissez le critère ici, choisissez le type de correspondance : **Match** (Correspondance) (le trafic doit correspondre au critère) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au critère). Par exemple, si No Match est sélectionné sur la chaîne « example.com », tout trafic contenant « example.com » est exclu de la carte de trafic. Configurez ensuite le critère comme suit :

- Indicateur d'en-tête : sélectionnez si l'indicateur doit être égal ou contenir la valeur spécifiée, puis sélectionnez le nom de l'indicateur d'en-tête ou saisissez la valeur hexadécimale de l'en-tête (0x0 à 0xfff). Si vous sélectionnez plusieurs valeurs d'en-tête, « Égal » nécessite la présence de tous les indicateurs et « Contient » que l'un des indicateurs est présent, dans le paquet. Les noms d'indicateurs d'en-tête sont **AA** (réponse faisant autorité), **QR** (requête), **RA** (récursivité disponible), **RD** (récursivité souhaitée), **TC** (troncage).
- Type : nom ou valeur du champ Type de DNS dans le paquet. Les noms des champs sont **A** (adresse IPv4), **AXFR** (transfert de zone complet), **CNAME** (nom canonique), **IXFR** (transfert de zone supplémentaire), **NS** (serveur de nom faisant autorité), **SOA** (démarrage d'une zone d'autorité) ou **TSIG** (signature de transaction). Les valeurs sont des nombres quelconques dans le champ Type de DNS de 0 à 65535 : saisissez une valeur spécifique ou une plage de valeurs.
- Classe : nom ou valeur du champ Classe DNS dans le paquet. Internet est le seul nom de champ possible. Les valeurs sont des nombres quelconques dans le champ carte DNS de 0 à 65 535 : saisissez une valeur spécifique ou une plage de valeurs.
- Question : la partie question d'un message DNS.
- Enregistrement de ressource : enregistrement de la ressource DNS. Choisissez si vous souhaitez faire correspondre la section de l'enregistrement de ressource supplémentaire, de réponse ou d'autorité.

d) Choisissez l'action principale à effectuer pour le trafic correspondant : abandonner le paquet, abandonner la connexion, masquer (pour les correspondances d'indicateur d'en-tête uniquement) ou aucune.

e) Choisissez d'activer ou de désactiver la journalisation. Vous devez désactiver la journalisation si vous souhaitez appliquer TSIG.

f) Choisissez s'il faut appliquer la présence d'un enregistrement de ressource TSIG. Vous pouvez abandonner le paquet, le journaliser, ou l'abandonner et le journaliser. Généralement, vous devez sélectionner **Primary Action (Action principale) : None** (Aucun) et **Log (Journal) : Disable** (Désactiver) pour appliquer TSIG. Cependant, pour les correspondances d'indicateurs d'en-tête, vous pouvez appliquer TSIG avec l'action principale de masque.

g) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 9 Cliquez sur l'onglet **Cisco Umbrella Connections (connexions Cisco Umbrella)** et activez la connexion à Cisco Umbrella dans le nuage.

Les options de cet onglet ne fonctionnent que si vous configurez la connexion Cisco Umbrella sur la page **Configuration** > **Firewall** > **(Pare-feu)** > **Objects** > **(Objets)** > **Umbrella**. Vous devez ensuite configurer les options de cet onglet pour que l'appareil s'enregistre auprès de Cisco Umbrella, afin que l'appareil puisse rediriger les recherches DNS vers Cisco Umbrella. Cisco Umbrella peut ensuite appliquer vos politiques de sécurité basées sur FQDN. Pour en savoir plus, consultez Cisco Umbrella, à la page 95.

- **Umbrella** : active Cisco Umbrella. Vous pouvez éventuellement spécifier le nom de la politique Cisco Umbrella à appliquer au périphérique dans le champ **Umbrella Tag** (Balise Cisco Umbrella). Si vous ne spécifiez pas de politique, la politique par défaut est appliquée. Après l'enregistrement, l'ID de l'appareil Cisco Umbrella s'affiche à côté de la balise.
- **Enable DNScrypt** (Activer DNScrypt) : active DNScrypt pour chiffrer les connexions entre le périphérique et Cisco Umbrella. L'activation de DNScrypt démarre le fil d'échange de clés avec le résolveur Umbrella. Le fil d'échange de clés effectue l'établissement de liaison avec le résolveur toutes les heures et met à jour le périphérique avec une nouvelle clé secrète. Comme DNScrypt utilise UDP/443, vous devez vous assurer que la carte de trafic utilisée pour l'inspection DNS comprend ce port. Notez que la classe d'inspection par défaut comprend déjà UDP/443 pour l'inspection DNS.
- **Fail Open** (Autoriser en cas de défaillance) : activez cette option si vous souhaitez que la résolution DNS continue de fonctionner lorsque le serveur DNS Cisco Umbrella est indisponible. En cas d'échec de l'ouverture, si le serveur DNS Cisco Umbrella n'est pas disponible, Cisco Umbrella se désactive dans cette liste des politiques et permet aux demandes DNS d'accéder aux autres serveurs DNS configurés sur le système, le cas échéant. Lorsque les serveurs DNS Cisco Umbrella sont de nouveau disponibles, la liste des politiques reprend de leur utilisation. Si vous ne sélectionnez pas cette option, les requêtes DNS continuent d'être acheminées vers le résolveur Cisco Umbrella inaccessible, de sorte qu'elles ne recevront pas de réponse

Étape 10 Cliquez sur **OK** dans la boîte de dialogue de la liste d'inspection DNS.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection DNS.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection FTP

L'inspection FTP est activée par défaut. Vous ne devez le configurer que si vous souhaitez un traitement autre que celui par défaut. Les sections suivantes décrivent le moteur d'inspection FTP.

Présentation de l'inspection FTP

L'inspection d'application FTP inspecte les sessions FTP et effectue quatre tâches :

- Prépare les canaux de connexion de données secondaires dynamiques pour le transfert de données FTP. Les ports pour ces canaux sont négociés au moyen de commandes PORT ou PASV. Les canaux sont alloués en réponse à un chargement de fichier, à un téléchargement de fichier ou à un événement de liste de répertoires
- Effectue le suivi de la séquence de commande-réponse FTP.
- Génère une trace d'audit.
  - L'enregistrement d'audit 303002 est généré pour chaque fichier récupéré ou chargé.
  - L'enregistrement d'audit 201005 est généré si la préparation du canal dynamique secondaire a échoué en raison d'un manque de mémoire.
- Traduit l'adresse IP intégrée.

Remarque Si vous désactivez l'inspection FTP, les utilisateurs sortants ne peuvent démarrer les connexions qu'en mode passif, et tous les FTP entrants sont désactivés.

FTP strict

Le protocole FTP strict augmente la sécurité des réseaux protégés en empêchant les navigateurs Web d'envoyer des commandes intégrées dans les demandes FTP. Pour activer un protocole FTP strict, cliquez sur le bouton **Configure** (Configurer) situé à côté de FTP dans Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service) > Edit Service Policy Rule (Modifier une règle de politique de service) > Rule Actions (Actions des règles) > Protocol Inspection (Inspection du protocole).

Lorsque vous utilisez un protocole FTP strict, vous pouvez éventuellement spécifier une liste des politiques d'inspection FTP pour préciser les commandes FTP qui ne sont pas autorisées à passer par l'ASA.

L'inspection FTP strict applique le comportement suivant :

- Une commande FTP doit être reconnue avant que l'ASA autorise une nouvelle commande.
- L'ASA abandonne les connexions qui envoient des commandes intégrées.
- Les commandes 227 et PORT sont vérifiées pour s'assurer qu'elles ne s'affichent pas dans une chaîne d'erreur.

Mise en garde L'utilisation de FTP strict peut entraîner des défaillances chez les clients FTP qui ne sont pas strictement conformes aux RFC FTP. En outre, vous devez vous assurer d'appliquer l'inspection à vos ports FTP uniquement (TCP/21 est le port FTP normal). Une inspection FTP stricte appliquée au trafic non FTP peut entraîner une perte de trafic inattendue, en particulier le trafic HTTP.

Grâce à une inspection FTP stricte, chaque commande et séquence de réponse FTP est suivie pour l'activité anormale suivante :

- Commande tronquée : le nombre de virgules dans la commande de réponse PORT et PASV est vérifié pour voir s'il est de cinq. S'il n'y a pas cinq, la commande PORT est considérée comme tronquée et la connexion TCP est fermée.
- Commande incorrecte : vérifie la commande FTP pour voir si elle se termine par <CR><LF> caractères, comme l'exige la RFC. Si ce n'est pas le cas, la connexion est fermée.
- Taille des commandes RETR et STOR : celles-ci sont vérifiées par rapport à une constante fixe. Si la taille est supérieure, un message d'erreur est enregistré et la connexion est fermée.
- Usurpation de commande : la commande PORT doit toujours être envoyée par le client. La connexion TCP est refusée si une commande PORT est envoyée à partir du serveur.
- Usurpation de réponse : la commande de réponse PASV (227) doit toujours être envoyée à partir du serveur. La connexion TCP est refusée si une commande de réponse PASV est envoyée par le client. Cela empêche le gouffre de sécurité lorsque l'utilisateur exécute « 227 xxxx a1, a2, a3, a4, p1, p2 ».
- Modification du flux TCP : l'ASA ferme la connexion s'il détecte une modification du flux TCP.
- Négociation de port non valide : la valeur de port dynamique négociée est vérifiée pour voir si elle est inférieure à 1024. Comme les numéros de port dans la plage de 1 à 1024 sont réservés aux connexions bien connues, si le port négocié se trouve dans cette plage, la connexion TCP est libérée.
- Filtrage de commande : le nombre de caractères présents après les numéros de port dans les commandes de réponse PORT et PASV est vérifié par recoupement avec une valeur constante de 8. S'il est supérieur à 8, la connexion TCP est fermée.
- L'ASA remplace la réponse du serveur FTP à la commande SYST par une série de X pour empêcher le serveur de révéler son type de système aux clients FTP. Pour remplacer ce comportement par défaut, utilisez la commande **no mask-syst-reply** dans la liste FTP.

Configurer une liste des politiques d'inspection FTP

Le filtrage des commandes FTP et les vérifications de sécurité sont fournis à l'aide de l'inspection FTP stricte pour améliorer la sécurité et le contrôle. La conformité au protocole comprend les vérifications de la longueur des paquets, les vérifications des délimiteurs et du format des paquets, les vérifications du terminateur de commande et la validation des commandes.

Le blocage de FTP en fonction des valeurs des utilisateurs est également pris en charge afin que les sites FTP puissent publier des fichiers à télécharger, tout en limitant l'accès à certains utilisateurs. Vous pouvez bloquer les connexions FTP en fonction du type de fichier, du nom du serveur et d'autres attributs. Des journaux de messages système sont générés si une connexion FTP est refusée après l'inspection.

Si vous souhaitez que l'inspection FTP permette aux serveurs FTP de révéler leur type de système aux clients FTP et limite les commandes FTP autorisées, créez et configurez une liste des politiques d'inspection FTP. Vous pouvez ensuite appliquer la liste lorsque vous activez l'inspection FTP.

Vous pouvez éventuellement créer une carte de trafic d'inspection FTP pour définir la carte de trafic pour l'inspection FTP. L'autre option consiste à définir les cartes de trafic directement dans la liste des politiques d'inspection FTP. La différence entre la création d'une carte de trafic et la définition de la correspondance de trafic directement dans la liste d'inspection est que vous pouvez créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafic. Bien que cette procédure explique les cartes

d'inspection, les critères de correspondance utilisés dans les cartes de trafics sont les mêmes que ceux expliqués à l'étape relative à l'onglet **Inspection**. Vous pouvez configurer les cartes de trafic FTP en sélectionnant **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Class Maps (Cartes de trafic)** > **FTP**, ou en les créant lors de la configuration de la liste d'inspection.

Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **FTP** .

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier le niveau de sécurité directement ou cliquer sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Niveau de sécurité** de la boîte de dialogue de la liste d'inspection FTP sélectionnez le niveau qui correspond le mieux à la configuration souhaitée. La valeur par défaut est High (Élevé).

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection FTP.

Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails) et poursuivez la procédure.

Astuces
Le bouton **File Type Filtering** (Filtrage de type de fichier) est un raccourci pour configurer l'inspection du média de fichier ou du type MIME, qui est expliquée plus loin dans cette procédure.

Étape 5 Cliquez sur l'onglet **Parameters** (Paramètres) et choisissez de masquer la bannière de message d'accueil du serveur ou de masquer la réponse à la commande SYST.

Le masquage de ces éléments empêche le client de découvrir des informations sur le serveur qui pourraient être utiles lors d'une attaque.

Étape 6 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

Vous pouvez définir les critères de correspondance du trafic en fonction des cartes de trafic DNS, en configurant les correspondances directement dans la liste d'inspection, ou les deux.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez **Single Match** (Correspondance unique) pour définir le critère directement, ou **Multiple Match** (Correspondance multiple), auquel cas vous sélectionnez la carte de trafic FTP qui définit les critères.

c) Si vous définissez le critère ici, choisissez le type de correspondance : **Match** (Correspondance) (le trafic doit correspondre au critère) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au critère). Par exemple, si No Match (Aucune correspondance) est sélectionné pour la chaîne « example.com », tout trafic contenant « example.com » est exclu de la carte de trafic. Configurez ensuite le critère comme suit :

- Nom du fichier : correspond au nom du fichier transféré par rapport à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- Type de fichier : correspond au type MIME ou de média du fichier transféré par rapport à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- Serveur : fait correspondre le nom du serveur FTP avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
- Utilisateur : fait correspondre le nom de l'utilisateur connecté à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- Commande de demande : commande FTP utilisée dans le paquet, toute combinaison des éléments suivants :
  - **APPE** : ajouter à un fichier.
  - **CDUP** : passe au répertoire parent du répertoire de travail actuel.
  - **DELE** : supprime un fichier sur le serveur.
  - **GET** : obtient un fichier du serveur.
  - **HELP** : fournit des renseignements d'aide.
  - **MKD** : crée un répertoire sur le serveur.
  - **PUT** : envoie un fichier au serveur.
  - **RMD** : supprime un répertoire sur le serveur.
  - **RNFR** : spécifie le nom de fichier « rename-from ».
  - **RNTO** : spécifie le nom de fichier « rename-to ».
  - **SITE** : utilisé pour spécifier une commande spécifique au serveur. Ceci est généralement utilisé pour l'administration à distance.
  - **STOU** : stocke un fichier en utilisant un nom de fichier unique.

d) Choisissez d'activer ou de désactiver la journalisation. L'action consiste toujours à réinitialiser la connexion, ce qui abandonne le paquet, ferme la connexion et envoie une réinitialisation TCP au serveur ou au client.
e) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 7 Cliquez sur **OK** dans la boîte de dialogue FTP Inspect Map (Liste d'inspection FTP).

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection FTP.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection HTTP

L'inspection HTTP n'est pas activée dans la politique d'inspection par défaut, vous devez donc l'activer si vous avez besoin de cette inspection. Cependant, la carte de trafic d'inspection par défaut comprend les ports HTTP par défaut, vous pouvez donc simplement modifier la politique d'inspection globale par défaut pour ajouter l'inspection HTTP. Vous pouvez également créer une nouvelle politique de service comme vous le souhaitez, par exemple, une politique spécifique à l'interface.

Les sections suivantes décrivent le moteur d'inspection HTTP.

Présentation de l'inspection HTTP

Utilisez le moteur d'inspection HTTP pour une protection contre les attaques spécifiques et d'autres menaces associées au trafic HTTP.

L'inspection des applications HTTP analyse les en-têtes et le corps HTTP et effectue diverses vérifications sur les données. Ces vérifications empêchent diverses constructions HTTP, types de contenu et protocoles de tunnellisation et de messagerie de traverser l'appareil de sécurité.

La fonctionnalité d'inspection HTTP améliorée, également connue sous le nom de pare-feu d'application et disponible lorsque vous configurez une liste des politiques d'inspection HTTP, peut aider à empêcher les attaquants d'utiliser les messages HTTP pour contourner la politique de sécurité du réseau.

L'inspection des applications HTTP peut bloquer les applications tunnellisées et les caractères non ASCII dans les demandes et réponses HTTP, ce qui empêche le contenu malveillant d'atteindre le serveur Web. La limitation de taille de divers éléments dans les en-têtes de demande et de réponse HTTP, le blocage d'URL et l'usurpation d'en-tête de serveur HTTP sont également pris en charge.

L'inspection HTTP améliorée vérifie les éléments suivants pour tous les messages HTTP :

- Conformité à la RFC 2616
- Utilisation uniquement des méthodes définies par la RFC.
- Conformité avec les critères supplémentaires.

Configurer une liste des politiques d'inspection HTTP

Pour préciser les actions lorsqu'un message enfreint un paramètre, créez une liste des politiques d'inspection HTTP. Vous pouvez ensuite appliquer la liste des politiques d'inspection lorsque vous activez l'inspection HTTP.

Vous pouvez éventuellement créer une carte de trafic d'inspection HTTP pour définir la classe de trafic pour l'inspection HTTP. L'autre option consiste à définir les classes de trafic directement dans la liste des politiques d'inspection HTTP. La différence entre la création d'une carte de trafic et la définition de la correspondance de trafic directement dans la liste d'inspection est que vous pouvez créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafics. Bien que cette procédure explique les cartes d'inspection, les critères de correspondance utilisés dans les cartes de trafics sont les mêmes que ceux expliqués à l'étape relative à l'onglet **Inspection**. Vous pouvez configurer les cartes de trafic HTTP en sélectionnant **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Class Maps (Cartes de trafic)** > **HTTP**, ou en les créant lors de la configuration de la liste d'inspection.

Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **HTTP**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier le niveau de sécurité directement ou cliquer sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Niveau de sécurité** de la boîte de dialogue de la liste d'inspection HTTP, sélectionnez le niveau qui correspond le mieux à la configuration souhaitée. Le niveau par défaut est Bas.

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection HTTP.

Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails) et poursuivez la procédure.

Astuces

Le bouton **URI Filtering** (Filtrage URI) est un raccourci pour configurer l'inspection Request URI (URI de demande), qui est expliquée plus loin dans cette procédure.

Étape 5 Cliquez sur l'onglet **Parameters** (Paramètres) et configurez les options souhaitées.

- **Body Match Maximum** (Nombre maximal de caractères pour la correspondance de corps) : nombre maximal de caractères dans le corps d'un message HTTP qui doivent être recherchés dans une correspondance de corps. La valeur par défaut est de 200 octets. Un grand nombre aura un impact considérable sur les performances.
- **Check for protocol violations** (Vérifier les violations de protocole) : indique s'il faut vérifier que les paquets sont conformes au protocole HTTP. En cas de non-conformité, vous pouvez abandonner la connexion, la réinitialiser ou la journaliser. Lors de l'abandon ou de la réinitialisation, vous pouvez également activer la journalisation.
- **Spoof server String (chaîne de serveur Spoof)** : remplace la valeur d'en-tête HTTP du serveur par la chaîne spécifiée, jusqu'à 82 caractères.

Étape 6 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

Vous pouvez définir les critères de correspondance du trafic en fonction des cartes de trafic HTTP, en configurant les correspondances directement dans la liste d'inspection, ou les deux.

a) Effectuez l'une des actions suivantes :
   - Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
   - Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez **Single Match** (Correspondance unique) pour définir le critère directement, ou **Multiple Match** (Correspondance multiple), auquel cas vous sélectionnez la carte de trafic HTTP qui définit les critères.

c) Si vous définissez le critère ici, choisissez le type de correspondance : **Match** (Correspondance) (le trafic doit correspondre au critère) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au critère). Par exemple, si No Match (Aucune correspondance) est sélectionné dans la chaîne « example.com », tout trafic contenant « example.com » est exclu de la carte de trafic. Configurez ensuite le critère comme suit :
   - Incompatibilité de type de contenu de la demande/de la réponse : correspond aux paquets dont le type de contenu dans la réponse ne correspond pas à l'un des types MIME dans le champ accept de la demande.
   - Arguments de la demande : faites correspondre les arguments de la demande à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
   - Longueur du corps de la demande : correspond aux paquets dont le corps de la demande est supérieur au nombre d'octets spécifié.
   - Corps de la demande : faites correspondre le corps de la demande avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
   - Nombre de champs d'en-tête de demande : correspond aux paquets dont le nombre de champs d'en-tête dans la demande est supérieur au nombre spécifié. Vous pouvez faire correspondre le type d'en-tête de champ à une expression régulière ou à un type prédéfini. Les types prédéfinis sont les suivants : accept, accept-charset, accept-encoding, accept-language, allow, authorization, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5,

content-range, content-type, cookie, date, expect, expires, from, host, if-match, if-modified-since, if-none-match, if-range, if-unmodified-since, last-modified, max-forwards, pragma, proxy-authorization, range, referer, te, trailer, transfer-encoding, upgrade, user-agent, via, warning.

- Longueur du champ d'en-tête de la demande : correspond aux paquets dont la longueur du champ d'en-tête dans la demande est supérieure aux octets spécifiés. Vous pouvez faire correspondre le type d'en-tête de champ à une expression régulière ou à un type prédéfini. Les types prédéfinis sont répertoriés ci-dessus pour le nombre de champs d'en-tête de demande.
- Champ d'en-tête de demande : faites correspondre le contenu du champ d'en-tête sélectionné dans la demande avec l'expression régulière ou la liste d'expressions régulières sélectionnée. Vous pouvez spécifier un type d'en-tête prédéfini ou utiliser une expression régulière pour sélectionner les en-têtes.
- Nombre d'en-têtes de demande : correspond aux paquets dont le nombre d'en-têtes dans la demande est supérieur au nombre spécifié.
- Longueur de l'en-tête de la demande : correspond aux paquets dont la longueur de l'en-tête dans la demande est supérieure aux octets spécifiés.
- Request Header Non-ASCII : correspond aux paquets dont l'en-tête de la demande contient des caractères non ASCII.
- Méthode de demande : correspond aux paquets dans lesquels la méthode de demande correspond au type prédéfini ou à l'expression régulière ou à la liste d'expressions régulières sélectionnée. Les types prédéfinis sont les suivants : bcopy, bdelete, bmove, bpropfind, bproppatch, connect, copy, delete, edit, get, getattribute, getattributenames, getproperties, head, index, lock, mkcol, mkdir, move, notify, options, poll, post, propfind, proppatch, put, revadd, revlabel, revlog, revnum, save, search, setattribute, startrev, stoprev, subscribe, trace, unedit, unlock, unsubscribe.
- Longueur de l'URI de la demande : correspond aux paquets dans lesquels la longueur de l'URI de la demande est supérieure aux octets spécifiés.
- URI de la demande : faites correspondre le contenu de l'URI de la demande à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- Corps de la demande : faites correspondre le corps de la demande à l'expression régulière ou à la liste d'expressions régulières sélectionnée, ou au contenu d'ActiveX ou de Java Applet.
- Longueur du corps de la réponse : correspond aux paquets dans lesquels la longueur du corps de la réponse est supérieure aux octets spécifiés.
- Nombre de champs d'en-tête de réponse : correspond aux paquets dont le nombre de champs d'en-tête dans la réponse est supérieur au nombre spécifié. Vous pouvez faire correspondre le type d'en-tête de champ à une expression régulière ou à un type prédéfini. Les types prédéfinis sont les suivants : accept-ranges, age, allow, cache-control, connection, content-encoding, content-language, content-length, content-location, content-md5, content-range, content-type, date, etag, expires, last-modified, location, pragma, proxy-authenticate, retry-after, server, set-cookie, trailer, transfer-encoding, upgrade, vary, via, warning, www-authenticate.
- Longueur du champ d'en-tête de la réponse : correspond aux paquets dont la longueur du champ d'en-tête dans la réponse est supérieure aux octets spécifiés. Vous pouvez faire correspondre le type d'en-tête de champ à une expression régulière ou à un type prédéfini. Les types prédéfinis sont répertoriés ci-dessus pour le nombre de champs d'en-tête de réponse.

- Champ d'en-tête de réponse : fait correspondre le contenu du champ d'en-tête sélectionné dans la réponse à l'expression régulière ou à la liste d'expressions régulières sélectionnée. Vous pouvez spécifier un type d'en-tête prédéfini ou utiliser une expression régulière pour sélectionner les en-têtes.
- Nombre d'en-têtes de réponse : correspond aux paquets dont le nombre d'en-têtes dans la réponse est supérieur au nombre spécifié.
- Longueur de l'en-tête de la réponse : correspond aux paquets dont la longueur de l'en-tête dans la réponse est supérieure aux octets spécifiés.
- En-tête de réponse non-ASCII : correspond aux paquets dont l'en-tête de la réponse contient des caractères non ASCII.
- Ligne d'état de la réponse : faites correspondre le contenu de la ligne d'état de la réponse à l'expression régulière ou à la liste d'expressions régulières sélectionnée.

d) Choisissez d'abandonner la connexion, de la réinitialiser ou de la journaliser. Pour abandonner la connexion et la réinitialisation, vous pouvez activer ou désactiver la journalisation.
e) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 7 Cliquez sur **OK** dans la boîte de dialogue de la liste d'inspection HTTP.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection HTTP.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection ICMP

Le moteur d'inspection ICMP permet au trafic ICMP d'avoir une « session » afin qu'il puisse être inspecté comme le trafic TCP et UDP. Sans le moteur d'inspection ICMP, nous vous recommandons de ne pas autoriser ICMP par l'intermédiaire de l'ASA dans une liste de contrôle d'accès. Sans inspection dynamique, ICMP peut être utilisé pour attaquer votre réseau. Le moteur d'inspection ICMP garantit qu'il n'y a qu'une seule réponse à chaque demande et que le numéro de séquence est correct.

Cependant, le trafic ICMP dirigé vers une interface ASA n'est jamais inspecté, même si vous activez l'inspection ICMP. Ainsi, un ping (requête d'écho) à une interface peut échouer dans des circonstances spécifiques, comme lorsque la demande d'écho provient d'une source que l'ASA peut atteindre par une route de sauvegarde par défaut.



Remarque La NAT utilise l'inspection ICMP lors de la traduction des paquets, même si vous désactivez l'inspection ICMP.

Pour en savoir plus sur l'activation de l'inspection ICMP, consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection des erreurs ICMP

Lorsque l'inspection des erreurs ICMP est activée, l'ASA crée des sessions de traduction pour les sauts intermédiaires qui envoient des messages d'erreur ICMP, en fonction de la configuration NAT. L'ASA remplace les adresses IP du paquet par les adresses IP traduites.

Lorsque cette option est désactivée, l'ASA ne crée pas de sessions de traduction pour les nœuds intermédiaires qui génèrent des messages d'erreur ICMP. Les messages d'erreur ICMP générés par les nœuds intermédiaires entre l'hôte interne et l'ASA atteignent l'hôte externe sans utiliser de ressource NAT supplémentaire. Cela n'est pas souhaité lorsqu'un hôte externe utilise la commande traceroute pour retracer les sauts jusqu'à la destination à l'intérieur de l'ASA. Lorsque l'ASA ne traduit pas les sauts intermédiaires, tous les sauts intermédiaires s'affichent avec l'adresse IP de destination mappée.



Remarque Vous devez toujours activer l'inspection d'erreur ICMP s'il est possible que la NAT soit utilisée sur les paquets ICMP. Comme la NAT utilise automatiquement l'inspection ICMP pour les paquets ICMP, même si l'inspection ICMP est désactivée, l'utilisation de l'adresse de destination mappée comme adresse source peut donner l'impression qu'un analyseur examine votre réseau. Par exemple, sans inspection d'erreur ICMP également activée, si le paquet de demande ECHO a sa destination traduite, lorsqu'il est intégré dans une réponse de délai ICMP dépassé, l'en-tête externe de la demande de délai dépassé utilise la destination traduite comme adresse source. Si vous activez l'inspection d'erreur ICMP, l'adresse source de dépassement sera définie à la valeur correcte.

Pour en savoir plus sur l'activation de l'inspection des erreurs ICMP, consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection ILS

Le moteur d'inspection Internet Locator Service (ILS) prend en charge la NAT pour les produits Microsoft NetMeeting, SiteServer et Active Directory qui utilisent LDAP pour échanger des informations de répertoire avec un serveur ILS. Vous ne pouvez pas utiliser la PAT avec l'inspection ILS, car seules les adresses IP sont stockées par une base de données LDAP.

Pour les réponses de recherche, lorsque le serveur LDAP est situé à l'extérieur, considérez l'utilisation de la NAT pour permettre aux homologues internes de communiquer localement lorsqu'ils sont enregistrés sur des serveurs LDAP externes. Si vous n'avez pas besoin d'utiliser la NAT, nous vous recommandons de désactiver le moteur d'inspection pour obtenir de meilleures performances.

Une configuration supplémentaire peut être nécessaire lorsque le serveur ILS est situé à l'intérieur de la frontière ASA. Cela nécessiterait une ouverture pour que les clients externes accèdent au serveur LDAP sur le port spécifié, généralement TCP 389.



Remarque Comme le trafic ILS (signalisation d'appel H225) ne se produit que sur le canal UDP secondaire, la connexion TCP est déconnectée après l'intervalle d'inactivité TCP. Par défaut, cet intervalle est de 60 minutes et peut être ajusté à l'aide de la commande TCP **timeout**. Dans ASDM, cela se trouve dans le volet **Configuration > Firewall (Pare-feu) > Advanced (Avancé) > Global Timeouts (Délais d'expiration globaux)**.

L'inspection ILS a les limites suivantes :

- Les demandes de parrainage et les réponses ne sont pas prises en charge.
- Les utilisateurs de plusieurs répertoires ne sont pas unifiés.
- Les utilisateurs uniques ayant plusieurs identités dans plusieurs répertoires ne peuvent pas être reconnus par la NAT.

Pour en savoir plus sur l'activation de l'inspection ILS, consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection de la messagerie instantanée

Le moteur d'inspection de messagerie instantanée (IM) vous permet de contrôler l'utilisation du réseau d'IM et d'arrêter la fuite de données confidentielles, la propagation des vers et d'autres menaces pour le réseau d'entreprise.

L'inspection IM n'est pas activée dans la politique d'inspection par défaut, vous devez donc l'activer si vous avez besoin de cette inspection. Cependant, la carte de trafic d'inspection par défaut comprend les ports IM par défaut, vous pouvez donc simplement modifier la politique d'inspection globale par défaut pour ajouter l'inspection IM. Vous pouvez également créer une nouvelle politique de service comme vous le souhaitez, par exemple, une politique spécifique à l'interface.

Si vous décidez de mettre en œuvre l'inspection IM, vous pouvez également configurer une liste des politiques d'inspection IM pour préciser les actions lorsqu'un message enfreint un paramètre. La procédure suivante explique les mappages de politiques d'inspection d'IM.

Vous pouvez également créer une carte de trafic d'inspection IM pour définir la carte de classes de trafic utilisée pour l'inspection IM. L'autre option consiste à définir les cartes de classes de trafic directement dans la liste des politiques d'inspection d'IM. La différence entre la création d'une carte de trafic et la définition de la correspondance du trafic directement dans la liste d'inspection est que vous pouvez créer des critères de correspondance plus complexes et réutiliser les cartes de trafic. Cette procédure explique les cartes d'inspection, mais les cartes de trafic sont essentiellement les mêmes, sauf que vous ne spécifiez pas les actions appliquées au trafic correspondant. Vous pouvez configurer les cartes de trafic IM en sélectionnant **Configuration > Firewall (Pare-feu) > Objects (Objets) > Class Maps (Cartes de trafic) > Instant Messaging (IM) [Messagerie instantanée]**.



Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **Instant Messaging (IM)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste et cliquez sur **Edit** (Modifier).

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

Vous pouvez définir les critères de correspondance du trafic en fonction des cartes de trafic IM, en configurant les correspondances directement dans la liste d'inspection, ou les deux.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez **Single Match** (Correspondance unique) pour définir directement le critère, ou **Multiple Match** (Correspondance multiple), puis sélectionnez la carte de trafic IM qui définit les critères. Cliquez sur **Manage** (Gérer) pour créer de nouvelles cartes de trafic.

c) Si vous définissez le critère ici, choisissez le type de correspondance pour les critères : **correspondance** (le trafic doit correspondre au critère) ou **aucune correspondance** (le trafic ne doit pas correspondre au critère). Par exemple, si Aucune correspondance est sélectionné dans la chaîne « example.com », tout trafic contenant « example.com » est exclu de la carte de trafic. Configurez ensuite le critère.

- Protocole : correspond au trafic d'un protocole IM spécifique, tel que Yahoo Messenger ou MSN Messenger.
- Service : correspond à un service de messagerie instantanée spécifique, tel que la conversation, le transfert de fichiers, la caméra Web, la conversation vocale, la conférence ou les jeux.
- Version : faites correspondre la version du message IM à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- Nom de connexion du client : faites correspondre le nom de connexion du client source du message IM avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
- Nom de connexion de l'homologue du client : faites correspondre le nom de connexion de l'homologue de destination du message IM avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
- Adresse IP source : faites correspondre l'adresse IP source et le masque.
- Adresse IP de destination : faites correspondre l'adresse IP de destination et le masque.
- Nom de fichier : faites correspondre le nom de fichier du message IM avec l'expression régulière ou la liste d'expressions régulières sélectionnée.

d) Choisissez d'abandonner la connexion, de la réinitialiser ou de la journaliser. Pour abandonner la connexion et la réinitialisation, vous pouvez activer ou désactiver la journalisation.
e) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 5 Cliquez sur **OK** dans la boîte de dialogue de la liste d'inspection IM.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection IM.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection des options IP

Vous pouvez configurer l'inspection des options IP pour contrôler les paquets IP qui sont autorisés en fonction du contenu du champ Options IP dans l'en-tête du paquet. Vous pouvez abandonner les paquets qui ont des options indésirables, effacer les options (et autoriser le paquet) ou autoriser le paquet sans modification.

Les options IP fournissent des fonctions de contrôle nécessaires dans certaines situations, mais inutiles pour la plupart des communications courantes. En particulier, les options IP comprennent des dispositions pour les horodatages, la sécurité et le routage spécial. L'utilisation des options IP est facultative, et le champ peut contenir zéro, une ou plusieurs options.

Pour obtenir la liste des options IP, avec des références aux RFC pertinents, consultez la page IANA, http://www.iana.org/assignments/ip-paramètres/ip-paramètres.xhtml.

L'inspection des options IP est activée par défaut, mais pour le trafic RSVP uniquement. Vous ne devez le configurer que si vous souhaitez autoriser des options supplémentaires que la liste par défaut, ou si vous souhaitez l'appliquer à d'autres types de trafic à l'aide d'une carte de classe de trafic d'inspection autre que celle par défaut.

Remarque L'inspection des options IP ne fonctionne pas sur les paquets fragmentés. Par exemple, les options ne sont pas effacées des fragments.

Les sections suivantes décrivent l'inspection des options IP.

Valeurs par défaut pour l'inspection des options IP

L'inspection des options IP est activée par défaut pour le trafic RSVP uniquement, à l'aide de la liste des politiques d'inspection _default_ip_options_map.

- L'option Router Alert est autorisée.

  Cette option informe les routeurs de transit d'inspecter le contenu du paquet même lorsque le paquet n'est pas destiné à ce routeur. Cette inspection est utile lors de la mise en œuvre de RSVP et de protocoles similaires qui nécessitent un traitement plutôt complexe de la part des routeurs le long du chemin de livraison du paquet. L'abandon de paquets RSVP contenant l'option Router Alert peut entraîner des problèmes dans les implémentations VoIP.

- Les paquets qui contiennent d'autres options sont abandonnés.

  Chaque fois qu'un paquet est abandonné en raison d'une inspection, le journal système 106012 est émis. Le message indique quelle option a causé l'abandon. Utilisez la commande **show service-policy inspect ip-options** pour afficher les statistiques de chaque option.

Configurer une liste des politiques d'inspection des options IP

Si vous souhaitez effectuer une inspection d'options IP autres que celles par défaut, créez une liste des politiques d'inspection d'options IP pour préciser comment vous souhaitez gérer chaque type d'option.



Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **IP Options (Options IP)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste, puis cliquez sur **Edit** (Modifier).

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Choisissez les options que vous souhaitez autoriser en les déplaçant de la liste d'abandon vers la liste d'autorisation.

Tenez compte des conseils suivants :

- L'option « default » (défaut) définit le comportement par défaut pour les options non incluses dans la liste. Si vous le déplacez vers la liste Autorisé, même les options affichées dans la liste Abandon seront autorisées.
- Pour toute option que vous autorisez, vous pouvez cocher la case Clear (Effacer) pour supprimer l'option de l'en-tête du paquet avant de transmettre le paquet.
- Certaines options sont répertoriées par numéro de type d'option. Le nombre est l'octet complet du type d'option (copie, carte et numéro d'option), et pas seulement la partie numéro d'option de l'octet. Ces types d'options peuvent ne pas représenter des options réelles. Les options non standard doivent être au format type-longueur attendu défini dans le protocole Internet RFC 791, http://tools.ietf.org/html/rfc791.
- Si un paquet comprend plus d'un type d'option, il est abandonné tant que l'action pour l'un de ces types est d'abandonner le paquet.

Pour obtenir la liste des options IP, avec des références aux RFC pertinents, consultez la page IANA, http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml.

Étape 5 Cliquez sur **OK**.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection d'options IP.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection IPsec Pass Through

L'inspection IPsec Pass Through n'est pas activée dans la politique d'inspection par défaut. Vous devez donc l'activer si vous avez besoin de cette inspection. Cependant, la carte de trafic d'inspection par défaut comprend les ports IPsec par défaut, vous pouvez donc simplement modifier la politique d'inspection globale par défaut pour ajouter l'inspection IPsec. Vous pouvez également créer une nouvelle politique de service comme vous le souhaitez, par exemple, une politique spécifique à l'interface.

Les sections suivantes décrivent le moteur d'inspection IPsec Pass Through.

Aperçu de l'inspection de transmission directe IPsec

Internet Protocol Security (IPsec) est une suite de protocoles permettant de sécuriser les communications IP en authentifiant et en chiffrant chaque paquet IP d'un flux de données. IPsec comprend également des protocoles pour établir une authentification mutuelle entre les agents au début de la session et la négociation des clés cryptographiques à utiliser pendant la session. IPsec peut être utilisé pour protéger les flux de données entre une paire d'hôtes (par exemple, utilisateurs d'ordinateurs ou serveurs), entre une paire de passerelles de sécurité (comme les routeurs ou les pare-feu) ou entre une passerelle de sécurité et un hôte.

L'inspection applicative d'IPsec Pass Through (transmission directe IPsec) permet la traversée transparente du trafic ESP (protocole IP 50) et AH (protocole IP 51) associé à une connexion IKE sur le port UDP 500. Il évite une longue configuration d'ACL pour autoriser le trafic ESP et AH et offre également une sécurité à l'aide du délai d'expiration et du nombre maximal de connexions.

Configurez une liste des politiques pour la transmission directe IPsec afin de préciser les restrictions relatives au trafic ESP ou AH. Vous pouvez définir le nombre maximal de connexions par client et le délai d'inactivité.

Le trafic NAT et non NAT est autorisé. Cependant, la PAT n'est pas prise en charge.

Configurer une liste des politiques d'inspection de transmission directe IPsec

Une liste IPsec Passthrough vous permet de modifier les valeurs de configuration par défaut utilisées pour l'inspection de l'application IPsec Pass Through. Vous pouvez utiliser une liste IPsec Passthrough pour autoriser certains flux sans utiliser d'ACL.

La configuration comprend une liste par défaut, _default_ipsec_passthru_map, qui n'établit aucune limite maximale aux connexions ESP par client, et définit le délai d'inactivité ESP à 10 minutes. Vous ne devez configurer une liste des politiques d'inspection que si vous souhaitez des valeurs différentes ou si vous souhaitez définir des valeurs AH.

Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Listes d'inspection)** > **IPsec Pass Through (IPsec Pass Through)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier le niveau de sécurité directement ou cliquer sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Security Level** (Niveau de sécurité) de la boîte de dialogue IPsec Pass Through Inspect Map (Liste d'inspection IPsec Pass Through), sélectionnez le niveau qui correspond le mieux à la configuration souhaitée.

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection IPsec Pass Through.

Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails) et poursuivez la procédure.

Étape 5 Choisissez d'autoriser les tunnels ESP et HA.

Pour chaque protocole, vous pouvez également définir le nombre maximal de connexions autorisées par client et le délai d'inactivité.

Étape 6 Cliquez sur **OK**.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection IPsec Pass Through.

Inspection IPv6

L'inspection IPv6 vous permet de consigner ou d'abandonner sélectivement le trafic IPv6 en fonction de l'en-tête d'extension. En outre, l'inspection IPv6 peut vérifier la conformité à la RFC 2460 pour le type et l'ordre des en-têtes d'extension dans les paquets IPv6.

L'inspection IPv6 n'est pas activée dans la politique d'inspection par défaut, vous devez donc l'activer si vous avez besoin de cette inspection. Vous pouvez simplement modifier la politique d'inspection globale par défaut

pour ajouter l'inspection IPv6. Vous pouvez également créer une nouvelle politique de service comme vous le souhaitez, par exemple, une politique spécifique à l'interface.

Valeurs par défaut pour l'inspection IPv6

Si vous activez l'inspection IPv6 et que vous ne spécifiez pas de liste des politiques d'inspection, la liste des politiques d'inspection IPv6 par défaut est utilisée, et les actions suivantes sont effectuées :

- Autorise uniquement les en-têtes d'extension IPv6 connus. Les paquets non conformes sont abandonnés et journalisés.
- Applique l'ordre des en-têtes d'extension IPv6 tel que défini dans la spécification RFC 2460. Les paquets non conformes sont abandonnés et journalisés.
- Abandonne tout paquet avec un en-tête de type routage.

Configurer une liste des politiques d'inspection IPv6

Pour identifier les en-têtes d'extension à abandonner ou à journaliser, ou pour désactiver la vérification des paquets, créez une liste des politiques d'inspection IPv6 à utiliser par la politique de service.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Listes d'inspection)** > **IPv6**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste, puis cliquez sur **Edit** (Modifier).

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Cliquez sur l'onglet **Enforcement** (Application) et choisissez d'autoriser uniquement les en-têtes d'extension IPv6 connus ou d'appliquer l'ordre des en-têtes d'extension IPv6 comme défini dans la RFC 2460. Les paquets non conformes sont abandonnés et journalisés.

Étape 5 (Facultatif) Cliquez sur l'onglet **Header Matches** (Correspondances d'en-têtes) pour identifier le trafic à abandonner ou à journaliser en fonction des en-têtes des messages IPv6.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez l'en-tête d'extension IPv6 correspondant :

- En-tête d'authentification (HA).
- En-tête des options de destination.
- En-tête Encapsulating Security Payload (ESP).

- En-tête de fragment.
- En-tête Hop-by-hop Options.
- En-tête de routage : spécifiez un numéro de type d'en-tête unique ou une plage de numéros.
- Nombre d'en-têtes : spécifiez le nombre maximal d'en-têtes d'extension que vous autoriserez sans supprimer ni journaliser le paquet.
- Nombre d'adresses d'en-tête de routage : spécifiez le nombre maximal d'adresses dans l'en-tête de routage de type 0 que vous autoriserez sans supprimer ni journaliser le paquet.

c) Choisissez d'abandonner ou de consigner le paquet. Si vous abandonnez le paquet, vous pouvez également activer la journalisation.
d) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 6 Cliquez sur **OK** dans la boîte de dialogue IPv6 Inspect Map (Liste d'inspection IPv6).

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection IPv6.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection NetBIOS

L'inspection d'application NetBIOS effectue une NAT pour l'adresse IP intégrée dans les paquets du service de nom NetBIOS (NBNS) et les paquets des services de datagramme NetBIOS. Il applique également la conformité du protocole en vérifiant la cohérence des champs de nombre et de longueur.

L'inspection NetBIOS est activée par défaut. Vous pouvez éventuellement créer une liste des politique abandonner ou journaliser les violations du protocole NetBIOS. La procédure suivante explique comment configurer une liste des politiques d'inspection NetBIOS.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **NetBIOS**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste, puis cliquez sur **Edit** (Modifier).

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Sélectionnez **Check for Protocol Violations** (Vérifier les violations de protocole). Il n'y a aucune raison de créer une liste si vous ne sélectionnez pas cette option.

Étape 5 Sélectionnez l'action à effectuer, soit abandonner le paquet, soit le consigner. Si vous abandonnez le paquet, vous pouvez également activer la journalisation.

Étape 6 Cliquez sur **OK**.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection NetBIOS.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection PPTP

PPTP est un protocole de tunnellisation du trafic PPP. Une session PPTP est composée d'un canal TCP et généralement de deux tunnels GRE PPTP. Le canal TCP est le canal de contrôle utilisé pour négocier et gérer les tunnels PPTP GRE. Les tunnels GRE acheminent les sessions PPP entre les deux hôtes.

Lorsque cette option est activée, le moteur d'inspection PPTP inspecte les paquets du protocole PPTP et crée dynamiquement les connexions GRE et les xlates nécessaires pour autoriser le trafic PPTP.

Plus précisément, l'ASA inspecte les annonces de version PPTP et la séquence de demande/réponse d'appel sortant. Seul PPTP version 1, tel que défini dans la RFC 2637, est inspecté. L'inspection plus approfondie sur le canal de contrôle TCP est désactivée si la version annoncée par l'un ou l'autre des côtés n'est pas la version 1. En outre, la demande d'appel sortant et la séquence de réponse sont suivies. Les connexions et les xlates sont allouées dynamiquement selon les besoins pour permettre le trafic de données GRE secondaire subséquent.

Le moteur d'inspection PPTP doit être activé pour que le trafic PPTP soit traduit par PAT. En outre, la PAT n'est effectuée que pour une version modifiée de GRE (RFC2637) et uniquement si elle est négociée sur le canal de contrôle TCP PPTP. La PAT n'est pas effectuée pour la version non modifiée de GRE (RFC 1701 et RFC 1702).

Pour en savoir plus sur l'activation de l'inspection PPTP, consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection RSH

L'inspection RSH est activée par défaut. Le protocole RSH utilise une connexion TCP du client RSH au serveur RSH sur le port TCP 514. Le client et le serveur négocient le numéro de port TCP où le client est à l'écoute du flux de sortie STDERR. L'inspection RSH prend en charge la NAT du numéro de port négocié, si nécessaire.

Pour en savoir plus sur l'activation de l'inspection RSH, consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection SMTP et SMTP étendue

L'inspection ESMTP détecte les attaques, y compris les attaques de pourriels, d'hameçonnage, de messages malformés et les attaques de débordement ou d'insuffisance de la mémoire tampon. Elle prend également en charge la sécurité des applications et la conformité des protocoles, qui imposent la validité des messages ESMTP, bloquent les expéditeurs/récepteurs et bloquent le relais de messagerie.

L'inspection ESMTP est activée par défaut. Vous ne devez le configurer que si vous souhaitez un traitement différent de celui fourni par la liste d'inspection par défaut.

Les sections suivantes décrivent le moteur d'inspection ESMTP.

Aperçu de l'inspection SMTP et ESMTP

L'inspection des applications SMTP étendue (ESMTP) offre une protection améliorée contre les attaques basées sur SMTP en limitant les types de commandes SMTP qui peuvent passer par l'ASA et en ajoutant des fonctionnalités de surveillance. ESMTP est une amélioration du protocole SMTP et est similaire à SMTP à bien des égards.

L'inspection d'application ESMTP contrôle et réduit les commandes que l'utilisateur peut utiliser ainsi que les messages que le serveur renvoie. L'inspection ESMTP effectue trois tâches principales :

- Restreint les requêtes SMTP à sept commandes SMTP de base et à huit commandes étendues. Les commandes prises en charge sont les suivantes :
  - SMTP étendu : AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML, STARTTLS et VRFY.
  - SMTP (RFC 821) : DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET.
- Surveille la séquence de commande-réponse SMTP.
- Génère une trace d'audit : l'enregistrement d'audit 108002 est généré lorsqu'un caractère non valide intégré dans l'adresse courriel est remplacé. Pour en savoir plus, consultez la RFC 821.

L'inspection ESMTP surveille la séquence de commande et de réponse pour les signatures anormales suivantes :

- Commandes tronquées.
- Fin de commande incorrecte (absence de terminaison par <CR> <LF>).
- Les commandes MAIL et RCPT précisent qui sont l'expéditeur et le destinataire du courriel. Les adresses de messagerie sont analysées pour détecter les caractères inconnus. Le caractère de routage (|) est supprimé (changé en espace vide) et « < » □« > » ne sont autorisés que s'ils sont utilisés pour définir une adresse de courriel (« > » doit être précédé de « < »).
- Transition inattendue du serveur SMTP. 3379
- Pour les commandes inconnues ou non prises en charge, le moteur d'inspection modifie tous les caractères du paquet en X, qui sont rejetés par le serveur interne. Il en résulte un message tel que « 500 Command unknown: « XXX » (Commande inconnue : « XXX »). Les commandes incomplètes sont rejetées

  Les commandes ESMTP non prises en charge sont ATRN, ONEX, VERB, CHUNKING et les extensions privées.
- Modification du flux TCP.

- Pipelining de commandes.

Remarque Lorsque l'inspection ESMTP est activée, une session Telnet utilisée pour le protocole SMTP interactif peut se bloquer si les règles suivantes ne sont pas respectées : les commandes SMTP doivent comporter au moins quatre caractères ; elles doivent se terminer par un retour chariot et un saut de ligne; et vous devez attendre une réponse avant d'envoyer la commande suivante.

Valeurs par défaut pour l'inspection ESMTP

L'inspection ESMTP est activée par défaut, à l'aide de la liste des politiques d'inspection _default_esmtp_map.

- La bannière du serveur est masquée. Le moteur d'inspection ESMTP remplace les caractères de la bannière SMTP du serveur par des astérisques, à l'exception des caractères « 2 », « 0 », « 0 ». Les caractères de retour chariot (CR) et de retour de ligne (LF) sont ignorés.
- Les connexions chiffrées sont autorisées, mais pas inspectées.
- Les caractères spéciaux dans les adresses de l'expéditeur et du destinataire ne sont pas détectés et aucune action n'est entreprise.
- Les connexions dont la longueur de ligne de commande est supérieure à 512 sont abandonnées et journalisées.
- Les connexions de plus de 100 destinataires sont abandonnées et journalisées.
- Les messages dont la longueur du corps est supérieure à 998 octets sont journalisés.
- Les connexions dont la longueur de ligne d'en-tête est supérieure à 998 sont abandonnées et journalisées.
- Les messages avec des noms de fichier MIME supérieurs à 255 caractères sont abandonnés et journalisés.
- Les paramètres de réponse EHLO correspondant à « autres » sont masqués.

Configurer une liste des politiques d'inspection ESMTP

Pour préciser les actions lorsqu'un message enfreint un paramètre, créez une liste des politiques d'inspection ESMTP. Vous pouvez ensuite appliquer la liste des politiques d'inspection lorsque vous activez l'inspection ESMTP.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **ESMTP**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier le niveau de sécurité directement ou cliquer sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Security Level** (Niveau de sécurité) de la boîte de dialogue ESMTP Inspect Map (Liste d'inspection ESMTP), sélectionnez le niveau qui correspond le mieux à la configuration souhaitée.

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection ESMTP.

Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails) et poursuivez la procédure.

Astuces

Le bouton **MIME File Type Filtering** (Filtrage de type de fichier MIME) est un raccourci pour configurer l'inspection du type de fichier, qui est expliquée ultérieurement dans cette procédure.

Étape 5 Cliquez sur l'onglet **Parameters** (Paramètres) et configurez les options souhaitées.

- **Mask Server Banner** (Masquer la bannière du serveur) : indique s'il faut masquer la bannière du serveur ESMTP.
- **Encrypted Packet Inspection** (Inspection des paquets chiffrés) : indique s'il faut autoriser ESMTP sur TLS (connexions chiffrées) sans inspection. Vous pouvez éventuellement journaliser les connexions chiffrées. La valeur par défaut est d'autoriser les sessions TLS sans inspection. Si vous désélectionnez l'option, le système supprime l'indication STARTTLS de toute tentative de connexion de session chiffrée et force une connexion en texte brut.

Étape 6 Cliquez sur l'onglet **Filtering** (Filtrage) et configurez les options souhaitées.

- **Configure mail relay** (Configurer le relais de messagerie) : identifie un nom de domaine pour le relais de messagerie. Vous pouvez soit abandonner la connexion et éventuellement la journaliser, soit la journaliser.
- **Check for special characters** (Vérifier les caractères spéciaux) : identifie l'action à prendre pour les messages qui incluent les caractères spéciaux pipe (|), guillemet arrière et NUL dans les adresses courriel de l'expéditeur ou du destinataire. Vous pouvez soit abandonner la connexion et éventuellement la journaliser, soit la journaliser.

Étape 7 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez le type de correspondance pour les critères : **Match** (le trafic doit correspondre au critère) ou **No Match** (le trafic ne doit pas correspondre au critère). Par exemple, si No Match est sélectionné sur la chaîne « example.com », tout trafic contenant « example.com » est exclu de la carte de trafic. Configurez ensuite le critère :

- **Body Length** (Longueur du corps) : correspond aux messages où la longueur d'un message de corps ESMTP est supérieure au nombre d'octets spécifié.
- **Body Line Length** (Longueur de ligne du corps) : correspond aux messages où la longueur d'une ligne dans un message de corps ESMTP est supérieure au nombre d'octets spécifié.
- **Commands** (Commandes) : correspond au verbe de commande dans le message. Vous pouvez spécifier une ou plusieurs des commandes suivantes : auth, data, ehlo, etrn, helo, help, mail, noop, quit, rcpt, rset, saml, soml, vrfy.
- **Command Recipient Count** (Nombre de destinataires de commande) : correspond aux messages où le nombre de destinataires est supérieur au nombre spécifié.
- **Command Line Length** (Longueur de ligne de commande) : correspond aux messages où la longueur d'une ligne dans le verbe de commande est supérieure au nombre d'octets spécifié.
- **EHLO Reply Parameters** (Paramètres de réponse EHLO) : correspond aux paramètres de réponse EHLO ESMTP. Vous pouvez spécifier un ou plusieurs des paramètres suivants : 8bitmime, auth, binaryname, checkpoint, dsn, etrn, others, pipelining, size, vrfy.
- **Header Length** (Longueur de l'en-tête) : correspond aux messages où la longueur d'un en-tête ESMTP est supérieure au nombre d'octets spécifié.
- **Header Line Length** (Longueur de ligne de l'en-tête) : correspond aux messages où la longueur d'une ligne dans un en-tête ESMTP est supérieure au nombre d'octets spécifié.
- **Header To: Fields Count** (Nombre de champs To dans l'en-tête) : correspond aux messages où le nombre de champs To dans l'en-tête est supérieur au nombre spécifié.
- **Invalid Recipients Count** (Nombre de destinataires non valides) : correspond aux messages où le nombre de destinataires non valides est supérieur au nombre spécifié.
- **MIME File Type** (Type de fichier MIME) : correspond au type de fichier MIME ou média avec l'expression régulière ou la liste d'expressions régulières spécifiée.
- **MIME Filename Length** (Longueur du nom de fichier MIME) : correspond aux messages dans lesquels le nom de fichier est plus long que le nombre d'octets spécifié.
- **MIME Encoding** (Encodage MIME) : correspond au type d'encodage MIME. Vous pouvez spécifier un ou plusieurs des types suivants : 7bit, 8bit, base64, binary, others, quoted-printable.
- **Sender Address** (Adresse de l'expéditeur) : correspond à l'adresse courriel de l'expéditeur avec l'expression régulière ou la liste d'expressions régulières spécifiée.
- **Sender Address Length** (Longueur de l'adresse de l'expéditeur) : correspond aux messages dont l'adresse de l'expéditeur est supérieure au nombre d'octets spécifié.

c) Choisissez d'abandonner la connexion, de la réinitialiser ou de la journaliser. Pour abandonner la connexion et la réinitialisation, vous pouvez activer ou désactiver la journalisation. Pour la mise en correspondance de la commande et du paramètre de réponse EHLO, vous pouvez également masquer la commande. Pour la correspondance de commande, vous pouvez également appliquer une limite de débit en paquets par seconde.

d) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 8 Cliquez sur **OK** dans la boîte de dialogue de la liste d'inspection ESMTP.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection ESMTP.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection SNMP

L'inspection des applications SNMP est appliquée à la fois au trafic vers le périphérique et au trafic traversant le périphérique. Cette inspection est nécessaire si vous configurez SNMP v3 où les utilisateurs sont limités à des hôtes SNMP spécifiques. Sans inspection, un utilisateur v3 défini peut interroger le périphérique à partir de n'importe quel hôte autorisé. L'inspection SNMP est activée par défaut pour les ports par défaut. Vous ne devez donc la configurer que si vous utilisez des ports autres que les ports par défaut. Les ports par défaut sont UDP/161, 162 (pour tous les types de périphériques) et UDP/4161 pour les périphériques qui exécutent également FXOS, car FXOS écoute sur UDP/161.

Par défaut, l'inspection SNMP limite l'interrogation à la version configurée.

Remarque Si vous configurez SNMP sur un périphérique qui exécute également FXOS, l'inspection SNMP est obligatoire et est réactivée si vous la désactivez. L'inspection SNMP est activée sur une classe de trafic qui comprend le port UDP/4161.

Vous pouvez également restreindre le trafic SNMP à une version particulière de SNMP. Les versions antérieures de SNMP sont moins sécurisées; par conséquent, le refus de certaines versions SNMP peut être requis par votre politique de sécurité. Le système peut refuser les versions SNMP 1, 2, 2c ou 3. Vous contrôlez les versions autorisées en créant une liste SNMP, comme expliqué ci-dessous. Si vous n'avez pas besoin de contrôler les versions, activez simplement l'inspection SNMP sans liste.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **SNMP**.

Étape 2 Cliquez sur **Add** (Ajouter), ou sélectionnez une liste et cliquez sur **Edit** (Modifier). Lors de l'ajout d'une liste, saisissez un nom de liste.

Étape 3 Sélectionnez les versions SNMP à refuser.

Étape 4 Cliquez sur **OK**.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection SQL*Net

L'inspection SQL*Net est activée par défaut. Le moteur d'inspection prend en charge les versions 1 et 2 de SQL*Net, mais uniquement le format Transparent Network Substrate (TNS). L'inspection ne prend pas en charge le format Tabular Data Stream (TDS). Les messages SQL*Net sont analysés pour rechercher les adresses et les ports intégrés, et la réécriture NAT est appliquée au besoin.

L'affectation de port par défaut pour SQL*Net est 1521. Il s'agit de la valeur utilisée par Oracle pour SQL*Net, mais cette valeur n'est pas conforme aux affectations de port IANA pour Structured Query Language (SQL). Si votre application utilise un port différent, appliquez l'inspection SQL*Net à une carte de trafic qui comprend ce port.

Désactiver l'inspection SQL*Net dans les cas suivants :

- Le transfert de données SQL se produit sur le même port que le port TCP de contrôle SQL 1521. Le périphérique de sécurité agit comme un serveur proxy lorsque l'inspection SQL*Net est activée et réduit la taille de la fenêtre client de 65 000 à environ 16 000, ce qui entraîne des problèmes de transfert de données.
- L'inspection de débits élevés de trafic SQL entraîne des pointes inacceptables dans l'utilisation du processeur.

Après avoir désactivé l'inspection SQL*Net, utilisez la commande **clear conn port 1521** pour que les connexions puissent être recréées sans inspection.

Pour en savoir plus sur l'activation de l'inspection SQL*Net, consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection Sun RPC

Cette section décrit l'inspection des applications Sun RPC.

Aperçu de l'inspection Sun RPC

L'inspection du protocole Sun RPC est activée par défaut. Vous devez simplement gérer la table du serveur Sun RPC pour identifier les services autorisés à traverser le pare-feu. Cependant, l'ouverture dynamique de ports pour NFS est effectuée pour n'importe quel serveur, même sans configuration de la table du serveur.

Sun RPC est utilisé par NFS et NIS. Les services Sun RPC peuvent s'exécuter sur n'importe quel port. Lorsqu'un client tente d'accéder à un service Sun RPC sur un serveur, il doit connaître le port sur lequel le service est exécuté. Il le fait en interrogeant le processus de mappage de port, généralement rpcbind, sur le port bien connu de 111.

Le client envoie le numéro de programme Sun RPC du service et le processus de mappage de port répond en indiquant le numéro de port du service. Le client envoie ses requêtes Sun RPC au serveur, en précisant le port identifié par le processus de mappage de port. Lorsque le serveur répond, l'ASA intercepte ce paquet et ouvre les connexions TCP et UDP embryonnaires sur ce port.

La NAT ou la PAT des informations de charge utile Sun RPC n'est pas prise en charge.

Gérer les services Sun RPC

Utilisez la table des services Sun RPC pour contrôler le trafic de RPC en fonction des sessions de RPC établies.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **SUNRPC Server (Serveur SUNRPC)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau serveur.
- Sélectionnez un serveur, puis cliquez sur **Edit** (Modifier).

Étape 3 Configurez les propriétés du service :

- **Interface Name** (Nom de l'interface) : interface par laquelle le trafic vers le serveur transite.
- **IP Address/Mask** (Adresse IP/Masque) : adresse du serveur Sun RPC.
- **Service ID (ID** de service) : type de service sur le serveur. Pour déterminer le type de service (par exemple, 100003), utilisez la commande **sunrpcinfo** dans la ligne de commande UNIX ou Linux sur la machine du serveur Sun RPC.
- **Protocol** (Protocole) : indique si le service utilise TCP ou UDP
- **Port/Port Range** (Port/Plage de ports) : port ou plage de ports utilisés par le service.
- **Timeout** (Délai d'expiration) : délai d'inactivité du passage ouvert pour la connexion par l'inspection Sun RPC.

Étape 4 Cliquez sur **OK**.

Étape 5 (Facultatif) Surveillez les passages créés pour ces services.

Pour afficher les passages ouverts pour les services Sun RPC, saisissez la commande **show sunrpc-server active**. Sélectionnez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)** pour saisir la commande. Par exemple :

```
hostname# show sunrpc-server active
LOCAL FOREIGN SERVICE TIMEOUT
-----------------------------------------------
1 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
2 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
3 209.165.200.5/0 192.168.100.2/647 100005 0:30:00
4 209.165.200.5/0 192.168.100.2/650 100005 0:30:00
```

L'entrée dans la colonne LOCAL affiche l'adresse IP du client ou du serveur sur l'interface interne, tandis que la valeur dans la colonne FOREIGN affiche l'adresse IP du client ou du serveur sur l'interface externe.

Au besoin, vous pouvez effacer ces services à l'aide de **clear sunrpc-server active**

Inspection TFTP

L'inspection TFTP est activée par défaut.

TFTP, décrit dans la RFC 1350, est un protocole simple pour lire et écrire des fichiers entre un serveur TFTP et un client.

Le moteur d'inspection inspecte la demande de lecture (RRQ), la demande d'écriture (WRQ) et la notification d'erreur (ERROR) et crée dynamiquement des connexions et des traductions, au besoin, pour permettre le transfert de fichiers entre un client et un serveur TFTP.

Un canal secondaire dynamique et une traduction de PAT, le cas échéant, sont alloués lors de la réception d'une demande valide de lecture (RRQ) ou d'écriture (WRQ). Ce canal secondaire est ensuite utilisé par TFTP pour le transfert de fichiers ou la notification d'erreurs.

Seul le serveur TFTP peut initier le trafic sur le canal secondaire, et au plus un canal secondaire incomplet peut exister entre le client et le serveur TFTP. Une notification d'erreur du serveur ferme le canal secondaire.

L'inspection TFTP doit être activée si la PAT statique est utilisée pour rediriger le trafic TFTP.

Pour en savoir plus sur l'activation de l'inspection TFTP, consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection XDMCP

XDMCP est un protocole qui utilise le port UDP 177 pour négocier les sessions X, qui utilisent TCP lorsqu'elles sont établies.

Pour une négociation réussie et le démarrage d'une session XWindows, l'ASA doit autoriser la connexion TCP de retour à partir de l'ordinateur hébergeant X. Pour autoriser la connexion de retour, vous pouvez utiliser des règles d'accès pour autoriser les ports TCP. Sinon, vous pouvez exécuter la commande **established** sur l'ASA. Une fois que XDMCP a négocié le port pour envoyer l'affichage, la commande **established** est consultée pour vérifier si cette connexion arrière doit être autorisée.

Pendant la session XWindows, le gestionnaire communique avec le serveur X d'affichage sur le port bien connu 6000 | n. Chaque affichage a une connexion distincte au serveur X, en raison du paramètre de terminal suivant.

```
setenv DISPLAY Xserver:n
```

où *n* est le numéro d'affichage.

Lorsque XDMCP est utilisé, l'affichage est négocié à l'aide d'adresses IP, sur lesquelles l'ASA peut appliquer la NAT si nécessaire. L'inspection XDMCP ne prend pas en charge la PAT.

Pour en savoir plus sur l'activation de l'inspection XDMCP, consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection VXLAN

L'inspection du réseau local virtuel extensible (VXLAN) fonctionne sur le trafic encapsulé VXLAN qui passe par l'ASA. Il garantit que le format d'en-tête VXLAN est conforme aux normes, en abandonnant les paquets malformés. L'inspection VXLAN n'est pas effectuée sur le trafic pour lequel l'ASA agit comme point d'extrémité de tunnel VXLAN (VTEP) ou passerelle VXLAN, car ces vérifications sont effectuées dans le cadre normal de la désencapsulation des paquets VXLAN.

Les paquets VXLAN sont UDP, normalement sur le port 4789. Ce port fait partie de la classe par défaut-inspection-trafic, vous pouvez donc simplement ajouter l'inspection VXLAN à la règle de politique de service inspection_default. Vous pouvez également créer une carte de trafic pour celui-ci en utilisant la mise en correspondance de port ou d'ACL.

Historique de l'inspection du protocole Internet de base

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de l'inspection DCERPC pour le message UUID ISystemMapper, RemoteGetClassObject opnum3.	9.4(1)	L'ASA a commencé à prendre en charge les messages DCERPC non EPM dans la version 8.3, en prenant en charge le message UUID ISystemMapper, RemoteCreateInstance opnum4. Cette modification étend la prise en charge au message RemoteGetClassObject opnum3. Nous n'avons pas modifié d'écrans ASDM.
Inspection des paquets VXLAN	9.4(1)	L'ASA peut inspecter l'en-tête VXLAN pour faire respecter le format standard. Nous avons modifié l'écran suivant : **Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service) > Add Service Policy Rule (Ajouter une règle de politique de service) > Rule Actions (Actions découlant d'une règle) > Protocol Inspection (Inspection de protocole)**
L'inspection ESMTP change de comportement par défaut pour les sessions TLS.	9.4(1)	La valeur par défaut pour l'inspection ESMTP a été modifiée pour autoriser les sessions TLS, qui ne sont pas inspectées. Cependant, cette valeur par défaut s'applique aux systèmes nouveaux ou recréés. Si vous mettez à niveau un système qui inclut **no allow-tls**, la commande n'est pas modifiée. Le changement de comportement par défaut a également été apporté dans ces anciennes versions : 8.4(7.25), 8.5(1.23), 8.6(1.16), 8.7(1.15), 9.0(4.28), 9.1(6.1), 9.2(3.2) 9.3(1.2), 9.3(2.2).

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Améliorations de l'inspection des options d'IP	9.5(1)	L'inspection des options IP prend désormais en charge toutes les options IP possibles. Vous pouvez régler l'inspection pour autoriser, effacer ou abandonner toutes les options standard ou expérimentales, y compris celles non encore définies. Vous pouvez également définir un comportement par défaut pour les options non définies explicitement dans une carte d'inspection des options IP. Nous avons modifié la boîte de dialogue IP Options Inspect Map (Liste d'inspection des options IP) afin d'inclure des options supplémentaires. Vous sélectionnez maintenant les options à autoriser et éventuellement à effacer.
Améliorations de l'inspection DCERPC et du filtrage des UUID	9.5(2)	L'inspection DCERPC prend désormais en charge la NAT pour les messages opnum5 d'OxidResolver ServerAlive2. Vous pouvez également filtrer les identifiants universels (UUID) des messages DCERPC pour réinitialiser ou enregistrer des types de messages particuliers. Il existe une nouvelle carte des classes d'inspection DCERPC pour le filtrage des UUID. Nous avons ajouté l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Class Maps (Cartes de trafic)** > **DCERPC**. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **DCERPC**.
Inspection DNS sur TCP	9.6(2)	Vous pouvez désormais inspecter le trafic DNS sur TCP (TCP/53). Nous avons modifié la page suivante : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspection Maps (Cartes d'inspection)** > **DNS** Add/Edit dialog box (Boîte de dialogue Ajouter/modifier)
Prise en charge de Cisco Umbrella	9.10(1)	Vous pouvez configurer le périphérique pour rediriger les requêtes DNS vers Cisco Umbrella, afin que votre politique de sécurité d'entreprise définie dans Cisco Umbrella puisse être appliquée aux connexions des utilisateurs. Vous pouvez autoriser ou bloquer les connexions en fonction du FQDN ou, pour les FQDN suspects, vous pouvez rediriger l'utilisateur vers le mandataire intelligent Cisco Umbrella, qui peut effectuer le filtrage d'URL. La configuration de Cisco Umbrella fait partie de la politique d'inspection DNS. Écrans nouveaux ou modifiés : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Cisco Umbrella**, **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **DNS**.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Améliorations de Cisco Umbrella.	9.12(1)	Vous pouvez maintenant identifier les noms de domaine locaux qui doivent contourner Cisco Umbrella. Les demandes DNS pour ces domaines sont directement transmises aux serveurs DNS sans passer par Cisco Umbrella. Vous pouvez également identifier les serveurs Cisco Umbrella à utiliser pour la résolution des demandes DNS. Enfin, vous pouvez définir la politique d'inspection de Cisco Umbrella pour qu'elle s'ouvre même en cas de non-conformité, afin que les demandes DNS ne soient pas bloquées si le serveur Cisco Umbrella n'est pas disponible. Nous avons modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Cisco Umbrella**, **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **DNS**.
Inspection XDMCP désactivée par défaut dans les nouvelles installations.	9.15(1)	Auparavant, l'inspection XDMCP était activée par défaut pour tout le trafic. Désormais, sur les nouvelles installations, qui comprennent les nouveaux systèmes et les systèmes recréés, XDMCP est désactivé par défaut. Si vous avez besoin de cette inspection, veuillez l'activer. Notez que lors des mises à niveau, vos paramètres actuels pour l'inspection XDMCP sont conservés, même si vous les aviez simplement activés via les paramètres d'inspection par défaut.



CHAPITRE 14

Inspection des protocoles vocaux et vidéo

Les rubriques suivantes expliquent l'inspection des applications pour les protocoles vocaux et vidéo. Pour obtenir des renseignements de base sur la raison pour laquelle vous devez utiliser l'inspection pour certains protocoles et les méthodes globales d'application de l'inspection, consultez Premiers pas avec l'inspection du protocole de la couche application, à la page 285.

- Inspection CTIQBE, à la page 343
- Inspection H.323, à la page 344
- Inspection MGCP, à la page 349
- Inspection RTSP, à la page 352
- Inspection SIP, à la page 355
- Inspection Skinny (SCCP), à la page 360
- Inspection STUN, à la page 363
- Historique de l'inspection des protocoles vocaux et vidéo, à la page 364

Inspection CTIQBE

L'inspection de protocole CTIQBE prend en charge la NAT, la PAT et la NAT bidirectionnelle. Cela permet à Cisco IP SoftPhone et à d'autres applications de Cisco TAPI/JTAPI de fonctionner avec succès avec Cisco CallManager pour la configuration des appels dans l'ensemble de l'ASA.

TAPI et JTAPI sont utilisés par de nombreuses applications VoIP de Cisco. CTIQBE est utilisé par Cisco TSP pour communiquer avec Cisco CallManager.

Pour en savoir plus sur l'activation de l'inspection CTIQBE, consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Limites de l'inspection CTQBE

Le basculement dynamique des appels CTQBE n'est pas pris en charge.

La section suivante résume les considérations spéciales lors de l'utilisation de l'inspection d'application CTQBE dans des scénarios précis :

- Si deux téléphones IP de Cisco sont enregistrés sur des centres d'appel Cisco différents, qui sont connectés à différentes interfaces de l'appareil de sécurité adaptable Cisco, les appels entre ces deux téléphones échouent.

- Lorsque Cisco CallManager se trouve sur l'interface de sécurité plus élevée que les téléphones IP de Cisco, si une NAT ou une NAT externe est requise pour l'adresse IP de Cisco CallManager, le mappage doit être statique, car Cisco IP SoftPhone nécessite que l'adresse IP de Cisco CallManager soit spécifiée explicitement dans sa configuration Cisco TSP sur le PC.
- Lors de l'utilisation de la PAT ou de la PAT externe, si l'adresse IP de Cisco CallManager doit être traduite, son port TCP 2748 doit être mappé de manière statique au même port de l'adresse PAT (interface) pour que les enregistrements de Cisco IP SoftPhone réussissent. Le port d'écoute CTIQBE (TCP 2748) est fixe et ne peut pas être configuré par l'utilisateur sur Cisco CallManager, Cisco IP SoftPhone ou Cisco TSP.

Inspection H.323

L'inspection H.323 prend en charge les protocoles RAS, H.225 et H.245, et sa fonctionnalité traduit toutes les adresses IP et tous les ports intégrés. Elle effectue le suivi et le filtrage de l'état et peut effectuer une série d'activations de la fonction d'inspection. L'inspection H.323 prend en charge le filtrage des numéros de téléphone, le contrôle dynamique T.120, le contrôle de tunnellisation H.245, les groupes HSI, le suivi de l'état des protocoles, l'application de la durée des appels H.323, le télécopie T.38 et le contrôle audio/vidéo.

L'inspection H.323 est activée par défaut. Vous ne devez le configurer que si vous souhaitez un traitement autre que celui par défaut.

Les sections suivantes décrivent l'inspection des applications H.323.

Survol de l'inspection H.323

L'inspection H.323 prend en charge les applications conformes à la norme H.323, telles que Cisco CallManager. H.323 est un ensemble de protocoles définis par l'Union internationale des télécommunications pour les conférences multimédias sur les réseaux locaux. L'ASA prend en charge H.323 jusqu'à la version 6, y compris la fonctionnalité H.323 v3 Multiple Calls on One Call Signaling Channel.

Lorsque l'inspection H.323 est activée, l'ASA prend en charge plusieurs appels sur le même canal de signalisation d'appel, une fonctionnalité introduite avec la version 3 du protocole H.323. Cette fonctionnalité réduit le temps de configuration des appels et réduit l'utilisation des ports sur l'ASA.

Les deux fonctions principales de l'inspection H.323 sont les suivantes :

- Effectuez la NAT pour les adresses IPv4 intégrées nécessaires dans les messages H.225 et H.245. Comme les messages H.323 sont codés au format de codage PER, l'ASA utilise un décodeur ASN.1 pour décoder les messages H.323.
- Attribuez dynamiquement les connexions H.245 et RTP/RTCP négociées. La connexion H.225 peut également être attribuée dynamiquement lors de l'utilisation de RAS.

Fonctionnement de H.323

L'ensemble de protocoles H.323 peut utiliser jusqu'à deux connexions TCP et de quatre à huit connexions UDP. FastConnect utilise une seule connexion TCP et RAS utilise une seule connexion UDP pour l'enregistrement, les autorisations et l'état.

Un client H.323 peut initialement établir une connexion TCP avec un serveur H.323 en utilisant le port TCP 1720 pour demander la configuration de l'appel Q.931. Dans le cadre du processus de configuration de l'appel, le terminal H.323 fournit un numéro de port au client à utiliser pour une connexion TCP H.245. Dans les environnements où le portier H.323 est utilisé, le paquet initial est transmis à l'aide d'UDP.

L'inspection H.323 surveille la connexion TCP Q.931 pour déterminer le numéro de port H.245. Si les terminaux H.323 n'utilisent pas FastConnect, l'ASA alloue dynamiquement la connexion H.245 en fonction de l'inspection des messages H.225. La connexion H.225 peut également être attribuée dynamiquement lors de l'utilisation de RAS.

Dans chaque message H.245, les terminaux H.323 échangent des numéros de port qui sont utilisés pour les flux de données UDP suivants. L'inspection H.323 inspecte les messages H.245 pour identifier ces ports et crée dynamiquement les connexions nécessaires à l'échange des médias. RTP utilise le numéro de port négocié, tandis que RTCP utilise le numéro de port suivant.

Le canal de contrôle H.323 gère les protocoles H.225, H.245 et H.323 RAS. L'inspection H.323 utilise les ports suivants :

- 1718 : port UDP de découverte du Gatekeeper
- 1719 : port UDP RAS
- 1720 : port de contrôle TCP

Vous devez autoriser le trafic pour le port H.323 1719 pour la signalisation RAS. En outre, vous devez autoriser le trafic pour le port H.323 bien connu 1720 pour la signalisation d'appel H.225; cependant, les ports de signalisation H.245 sont négociés entre les terminaux dans la signalisation H.225. Lorsqu'un portier H.323 est utilisé, l'ASA ouvre une connexion H.225 en fonction de l'inspection des messages d'ACF et de RCF.

Après avoir inspecté les messages H.225, l'ASA ouvre le canal H.245, puis inspecte le trafic envoyé sur le canal H.245. Tous les messages H.245 passant par l'ASA sont soumis à l'inspection d'application H.245, qui traduit les adresses IP intégrées et ouvre les canaux de support négociés dans les messages H.245.

Chaque connexion UDP dont un paquet est soumis à l'inspection H.323 est marquée comme une connexion H.323 et expire selon le délai H.323 configuré dans Configuration > Firewall (Pare-feu) > Advanced (Avancé) > Global Timeouts (Délais d'expiration globaux).



Remarque Vous pouvez activer la configuration d'appel entre les terminaux H.323 lorsque le portier se trouve dans le réseau. L'ASA comprend des options pour ouvrir des passages pour les appels en fonction des messages RegistrationRequest/RegistrationConfirm (RRQ/RCF). Comme ces messages RRQ/RCF sont échangés avec le Gatekeeper, l'adresse IP du point terminal appelant est inconnue et l'ASA ouvre un passage avec l'adresse IP source et le port 0/0. Par défaut, cette option est activée.

Prise en charge H.239 dans les messages H.245

L'ASA se trouve entre deux points terminaux H.323. Lorsque les deux terminaux H.323 configurent une session de téléprésentation afin que les terminaux puissent envoyer et recevoir une présentation de données, telles que des données de feuille de calcul, l'ASA garantit la négociation réussie du protocole H.239 entre les terminaux.

La norme H.239 est une norme qui permet aux terminaux de la série H.300 d'ouvrir un canal vidéo supplémentaire en un seul appel. Dans un appel, un terminal (comme un téléphone vidéo) envoie un canal pour la vidéo et un canal pour la présentation des données. La négociation H.239 a lieu sur le canal H.245.

L'ASA ouvre des passages pour le canal de support supplémentaire et le canal de contrôle de support. Les terminaux utilisent le message de canal logique ouvert (OLC) pour signaler la création d'un nouveau canal. L'extension de message fait partie de la version 13 du protocole H.245.

Le décodage et l'encodage de la session de téléprésentation sont activés par défaut. L'encodage et le décodage H.239 sont effectués par le codeur ASN.1.

Limites de l'inspection H.323

L'inspection H.323 est testée et prise en charge pour Cisco Unified Communications Manager (CUCM) 7.0. Il n'est pas pris en charge pour CUCM 8.0 et les versions ultérieures. L'inspection H.323 peut fonctionner avec d'autres versions et produits.

Voici quelques-uns des problèmes et des limites connus lors de l'utilisation de l'inspection d'application H.323 :

- La PAT est prise en charge, à l'exception de la PAT étendue ou de la PAT par session.
- La PAT statique peut ne pas traduire correctement les adresses IP intégrées dans les champs facultatifs des messages H.323. Si vous rencontrez ce type de problème, n'utilisez pas la PAT statique avec H.323.
- Non pris en charge avec la NAT entre les interfaces de même niveau de sécurité.
- Non pris en charge avec NAT64.
- La NAT avec inspection H.323 n'est pas compatible avec la NAT lorsqu'elle est effectuée directement sur les terminaux. Si vous effectuez une NAT sur les terminaux, désactivez l'inspection H.323.

Configurer la liste des politiques d'inspection H.323

Vous pouvez créer une liste des politiques d'inspection H.323 pour personnaliser les actions d'inspection H.323 si le comportement d'inspection par défaut n'est pas suffisant pour votre réseau.

Vous pouvez éventuellement créer une carte de trafic d'inspection H.323 pour définir la classe de trafic pour l'inspection H.323. L'autre option consiste à définir les classes de trafic directement dans la liste des politiques d'inspection H.323. La différence entre la création d'une carte de trafic et la définition de la correspondance de trafic directement dans la liste d'inspection est que vous pouvez créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafic. Bien que cette procédure explique les cartes d'inspection, les critères de correspondance utilisés dans les cartes de trafics sont les mêmes que ceux expliqués à l'étape relative à l'onglet **Inspection**. Vous pouvez configurer les cartes de trafic H.323 en sélectionnant **Configuration** > **Firewall** > **Objects** > **Class Maps (Cartes de trafic)** > **H.323**, ou en les créant lors de la configuration de la liste d'inspection.

Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **H.323**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier le niveau de sécurité directement ou cliquer sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Security Level** (Niveau de sécurité) de la boîte de dialogue H.323 Inspect Map (Liste d'inspection H.323), sélectionnez le niveau qui correspond le mieux à la configuration souhaitée. Le niveau par défaut est Bas.

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection H.323.

Astuces

Le bouton **Phone Number Filtering** (Filtrage de numéro de téléphone) est un raccourci pour configurer l'inspection de l'appelé ou de l'appelant, qui est expliquée ultérieurement dans cette procédure.

Étape 5 Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails), puis procédez comme suit :

a) Cliquez sur l'onglet **State Checking** (Vérification de l'état) et choisissez d'activer la vérification de la transition d'état des messages RAS et H.225.

Vous pouvez également vérifier les messages RCF et ouvrir des passages pour les adresses de signal d'appel présentes dans les messages RRQ, ce qui permet la configuration d'appel entre les terminaux H.323 lorsque le portier se trouve dans le réseau. Utilisez cette option pour ouvrir des passages pour les appels en fonction des messages RegistrationRequest/RegistrationConfirm (RRQ/RCF). Comme ces messages RRQ/RCF sont envoyés à et par le portier, l'adresse IP du terminal appelant est inconnue et l'ASA ouvre un passage par l'adresse IP source/le port 0/0. Par défaut, cette option est activée.

b) Cliquez sur l'onglet **Call Attributes** (Attributs d'appel) et choisissez d'appliquer une limite de durée d'appel (maximum 1 193 heures) ou d'appliquer la présence de numéros d'appelant et d'appelé lors de l'établissement de l'appel.

Vous pouvez également autoriser les messages H.225 FACILITY à arriver avant les messages H.225 SETUP conformément à la norme H.460.18. Si vous rencontrez des problèmes de configuration d'appels, où les connexions sont fermées avant d'être terminées lors de l'utilisation de H.323/H.225, sélectionnez

cette option pour autoriser les messages précoces. Assurez-vous également d'activer l'inspection pour les services RAS H.323 et H.225 (ils sont tous deux activés par défaut).

c) Cliquez sur l'onglet **Tunneling and Protocol Conformance** (Conformité du protocole et tunnellisation) et choisissez de vérifier la tunnellisation H.245 ; vous pouvez soit abandonner la connexion, soit la journaliser.

Vous pouvez également choisir de vérifier la conformité du protocole des paquets RTP qui passent par les passages. Si vous vérifiez la conformité, vous pouvez également choisir de limiter la charge utile à l'audio ou à la vidéo, en fonction de l'échange de signalisation.

Étape 6 Si nécessaire, cliquez sur l'onglet **HSI Group Parameters** (Paramètres de groupe HSI) et définissez les groupes HSI.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau groupe.
- Sélectionnez un groupe existant et cliquez sur **Edit** (Modifier).

b) Précisez l'ID de groupe (de 0 à 2 147 483 647) et l'adresse IP du HSI.

c) Pour ajouter un terminal au groupe HSI, saisissez l'adresse IP, sélectionnez l'interface par laquelle le terminal est connecté à l'ASA, puis cliquez sur **Add>>** (Ajouter). Supprimez les terminaux qui ne sont plus nécessaires. Vous pouvez avoir jusqu'à 10 terminaux par groupe.

d) Cliquez sur **OK** pour ajouter le groupe. Répétez le processus au besoin.

Étape 7 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

Vous pouvez définir les critères de correspondance du trafic en fonction des cartes de trafic HTTP, en configurant les correspondances directement dans la liste d'inspection, ou les deux.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez **Single Match** (Correspondance unique) pour définir directement le critère, ou **Multiple Match** (Correspondance multiple), auquel cas vous sélectionnez la carte de trafic H.323 qui définit les critères.

c) Si vous définissez le critère ici, choisissez le type de correspondance : **Match** (Correspondance) (le trafic doit correspondre au critère) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au critère). Configurez ensuite le critère comme suit :

- **Called Party** (Partie appelée) : fait correspondre la partie appelée H.323 à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- **Calling Party** (Partie appelante) : fait correspondre la partie appelante H.323 à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- **Media Type** (Type de support) : correspond au type de support : audio, vidéo ou données.

d) Choisissez l'action à entreprendre pour le trafic correspondant. Pour la correspondance de la partie appelante ou appelée, vous pouvez abandonner le paquet, abandonner la connexion ou réinitialiser la connexion. Pour la correspondance du type de support, l'action est toujours d'abandonner le paquet; vous pouvez activer la journalisation pour cette action.

e) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 8 Cliquez sur **OK** dans la boîte de dialogue H.323 Inspect Map (Liste d'inspection H.323).

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection H.323.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection MGCP

L'inspection MGCP n'est pas activée dans la politique d'inspection par défaut, vous devez donc l'activer si vous avez besoin de cette inspection. Cependant, la carte de trafic d'inspection par défaut comprend les ports MGCP par défaut, de sorte que vous pouvez simplement modifier la politique d'inspection globale par défaut pour ajouter l'inspection MGCP. Vous pouvez également créer une nouvelle politique de service comme vous le souhaitez, par exemple, une politique spécifique à l'interface.

Les sections suivantes décrivent l'inspection des applications MGCP.

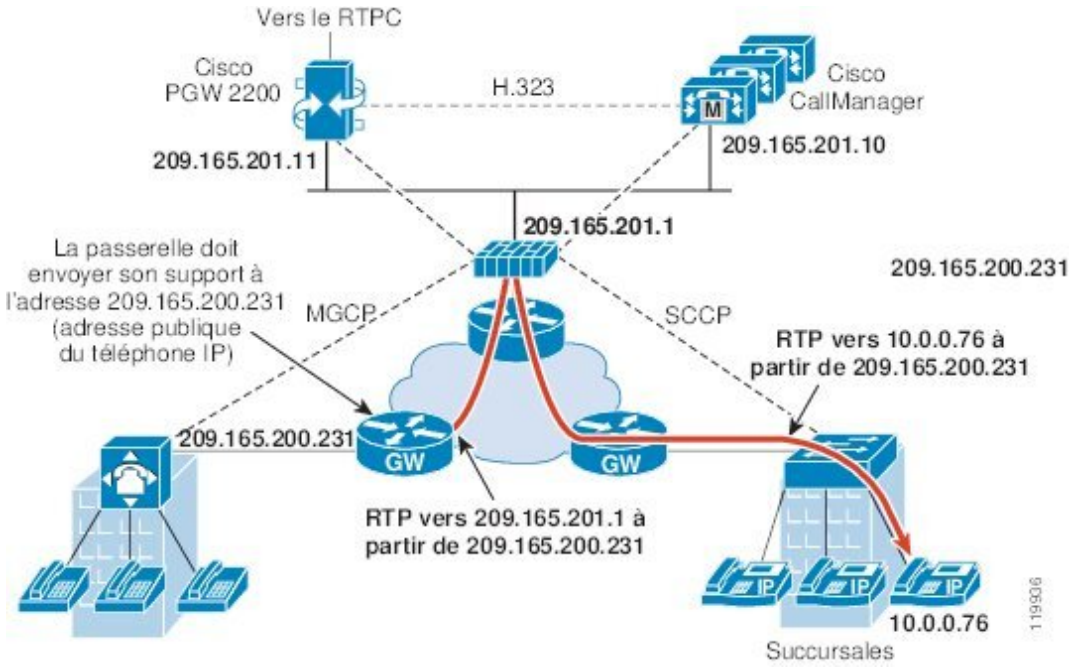
Aperçu de l'inspection MGCP

MGCP est utilisé pour contrôler les passerelles multimédias à partir d'éléments de contrôle d'appel externes appelés contrôleurs de passerelle multimédia ou agents d'appel. Une passerelle multimédia est généralement un élément de réseau qui assure la conversion entre les signaux audio acheminés sur les circuits téléphoniques et les paquets de données acheminés sur Internet ou d'autres réseaux de paquets. L'utilisation de la NAT et de la PAT avec MGCP vous permet de prendre en charge un grand nombre de périphériques sur un réseau interne avec un ensemble limité d'adresses externes (globales). Des exemples de passerelles multimédias sont les suivants :

- Passerelles de liaison, qui assurent l'interface entre le réseau téléphonique et un réseau de voix sur IP. Ces passerelles gèrent généralement un grand nombre de circuits numériques.
- Passerelles résidentielles, qui fournissent une interface analogique traditionnelle (RJ11) à un réseau de voix sur IP. Les exemples de passerelles résidentielles comprennent les modems câble ou les décodeurs câble, les périphériques xDSL et les périphériques sans fil à large bande.
- Passerelles d'entreprise, qui fournissent une interface PBX numérique traditionnelle ou une interface PBX logicielle intégrée à un réseau de voix sur IP.

Les messages MGCP sont transmis sur UDP. Une réponse est renvoyée à l'adresse source (adresse IP et numéro de port UDP) de la commande, mais la réponse peut ne pas provenir de la même adresse que celle à laquelle la commande a été envoyée. Cela peut se produire lorsque plusieurs agents d'appel sont utilisés dans une configuration de basculement et que l'agent d'appel qui a reçu la commande a transmis le contrôle à un agent d'appel de secours, qui envoie ensuite la réponse. La figure suivante illustre comment vous pouvez utiliser la NAT avec MGCP.

Illustration 37 : Utilisation de la NAT avec MGCP



Les terminaux MGCP sont des sources et des destinations physiques ou virtuelles de données. Les passerelles multimédias contiennent des points d'extrémité sur lesquels l'agent d'appel peut créer, modifier et supprimer des connexions pour établir et contrôler les sessions multimédias avec d'autres points d'extrémité multimédias. En outre, l'agent d'appel peut demander aux terminaux de détecter certains événements et de générer des signaux. Les terminaux communiquent automatiquement les modifications de l'état de service à l'agent appelant.

- Les passerelles sont généralement à l'écoute du port UDP 2427 pour recevoir des commandes de l'agent appelant.
- Le port sur lequel l'agent d'appel reçoit les commandes de la passerelle. Les agents d'appel écoutent généralement le port UDP 2727 pour recevoir des commandes de la passerelle.

Remarque L'inspection MGCP ne prend pas en charge l'utilisation d'adresses IP différentes pour la signalisation MGCP et les données RTP. Une pratique courante et recommandée consiste à envoyer les données RTP à partir d'une adresse IP résiliente, telle qu'une adresse de bouclage ou une adresse IP virtuelle; cependant, l'ASA exige que les données RTP proviennent de la même adresse que la signalisation MGCP.

Configurer une liste des politiques d'inspection MGCP

Si le réseau comporte plusieurs agents d'appel et passerelles pour lesquels l'ASA doit ouvrir des passages, créez une liste MGCP. Vous pouvez ensuite appliquer la liste MGCP lorsque vous activez l'inspection MGCP.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **MGCP**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste, puis cliquez sur **Edit** (Modifier).

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 (Facultatif) Cliquez sur l'onglet **Command Queue** (File d'attente de commandes) et spécifiez le nombre maximal de commandes autorisées dans la file d'attente de commande MGCP. La valeur par défaut est 200, et la plage autorisée est de 1 à 2 147 483 647.

Étape 5 Cliquez sur l'onglet **Gateways and Call Agents** (Passerelles et agents d'appel) et configurez les groupes de passerelles et les agents d'appel pour la liste.

a) Cliquez sur **Add** (Ajouter) pour créer un nouveau groupe, ou sélectionnez un groupe et cliquez sur **Edit** (Modifier).

b) Saisissez le **Group ID** (ID de groupe) du groupe d'agents d'appel. Un groupe d'agents d'appel associe un ou plusieurs agents d'appel à une ou plusieurs passerelles de support MGCP. La plage valide est de 0 à 2 147 483 647.

c) Ajoutez les adresses IP des passerelles de support qui sont contrôlées par les agents d'appel associés au groupe en les saisissant dans **Gateway to Be Added** (Passerelle à ajouter) et en cliquant sur **Add**>> (Ajouter). Supprimez les passerelles qui ne sont plus utilisées.

   Une passerelle multimédia est généralement un élément de réseau qui assure la conversion entre les signaux audio acheminés sur les circuits téléphoniques et les paquets de données acheminés sur Internet ou d'autres réseaux de paquets. Normalement, une passerelle envoie des commandes au port MGCP par défaut pour les agents d'appel, UDP 2727.

d) Ajoutez les adresses IP des agents d'appel qui contrôlent les passerelles de support MGCP en les saisissant dans **Call Agent to Be Added** (Agent d'appel à ajouter) et en cliquant sur **Add**>> (Ajouter). Supprimez tous les agents qui ne sont plus nécessaires.

   Normalement, un agent d'appel envoie des commandes au port MGCP par défaut pour les passerelles, UDP 2427.

e) Cliquez sur **OK** dans la boîte de dialogue MGCP Group (Groupe MGCP). Répétez le processus pour ajouter d'autres groupes, au besoin.

Étape 6 Cliquez sur **OK** dans la boîte de dialogue MGCP Inspect Map (Liste d'inspection MGCP).

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection MGCP.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection RTSP

L'inspection RTSP est activée par défaut. Vous ne devez le configurer que si vous souhaitez un traitement autre que celui par défaut. Les sections suivantes décrivent l'inspection des applications RTSP.

Survol de l'inspection RTSP

Le moteur d'inspection RTSP permet à l'ASA de transmettre les paquets RTSP. RTSP est utilisé par RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer et Cisco IP/TV.



Remarque Pour Cisco IP/TV, utilisez les ports TCP RTSP 554 et 8554.

Les applications RTSP utilisent le port bien connu 554 avec TCP (rarement UDP) comme canal de contrôle. L'ASA ne prend en charge que TCP, conformément à la RFC 2326. Ce canal de contrôle TCP est utilisé pour négocier les canaux de données utilisés pour transmettre le trafic audio/vidéo, en fonction du mode de transport configuré sur le client.

Les services de transport RDT pris en charge sont les suivants : rtp/avp, rtp/avp/udp, x-real-rdt, x-real-rdt/udp et x-pn-tng/udp.

L'ASA analyse les messages de réponse Setup avec un code d'état de 200. Si le message de réponse se déplace vers l'intérieur, le serveur est à l'extérieur par rapport à l'ASA et des canaux dynamiques doivent être ouverts pour les connexions entrantes du serveur. Si le message de réponse est sortant, l'ASA n'a pas besoin d'ouvrir de canaux dynamiques.

L'inspection RTSP ne prend pas en charge la PAT ou la NAT Twice. En outre, l'ASA ne peut pas reconnaître le camouflage HTTP où les messages RTSP sont masqués dans les messages HTTP.

Exigences de configuration de RealPlayer

Lorsque vous utilisez RealPlayer, il est important de configurer correctement le mode de transport. Pour l'ASA, ajoutez une commande **access-list** du serveur au client, ou vice versa. Pour RealPlayer, modifiez le mode de transport en cliquant sur **Options** > **Preferences (Préférences)** > **Transport** > **RTSP Settings (Paramètres RTSP)**.

Si vous utilisez le mode TCP sur RealPlayer, cochez les cases **Use TCP to Connect to Server** (Utiliser TCP pour la connexion au serveur) et **Attempt to use TCP for all content** (Tenter d'utiliser TCP pour tout le contenu). Sur l'ASA, il n'est pas nécessaire de configurer le moteur d'inspection.

Si vous utilisez le mode UDP sur RealPlayer, cochez les cases **Use TCP to Connect to Server** (Utiliser TCP pour se connecter au serveur) et **Attempt to use UDP for static content** (Tenter d'utiliser UDP pour le contenu statique), et pour le contenu en direct non disponible par multidiffusion. Sur l'ASA, ajoutez une commande **inspect rtsp**.

Limites de l'inspection RSTP

Les restrictions suivantes s'appliquent à l'inspection RSTP :

- L'ASA ne prend pas en charge le RTSP de multidiffusion ni les messages RTSP sur UDP.

- L'ASA n'a pas la capacité de reconnaître le camouflage HTTP où les messages RTSP sont masqués dans les messages HTTP.
- Avec Cisco IP/TV, le nombre de traductions effectuées par l'ASA sur la partie SDP du message est proportionnel au nombre de listes de programmes dans le gestionnaire de contenu (chaque liste de programme peut avoir au moins six adresses IP intégrées).
- Vous pouvez configurer la NAT pour Apple QuickTime 4 ou RealPlayer. Cisco IP/TV ne fonctionne qu'avec la NAT si la visionneuse et le gestionnaire de contenu se trouvent sur le réseau externe et si le serveur se trouve sur le réseau interne.

Configurer une liste des politiques d'inspection RTSP

Vous pouvez créer une liste des politiques d'inspection RTSP pour personnaliser les actions d'inspection RTSP si le comportement d'inspection par défaut n'est pas suffisant pour votre réseau.

Vous pouvez éventuellement créer une carte de trafic d'inspection RTSP pour définir la carte de trafic pour l'inspection RTSP. L'autre option consiste à définir les cartes de trafic directement dans la liste des politiques d'inspection RTSP. La différence entre la création d'une carte de trafic et la définition de la correspondance de trafic directement dans la liste d'inspection est que vous pouvez créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafic. Bien que cette procédure explique les cartes d'inspection, les critères de correspondance utilisés dans les cartes de trafics sont les mêmes que ceux expliqués à l'étape relative à l'onglet **Inspection**. Vous pouvez configurer les cartes de trafic RTSP en sélectionnant **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Class Maps (Cartes de trafic)** > **RTSP**, ou en les créant lors de la configuration de la liste d'inspection.

Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **RTSP**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste, puis cliquez sur **Edit** (Modifier).

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Cliquez sur l'onglet **Parameters** (Paramètres) et configurez les options souhaitées :

- **Enforce Reserve Port Protection** (Appliquer la protection des ports réservés) : indique s'il faut restreindre l'utilisation des ports réservés pendant la négociation du port de support.
- **Maximum URL Length** (Longueur maximale de l'URL) : longueur maximale de l'URL autorisée dans le message, de 0 à 6 000.

Étape 5 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

Vous pouvez définir les critères de correspondance du trafic en fonction des cartes de trafic HTTP, en configurant les correspondances directement dans la liste d'inspection, ou les deux.

a) Effectuez l'une des actions suivantes :
   - Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
   - Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez **Single Match** (Correspondance unique) pour définir le critère directement, ou **Multiple Match** (Correspondance multiple), auquel cas vous sélectionnez la carte de trafic RTSP qui définit les critères.

c) Si vous définissez le critère ici, choisissez le type de correspondance : **Match** (Correspondance) (le trafic doit correspondre au critère) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au critère). Par exemple, si No Match est sélectionné sur la chaîne « example.com », tout trafic contenant « example.com » est exclu de la carte de trafic. Configurez ensuite le critère comme suit :
   - **URL Filter** (Filtre d'URL) : met en correspondance l'URL avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
   - **Request Method** (Méthode de demande) : correspond à la méthode de demande : announce, describe, get_parameter, options, pause, play, record, redirect, setup, set_parameters, teardown.

d) Choisissez l'action à entreprendre pour le trafic correspondant. Pour la correspondance d'URL, vous pouvez abandonner la connexion ou la journaliser, et vous pouvez activer la journalisation des connexions abandonnées. Pour les correspondances de méthode de demande, vous pouvez appliquer une limite de débit en paquets par seconde.

e) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 6 Cliquez sur **OK** dans la boîte de dialogue RTSP Inspect Map (Liste d'inspection RTSP).

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection RTSP.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection SIP

SIP est un protocole très utilisé pour la conférence Internet, la téléphonie, la présence, la notification d'événements et la messagerie instantanée. En partie en raison de leur nature textuelle et en partie en raison de leur flexibilité, les réseaux SIP sont soumis à un grand nombre de menaces de sécurité.

L'inspection des applications SIP fournit la traduction d'adresses dans l'en-tête et le corps du message, l'ouverture dynamique de ports et les vérifications de base de l'intégrité. Elle prend également en charge la sécurité des applications et la conformité des protocoles, qui appliquent l'intégrité des messages SIP et détectent les attaques basées sur SIP.

L'inspection SIP est activée par défaut. Vous ne devez le configurer que si vous souhaitez un traitement autre que celui par défaut ou si vous souhaitez identifier un serveur proxy TLS pour activer l'inspection du trafic chiffré. Les rubriques suivantes expliquent l'inspection SIP plus en détail.

Présentation de l'inspection SIP

Le protocole SIP, tel que défini par l'IETF, permet les sessions de traitement d'appels, en particulier les conférences audio à deux parties, ou « appels ». SIP fonctionne avec SDP pour la signalisation d'appel. SDP spécifie les ports pour le flux de support. À l'aide du protocole SIP, l'ASA peut prendre en charge toutes les passerelles VoIP SIP et tous les serveurs proxy VoIP SIP. SIP et SDP sont définis dans les RFC suivantes :

- SIP : protocole d'initiation de session, RFC 3261
- SDP : protocole de description de session, RFC 2327

Pour prendre en charge les appels SIP par l'intermédiaire de l'ASA, les messages de signalisation pour les adresses de connexion du support, les ports du support et les connexions embryonnaires du support doivent être inspectés, car même si la signalisation est envoyée sur un port de destination bien connu (UDP/TCP 5060), les flux de support sont alloués dynamiquement. De plus, SIP intègre les adresses IP dans la partie données utilisateur du paquet IP. Notez que la longueur maximale de l'URI de la demande SIP prise en charge par l'ASA est de 255.

Les applications de messagerie instantanée (IM) utilisent également des extensions SIP (définies dans la RFC 3428) et des notifications d'événements spécifiques à SIP (RFC 3265). Une fois que les utilisateurs ont lancé une session de conversation (enregistrement/abonnement), les applications de messagerie instantanée utilisent les méthodes MESSAGE/INFO et les réponses 202 Accept lorsque les utilisateurs communiquent entre eux. Par exemple, deux utilisateurs peuvent être en ligne à tout moment, mais pas communiquer pendant des heures. Par conséquent, le moteur d'inspection SIP ouvre des passages qui expirent en fonction de la valeur de délai d'expiration SIP configurée. Cette valeur doit être configurée au moins cinq minutes de plus que la durée de l'abonnement. La durée de l'abonnement est définie dans la valeur Contact Expires et est généralement de 30 minutes.

Comme les demandes MESSAGE/INFO sont généralement envoyées en utilisant un port alloué dynamiquement autre que le port 5060, elles doivent passer par le moteur d'inspection SIP.



Remarque L'inspection SIP prend en charge uniquement la fonctionnalité de conversation. Le tableau blanc, le transfert de fichiers et le partage d'application ne sont pas pris en charge. Le client RTC 5.0 n'est pas pris en charge.

Limites pour l'inspection SIP

L'inspection SIP est testée et prise en charge pour Cisco Unified Communications Manager (CUCM) 7.0, 8.0, 8.6 et 10.5. Il n'est pas pris en charge pour CUCM 8.5 ou 9.x. L'inspection SIP peut fonctionner avec d'autres versions et produits.

Si vous constatez que les téléphones SIP ne se connectent pas au gestionnaire d'appels, vous pouvez essayer d'augmenter le nombre maximal de segments TCP non traités dans le CLI en utilisant la commande suivante : **sysopt connection tcp-max-unprocessed-seg** *6-24*. La valeur par défaut est 6, alors essayez un nombre plus élevé.

L'inspection SIP ne prend pas en charge le protocole IFP (Internet Facsimile Protocol) T.38. L'inspection SIP rejette les invitations SIP qui utilisent le sous-type audio MIME T.38. Si vous devez autoriser ce type, désactivez l'inspection SIP et écrivez une règle de contrôle d'accès qui autorise les flux RTP.

Limites de la NAT pour l'inspection SIP

- L'inspection SIP applique la NAT pour les adresses IP intégrées. Toutefois, si vous configurez la NAT pour traduire les adresses de source et de destination, l'adresse externe (« from » dans l'en-tête SIP pour le message de réponse « trying ») n'est pas réécrite. Ainsi, vous devez utiliser la NAT d'objet lorsque vous utilisez le trafic SIP afin d'éviter de traduire l'adresse de destination.
- Ne configurez pas la NAT ou la PAT pour les interfaces avec des niveaux de sécurité identiques ou inférieurs (source) à des niveaux de sécurité supérieurs (destination). Cette configuration n'est pas prise en charge.
- Si vous configurez l'inspection SIP pour une classe de trafic ciblé (c'est-à-dire pas la classe de trafic inspection_default), veillez à utiliser une liste de contrôle d'accès bidirectionnelle et à préciser uniquement le port de destination 5060. Sinon, vous risquez d'avoir des problèmes de NAT dans lesquels l'adresse IP dans l'en-tête SIP n'est pas traduite, même si le paquet IP est correctement traduit.
- Si vous codez en dur l'adresse mappée dans l'en-tête VIA de l'invitation SIP, n'activez pas l'inspection SIP. Vous pouvez rencontrer des problèmes si vous utilisez une NAT statique pour traduire l'adresse du client source et que l'interface de la route par défaut est différente de l'interface de la route connectée utilisée par le client.

Limites de la PAT pour l'inspection SIP

Les limitations et restrictions suivantes s'appliquent lorsque vous utilisez la PAT avec SIP :

- Si un terminal distant tente de s'enregistrer auprès d'un proxy SIP sur un réseau protégé par l'ASA, l'enregistrement échoue dans des conditions très spécifiques, comme suit :
  - La PAT est configurée pour le terminal distant.
  - Le serveur d'enregistrement SIP se trouve sur le réseau externe.
  - Le port est manquant dans le champ de contact du message REGISTER envoyé par le terminal au proxy.
- Si un périphérique SIP transmet un paquet dans lequel la partie SDP a une adresse IP dans le champ du propriétaire/créateur (o=) qui est différente de l'adresse IP dans le champ de connexion (c=), l'adresse IP dans le champ o= peut ne pas être correctement traduite. Cela est causé par une limitation du protocole SIP, qui ne fournit pas de valeur de port dans le champ o=. Comme la PAT a besoin d'un port pour la traduction, la traduction échoue.

- Lors de l'utilisation de la PAT, tout champ d'en-tête SIP qui contient une adresse IP interne sans port peut ne pas être traduit et, par conséquent, l'adresse IP interne sera transmise à l'extérieur. Si vous souhaitez éviter cette fuite, configurez la NAT au lieu de la PAT.

Inspection SIP par défaut

L'inspection SIP est activée par défaut à l'aide de la liste d'inspection par défaut, qui comprend les éléments suivants :

- Extensions de messagerie instantanée SIP : activées.
- Trafic non SIP sur le port SIP : abandonné.
- Masquer les adresses IP du serveur et du terminal : désactivé.
- Masquer la version du logiciel et les URI non SIP : désactivé.
- Assurez-vous que le nombre de sauts vers la destination est supérieur à 0 : activé.
- Conformité RTP : non appliquée.
- Conformité SIP : n'effectuez pas la vérification de l'état et la validation de l'en-tête.

Notez également que l'inspection du trafic chiffré n'est pas activée. Vous devez configurer un proxy TLS pour inspecter le trafic chiffré.

Configurer une liste des politiques d'inspection SIP

Vous pouvez créer une liste des politiques d'inspection SIP pour personnaliser les actions d'inspection SIP si le comportement d'inspection par défaut n'est pas suffisant pour votre réseau.

Vous pouvez éventuellement créer une carte de trafic d'inspection SIP pour définir la classes de trafic pour l'inspection SIP. L'autre option consiste à définir les classes de trafic directement dans la liste des politiques d'inspection SIP. La différence entre la création d'une carte de trafic et la définition de la correspondance de trafic directement dans la liste d'inspection est que vous pouvez créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafics. Bien que cette procédure explique les cartes d'inspection, les critères de correspondance utilisés dans les cartes de trafic sont les mêmes que ceux expliqués à l'étape relative à l'onglet **Inspection**. Vous pouvez configurer les cartes de trafic SIP en sélectionnant **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Class Maps (Cartes de trafic)** > **SIP**, ou en les créant lors de la configuration de la liste d'inspection.

Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **SIP** .

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier directement le niveau de sécurité ou cliquer sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans la vue **Security Level** (Niveau de sécurité) de la boîte de dialogue SIP Inspect Map (liste d'inspection SIP), sélectionnez le niveau qui correspond le mieux à la configuration souhaitée. Le niveau par défaut est Low (Bas).

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection SIP.

Étape 5 Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails), puis procédez comme suit :

a) Cliquez sur l'onglet **Filtering** (Filtrage) et choisissez d'activer les extensions de messagerie instantanée SIP ou d'autoriser le trafic non SIP sur le port SIP.

b) Cliquez sur l'onglet **IP Address Privacy** (Confidentialité des adresses IP) et choisissez de masquer les adresses IP du serveur et du terminal.

c) Cliquez sur l'onglet **Hop Count** (Nombre de sauts) et choisissez de vérifier que le nombre de sauts jusqu'à la destination est supérieur à 0. Cela vérifie la valeur de l'en-tête Max-Forwards, qui ne peut pas être nulle avant d'atteindre la destination. Vous devez également choisir l'action à prendre pour le trafic non conforme (abandon de paquet, abandon de connexion, réinitialisation ou journalisation) et activer ou désactiver la journalisation.

d) Cliquez sur l'onglet **Conformité RTP** et choisissez de vérifier ou non les paquets RTP qui passent par les passages pour vérifier la conformité du protocole. Si vous vérifiez la conformité, vous pouvez également choisir de limiter la charge utile à l'audio ou à la vidéo, en fonction de l'échange de signalisation.

e) Cliquez sur l'onglet **SIP Conformance** (Conformité SIP) et choisissez d'activer la vérification des transitions d'état et la validation stricte des champs d'en-tête. Pour chaque option que vous choisissez, sélectionnez l'action à entreprendre pour le trafic non conforme (abandon de paquet, abandon de connexion, réinitialisation ou journal) et indiquez si la journalisation doit être activée ou désactivée.

f) Cliquez sur l'onglet **Field Masking** (Masquage des champs) et choisissez d'inspecter les URI non SIP dans les en-têtes Alert-Info et Call-Info ainsi que la version du logiciel du serveur et du terminal dans les en-têtes User-Agent et Server. Pour chaque option choisie, sélectionnez l'action à appliquer (masquage ou journalisation) et indiquez si la journalisation doit être activée ou désactivée.

g) Cliquez sur l'onglet **TVS Server** (Serveur TVS) et identifiez les serveurs Trust Verification Services, qui permettent aux téléphones Cisco Unified IP d'authentifier les serveurs d'applications lors de l'établissement d'une connexion HTTPS. Vous pouvez identifier jusqu'à quatre serveurs; saisissez leurs adresses IP séparées par des virgules. L'inspection SIP ouvre des passages sur chaque serveur pour chaque téléphone enregistré, et le téléphone décide lequel utiliser.

Configurez le serveur des Services de vérification de confiance sur le serveur CUCM. Si la configuration utilise un port autre que celui par défaut, entrez le numéro de port (dans la plage de 1026 à 32 768). La valeur du port par défaut est 2445.

Étape 6 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

Vous pouvez définir les critères de correspondance du trafic à l'aide des cartes de trafic SIP, en configurant directement les correspondances dans la liste d'inspection, ou en combinant les deux méthodes.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez **Single Match** (Correspondance unique) pour définir directement le critère, ou **Multiple Match** (Correspondance multiple), puis sélectionnez la carte de trafic SIP qui définit les critères.

c) Si vous définissez le critère ici, choisissez le type de correspondance : **Match** (Correspondance) (le trafic doit correspondre au critère) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au critère). Par exemple, si No Match (Aucune correspondance) est sélectionné pour la chaîne « example.com », tout trafic contenant « example.com » est exclu de la carte de trafic. Configurez ensuite le critère comme suit :

- **Partie appelée** : correspond à la partie appelée, comme spécifié dans l'en-tête To, avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
- **Partie appelante** : correspond à la partie appelante, comme spécifié dans l'en-tête From, avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
- **Longueur du contenu** : correspond à un en-tête de contenu SIP d'une longueur supérieure à celle spécifiée, entre 0 et 65 536 octets.
- **Type de contenu** : correspond à l'en-tête Content Type, soit le type SDP, soit un type qui correspond à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- **Abonné IM** : correspond à l'abonné SIP IM à l'expression régulière ou à la liste d'expressions régulières sélectionnée.
- **Chemin du message** : correspond à l'en-tête SIP Via avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
- **Méthode de demande** : correspond à la méthode de demande SIP : ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, unknown, update.
- **Enregistrement tiers** : correspond au demandeur d'un enregistrement tiers avec l'expression régulière ou la liste d'expressions régulières sélectionnée.
- **Longueur de l'URI** : correspond à un URI dans les en-têtes SIP du type sélectionné (SIP ou TEL) qui est supérieur à la longueur spécifiée, entre 0 et 65 536 octets.

d) Choisissez l'action à prendre pour le trafic correspondant (abandon de paquet, perte de connexion, réinitialisation, journal) et s'il faut activer ou désactiver la journalisation. Pour les correspondances de méthode de demande avec « invite » et « register », vous pouvez également appliquer une limite de débit en paquets par seconde.

e) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 7 Cliquez sur **OK** dans la boîte de dialogue de la liste d'inspection SIP.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection SIP.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection Skinny (SCCP)

L'inspection d'application SCCP (Skinny) effectue la traduction de l'adresse IP et des numéros de port intégrés dans les données de paquets et l'ouverture dynamique de passages. Il effectue également des vérifications supplémentaires de conformité de protocole et un suivi de l'état de base.

L'inspection SCCP est activée par défaut. Vous ne devez le configurer que si vous souhaitez un traitement autre que celui par défaut ou si vous souhaitez identifier un serveur proxy TLS pour activer l'inspection du trafic chiffré.

Les sections suivantes décrivent l'inspection des applications SCCP.

Aperçu de l'inspection SCCP

Skinny (SCCP) est un protocole simplifié utilisé dans les réseaux VoIP. Les téléphones IP Cisco utilisant SCCP peuvent coexister dans un environnement H.323. Lorsqu'il est utilisé avec Cisco CallManager, le client SCCP peut interopérer avec les terminaux conformes à la norme H.323.

L'ASA prend en charge la PAT et la NAT pour SCCP. La PAT est nécessaire si vous avez plus de téléphones IP que d'adresses IP globales pour les téléphones IP à utiliser. En prenant en charge la NAT et la PAT des paquets de signalisation SCCP, l'inspection d'application Skinny garantit que tous les paquets de signalisation et de médias SCCP peuvent traverser l'ASA.

Le trafic normal entre Cisco CallManager et les téléphones IP Cisco utilise SCCP et est géré par l'inspection SCCP sans configuration spéciale. L'ASA prend également en charge les options DHCP 150 et 66, ce qu'il fait en envoyant l'emplacement d'un serveur TFTP aux téléphones IP Cisco et à d'autres clients DHCP. Les téléphones IP Cisco peuvent également inclure l'option DHCP 3 dans leurs demandes, qui définit la route par défaut.

Remarque L'ASA prend en charge l'inspection du trafic des téléphones IP Cisco exécutant le protocole SCCP version 22 et antérieures.

Prise en charge des téléphones IP Cisco

Dans les topologies où Cisco CallManager se trouve sur l'interface de sécurité la plus élevée par rapport aux téléphones IP Cisco, si la NAT est requise pour l'adresse IP Cisco CallManager, le mappage doit être statique, car un téléphone IP Cisco nécessite que l'adresse IP Cisco CallManager soit précisée explicitement dans sa

configuration. Une entrée d'identité statique permet à Cisco CallManager sur l'interface de sécurité supérieure d'accepter les enregistrements des téléphones IP Cisco.

Les téléphones IP Cisco nécessitent d'accéder à un serveur TFTP pour télécharger les informations de configuration dont ils ont besoin pour se connecter au serveur Cisco CallManager.

Lorsque les téléphones IP Cisco se trouvent sur une interface de sécurité inférieure à celle du serveur TFTP, vous devez utiliser une liste de contrôle d'accès pour vous connecter au serveur TFTP protégé sur le port UDP 69. Bien que vous ayez besoin d'une entrée statique pour le serveur TFTP, il n'est pas nécessaire qu'il s'agisse d'une entrée statique d'identité. Lors de l'utilisation de la NAT, une entrée statique d'identité est mappée à la même adresse IP. Lors de l'utilisation de la PAT, il est mappé à la même adresse IP et au même port.

Lorsque les téléphones IP Cisco se trouvent sur une interface de sécurité plus élevée que le serveur TFTP et Cisco CallManager, aucune entrée d'ACL ou statique n'est requise pour permettre aux téléphones IP Cisco d'établir la connexion.

Limites de l'inspection SCCP

L'inspection SCCP est testée et prise en charge pour Cisco Unified Communications Manager (CUCM) 7.0, 8.0, 8.6 et 10.5. Il n'est pas pris en charge pour CUCM 8.5 ou 9.x. L'inspection SCCP peut fonctionner avec d'autres versions et produits.

Si l'adresse d'un Cisco CallManager interne est configurée pour la NAT ou la PAT vers une adresse IP ou un port différent, les enregistrements pour les téléphones IP Cisco externes échouent, car l'ASA ne prend pas en charge la NAT ou la PAT pour le contenu du fichier transféré sur TFTP. Bien que l'ASA prenne en charge la NAT des messages TFTP et qu'il ouvre un passage pour le fichier TFTP, l'ASA ne peut pas traduire l'adresse IP et le port Cisco CallManager intégrés dans les fichiers de configuration du téléphone IP Cisco qui sont transférés par TFTP lors de l'enregistrement du téléphone.

Remarque L'ASA prend en charge le basculement avec état des appels SCCP, à l'exception des appels en cours d'établissement.

Inspection SCCP par défaut

L'inspection SCCP est activée par défaut en utilisant les valeurs par défaut suivantes :

- Enregistrement : non appliqué.
- ID de message maximal : 0x181.
- Longueur minimale du préfixe : 4
- Délai d'expiration du support : 00:05:00
- Délai d'expiration de la signalisation : 01:00:00.
- Conformité RTP : Non appliquée.

Configurer une liste des politiques d'inspection Skinny (SCCP)

Pour préciser les actions lorsqu'un message enfreint un paramètre, créez une liste des politiques d'inspection SCCP. Vous pouvez ensuite appliquer la liste des politiques d'inspection lorsque vous activez l'inspection SCCP.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **SCCP (Skinny)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Vous pouvez modifier le niveau de sécurité directement ou cliquer sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Security Level** (Niveau de sécurité) de la boîte de dialogue SCCP (Skinny) Inspect Map (Liste d'inspection SCCP [Skinny]), sélectionnez le niveau qui correspond le mieux à la configuration souhaitée. Le niveau par défaut est Low (Bas).

Si l'un des niveaux prédéfinis correspond à vos exigences, vous avez maintenant terminé. Cliquez simplement sur **OK**, ignorez le reste de cette procédure et utilisez la liste dans une règle de politique de service pour l'inspection SCCP.

Étape 5 Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails), puis procédez comme suit :

a) Cliquez sur l'onglet **Parameters** (Paramètres) et choisissez les options souhaitées.

- **Enforce endpoint registration** (Appliquer l'enregistrement des terminaux) : indique si les terminaux Skinny doivent s'enregistrer avant de passer ou de recevoir des appels.
- **Maximum Message ID** (ID de message maximal) : ID maximal de message de station SCCP autorisé. La valeur par défaut est 0x181. Le nombre hexadécimal peut être compris entre 0x0 et 0xffff.
- **SCCP Prefix Length** (Longueur du préfixe SCCP) : longueur maximale et minimale du préfixe SCCP. Le minimum par défaut est 4, et il n'y a pas de maximum par défaut.
- **Timeouts** (Délais d'expiration) : indique s'il faut définir des délais d'expiration pour les connexions de support et de signalisation, ainsi que la valeur de ces délais d'expiration. Les valeurs par défaut sont de 5 minutes pour les supports et de 1 heure pour la signalisation.

b) Cliquez sur l'onglet **RTP Conformance** (Conformité RTP) et choisissez de vérifier ou non les paquets RTP qui passent par les passages pour vérifier la conformité du protocole. Si vous vérifiez la conformité, vous pouvez également choisir de limiter la charge utile à l'audio ou à la vidéo, en fonction de l'échange de signalisation.

Étape 6 (Facultatif) Cliquez sur l'onglet **Message ID Filtering** (Filtrage d'ID de message) pour identifier le trafic à abandonner en fonction du champ d'ID de message de station dans les messages SCCP.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez le type de correspondance pour les critères : **Match** (le trafic doit correspondre au critère) ou **No Match** (le trafic ne doit pas correspondre au critère).
c) Dans les champs **Value** (Valeur), identifiez le trafic en fonction de la valeur de l'ID de message de station en hexadécimal, de 0x0 à 0xffff. Saisissez la valeur d'un seul ID de message ou saisissez la valeur de début et de fin pour une plage d'ID.
d) Choisissez d'activer ou de désactiver la journalisation. L'action est toujours d'abandonner le paquet.
e) Cliquez sur **OK** pour ajouter le filtre. Répétez le processus au besoin.

Étape 7 Cliquez sur **OK** dans la boîte de dialogue SCCP (Skinny) Inspect Map (Liste d'inspection SCCP [Skinny]).

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection SCCP.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Inspection STUN

Les utilitaires de traversée de session pour la NAT (STUN), définis dans la RFC 5389, sont utilisés par les clients WebRTC pour les communications en temps réel basées sur navigateur, de sorte que les modules d'extension ne sont pas nécessaires. Les clients WebRTC utilisent souvent des serveurs STUN en nuage pour connaître leurs adresses IP publiques et leurs ports. WebRTC utilise l'établissement de connectivité interactif (ICE, RFC 5245) pour vérifier la connectivité entre les clients. Ces clients utilisent généralement UDP, bien qu'ils puissent également utiliser TCP ou d'autres protocoles.

Comme les pare-feu bloquent souvent le trafic UDP sortant, les produits WebRTC tels que Cisco Spark peuvent avoir des problèmes pour effectuer les connexions. L'inspection STUN ouvre des passages pour les terminaux STUN et applique la conformité de base STUN et ICE pour permettre les communications pour les clients si la vérification de connectivité est reconnue par les deux côtés. Ainsi, vous pouvez éviter d'ouvrir de nouveaux ports dans vos règles d'accès pour activer ces applications.

Lorsque vous activez l'inspection STUN sur la carte de trafic d'inspection par défaut, le port TCP/UDP 3478 est surveillé pour le trafic STUN. L'inspection prend en charge uniquement les adresses IPv4 et TCP/UDP.

Il y a certaines limites de NAT pour l'inspection STUN. Pour le trafic WebRTC, les traductions NAT/PAT44 statiques sont prises en charge. Cisco Spark peut prendre en charge d'autres types de NAT, car Spark ne nécessite pas de passages. Vous pouvez également utiliser NAT/PAT64, y compris la NAT/PAT dynamique, avec Cisco Spark.

L'inspection STUN est prise en charge dans les modes de basculement et de grappe, car les passages sont dupliqués. Cependant, l'ID de transaction n'est pas répliqué sur les nœuds. Dans le cas où un nœud tombe en panne après avoir reçu une demande STUN et qu'un autre nœud a reçu la réponse STUN, la réponse STUN sera abandonnée.

Remarque L'inspection STUN utilise des identifiants de transaction pour faire correspondre les demandes et les réponses. Si vous utilisez le débogage pour résoudre les problèmes d'abandon de connexion, notez que le système modifie le format (endianness) des ID pour la sortie de débogage, de sorte qu'ils ne sont pas comparés directement à ceux que vous pourriez voir dans un pcap.

Pour en savoir plus sur l'activation de l'inspection STUN, consultez Configurer l'inspection du protocole de couche d'application, à la page 293.

Historique de l'inspection des protocoles vocaux et vidéo

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de SIP, SCCP et du proxy TLS pour IPv6	9.3(1)	Vous pouvez désormais inspecter le trafic IPv6 lorsque vous utilisez SIP, SCCP et le proxy TLS (à l'aide de SIP ou SCCP). Nous n'avons pas modifié d'écrans ASDM.
Prise en charge SIP pour les services de vérification de confiance, NAT66, CUCM 10.5 et les téléphones du modèle 8831.	9.3(2)	Vous pouvez maintenant configurer les serveurs des services de vérification de confiance dans l'inspection SIP. Vous pouvez également utiliser NAT66. L'inspection SIP a été testée avec CUCM 10.5. Nous avons ajouté la prise en charge de Trust Verification Services Server à la liste des politiques d'inspection SIP.
Amélioration des performances d'inspection SIP sur un ASA à plusieurs cœurs.	9.4(1)	Si vous avez plusieurs flux de signalisation SIP passant dans un ASA à plusieurs cœurs, les performances de l'inspection SIP ont été améliorées. Cependant, vous n'afficherez pas d'amélioration des performances si vous utilisez un mandataire TLS, téléphonique ou IME. Nous n'avons pas modifié d'écrans ASDM.
Prise en charge de l'inspection SIP dans la mise en grappe d'ASA	9.4(1)	Vous pouvez maintenant configurer l'inspection SIP sur la grappe ASA. Un flux de contrôle peut être créé sur n'importe quelle unité (en raison de l'équilibrage de charges), mais ses flux de données enfants doivent résider sur la même unité. La configuration du mandataire TLS n'est pas prise en charge. Nous n'avons pas modifié d'écrans.
La prise en charge de l'inspection SIP pour le mandataire téléphonique et le mandataire UC-IME a été supprimée.	9.4(1)	Vous ne pouvez plus utiliser le mandataire téléphonique ou le mandataire UC-IME lors de la configuration de l'inspection SIP. Utilisez le mandataire TLS pour inspecter le trafic chiffré. Nous avons supprimé le mandataire téléphonique et le mandataire UC-IME de la boîte de dialogue de politique de service Select SIP Inspect Map (Sélectionner la carte d'inspection SIP).

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de l'inspection H.323 pour le message H.225 FACILITY entrant avant le message H.225 SETUP pour la compatibilité avec H.460.18.	9.6(1)	Vous pouvez maintenant configurer une liste de politiques d'inspection H.323 pour permettre aux messages H.225 FACILITY de venir avant le message H.225 SETUP, ce qui peut se produire lorsque les terminaux sont conformes à H.460.18. Nous avons ajouté une option à l'onglet Call Attributes (Attributs d'appel) dans la liste des politiques d'inspection H.323.
Inspection STUN (Session Traversal Utilities for NAT)	9.6(2)	Vous pouvez désormais inspecter le trafic STUN pour les applications WebRTC, y compris Cisco Spark. L'inspection ouvre les passages nécessaires au trafic de retour. Nous avons ajouté une option à l'onglet Rule Actions (Actions de règles) > Protocol Inspection (Inspection de protocole) de la boîte de dialogue Add/Edit Service Policy (Ajouter/modifier une politique de service).
Prise en charge de TLSv1.2 dans le mandataire TLS et Cisco Unified Communications Manager 10.5.2.	9.7(1)	Vous pouvez désormais utiliser TLSv1.2 avec le mandataire TLS pour l'inspection SIP ou SCCP chiffrée avec Cisco Unified Communications Manager 10.5.2. Le mandataire TLS prend en charge les suites de chiffrement TLSv1.2 supplémentaires ajoutées dans le cadre de la commande **client cipher-suite**. Nous n'avons pas modifié d'écrans.
Le serveur mandataire TLS est obsolète pour l'inspection SCCP (Skinny).	9.13(1)	Le mot clé **tls-proxy** et la prise en charge de l'inspection chiffrée SCCP/Skinny sont désormais obsolètes. Le mot clé sera supprimé de la commande **inspect skinny** dans une version ultérieure.
La prise en charge du proxy TLS a été supprimée pour l'inspection SCCP (Skinny).	9.14(1)	Le mot-clé **tls-proxy** et la prise en charge de l'inspection chiffrée SCCP/Skinny ont été supprimés.
La liste des politiques d'inspection SIP par défaut abandonne le trafic non SIP.	9.16(1)	Pour le trafic inspecté pour le SIP, la valeur par défaut consiste désormais à abandonner le trafic non SIP. Auparavant, le trafic non SIP était autorisé sur les ports inspectés pour le SIP. Nous avons modifié la liste des politiques SIP par défaut pour inclure la commande **no traffic-non-sip**.



CHAPITRE 15

Inspection des réseaux mobiles

Les rubriques suivantes expliquent l'inspection des applications pour les protocoles utilisés dans les réseaux mobiles tels que LTE. Ces inspections nécessitent la licence Carrier (exploitant). Pour en savoir plus sur la raison pour laquelle vous devez utiliser l'inspection pour certains protocoles et sur les méthodes globales d'application de l'inspection, consultez Premiers pas avec l'inspection du protocole de la couche application, à la page 285.

- Aperçu de l'inspection du réseau mobile, à la page 367
- Licences pour l'inspection des protocoles de réseau mobile, à la page 375
- Valeurs par défaut pour l'inspection GTP, à la page 375
- Configurer l'inspection du réseau mobile, à la page 376
- Surveillance de l'inspection du réseau mobile, à la page 400
- Historique de l'inspection du réseau mobile, à la page 404

Aperçu de l'inspection du réseau mobile

Les rubriques suivantes expliquent les inspections disponibles pour les protocoles utilisés dans les réseaux mobiles tels que LTE. D'autres services sont disponibles pour le trafic SCTP en plus de l'inspection.

Présentation de l'inspection GTP

Le protocole de tunnellisation GPRS (GTP) est utilisé dans les réseaux GSM, UMTS et LTE pour le trafic GPRS (General Packet Radio Service). GTP fournit un protocole de gestion et de contrôle de tunnel pour fournir un accès réseau GPRS à une station mobile par la création, la modification et la suppression de tunnels. GTP utilise également un mécanisme de tunnellisation pour acheminer les paquets de données des utilisateurs.

Les réseaux des fournisseurs de services utilisent GTP pour tunnelliser les paquets multiprotocoles à travers le réseau fédérateur GPRS entre les terminaux. Dans GTPv0-1, GTP est utilisé pour la signalisation entre les nœuds de prise en charge GPRS de passerelle (GGSN) et les nœuds de prise en charge GPRS de service (SGSN). Dans GTPv2, la signalisation se fait entre les passerelles de réseau de données par paquets (PGW) et la passerelle de desserte (SGW), ainsi que d'autres terminaux. Le GGSN/PGW est l'interface entre le réseau de données sans fil GPRS et d'autres réseaux. Le SGSN/SGW effectue la mobilité, la gestion des sessions de données et la compression des données.

Vous pouvez utiliser l'ASA pour assurer une protection contre les partenaires d'itinérance pirates. Placez le périphérique entre le GGSN/PGW d'origine et les terminaux SGSN/SGW visités, et utilisez l'inspection GTP

sur le trafic. L'inspection GTP fonctionne uniquement sur le trafic entre ces terminaux. Dans GTPv2, cela s'appelle l'interface S5/S8.

GTP et les normes associées sont définies par le 3GPP (3e génération Partnership Project). Pour de plus amples renseignements, voir http://www.3gpp.org.

Suivi des changements d'emplacement pour les stations mobiles

Vous pouvez utiliser l'inspection GTP pour suivre les modifications d'emplacement des stations mobiles. Le suivi des modifications d'emplacement peut vous aider à identifier les frais d'itinérance frauduleux, par exemple, si vous voyez une station mobile se déplacer d'un emplacement à un autre dans un laps de temps improbable, comme le déplacement d'une cellule aux États-Unis vers une en Europe en 30 minutes.

Lorsque vous activez la journalisation de l'emplacement, le système génère des messages de journal système pour l'emplacement nouveau ou modifié pour chaque identité internationale d'abonné mobile (IMSI) :

- 324010 indique la création d'un nouveau contexte PDP et comprend le code de pays mobile (MCC), le code de réseau mobile (MNC), les éléments d'information et, éventuellement, l'ID de cellule où l'utilisateur est actuellement enregistré. L'ID de cellule est extrait de l'identification globale de cellule (CGI) ou de l'identifiant global de cellule E-UTRAN (ECGI).
- 324011 indique que l'IMSI s'est déplacée de celle stockée lors de la création du contexte PDP. Le message affiche le MCC/MNC précédent et actuel, les éléments d'information et, éventuellement, l'ID de cellule.

Par défaut, les messages syslog n'incluent pas d'informations d'horodatage. Si vous prévoyez d'analyser ces messages pour identifier l'itinérance improbable, vous devez également activer les horodatages. La journalisation de l'horodatage ne fait pas partie de la liste d'inspection GTP. Accédez à **Configuration** > **Device Management (Gestion des périphériques)** > **Logging (Journalisation)** > **Syslog Setup (Configuration Syslog)** et sélectionnez l'option **Enable Timestamp on Syslog Messages (Activer l'horodatage des messages Syslog)**.

Pour plus d'informations sur l'activation de la journalisation de l'emplacement, consultez Configurer une liste des politiques d'inspection GTP, à la page 376.

Limites d'inspection GTP

Voici quelques limites à l'inspection GTP :

- Les messages de superposition GTPv2 ne sont pas pris en charge. Ils sont toujours abandonnés.
- L'attachement d'UE d'urgence GTPv2 est pris en charge uniquement s'il contient l'IMSI (Identité Internationale d'Abonné Mobile).
- L'inspection GTP n'inspecte pas les données précoces. C'est-à-dire les données envoyées par un PGW ou SGW immédiatement après une demande de création de session, mais avant la réponse de création de session.
- Pour GTPv2, l'inspection prend en charge jusqu'à 3GPP 29.274 V15.5.0. Pour GTPv1, la prise en charge va jusqu'à 3GPP 29.060 V15.2.0. Pour GTPv0, la prise en charge est jusqu'à la version 8.
- L'inspection GTP ne prend pas en charge le transfert inter-SGSN vers le contexte PDP secondaire. L'inspection doit effectuer le transfert pour les contextes PDP principal et secondaire.
- Lorsque vous activez l'inspection GTP, les connexions qui utilisent l'encapsulation GTP-in-GTP sont toujours abandonnées.

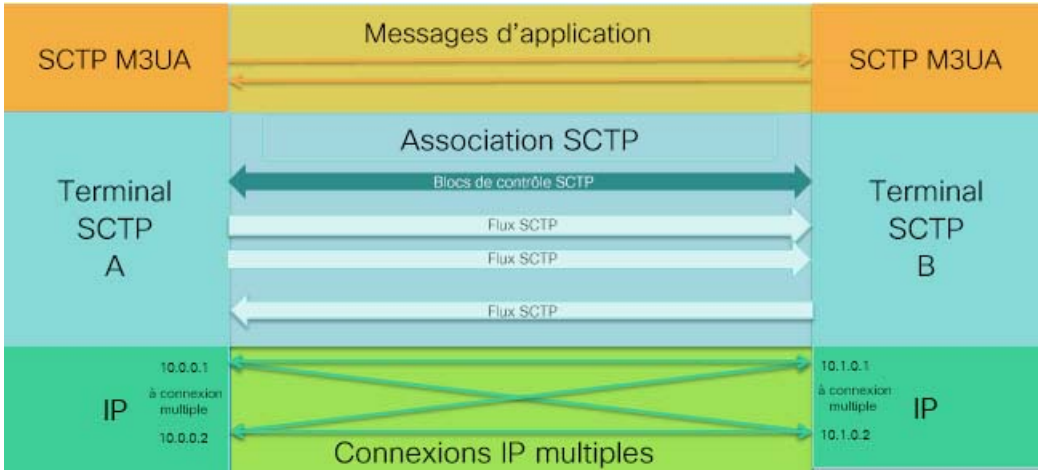
Inspection et contrôle d'accès SCTP (Stream Control Transmission Protocol)

Le protocole SCTP (Stream Control Transmission Protocol) est décrit dans la RFC 4960. Le protocole prend en charge le protocole de signalisation téléphonique SS7 sur IP et est également un protocole de transport pour plusieurs interfaces dans l'architecture de réseau mobile LTE 4G.

SCTP est un protocole de couche de transport fonctionnant au-dessus de l'IP dans la pile de protocoles, semblable à TCP et UDP. Cependant, SCTP crée un canal de communication logique, appelé association, entre deux nœuds terminaux sur une ou plusieurs adresses IP source ou de destination. C'est ce qu'on appelle la multilocalisation. Une association définit un ensemble d'adresses IP sur chaque nœud (source et destination) et un port sur chaque nœud. Toute adresse IP dans l'ensemble peut être utilisée comme adresse IP source ou de destination des paquets de données associés à cette association pour former plusieurs connexions. Dans chaque connexion, plusieurs flux peuvent exister pour envoyer des messages. Un flux dans SCTP représente un canal de données d'application logique.

La figure suivante illustre la relation entre une association et ses flux.

Illustration 38 : Relation entre l'association SCTP et les flux



Si vous avez un trafic SCTP passant par l'ASA, vous pouvez contrôler l'accès en fonction des ports SCTP et mettre en œuvre l'inspection de la couche d'application pour activer les connexions et éventuellement filtrer en fonction de l'ID du protocole de charge utile pour supprimer, consigner ou limiter le débit de manière sélective.

Remarque Chaque nœud peut avoir jusqu'à trois adresses IP. Toutes les adresses au-delà de la limite de trois sont ignorées et ne sont pas incluses dans l'association. Les passages pour les adresses IP secondaires s'ouvrent automatiquement. Vous n'avez pas besoin d'écrire de règles de contrôle d'accès pour les autoriser.

Pulsations et état d'association

Pour maintenir l'association et assurer un suivi précis, le moteur d'inspection surveille les pulsations SCTP. Le système relie la durée de la connexion aux signaux de pulsation. En cas de perte de la pulsation ou de fin explicite de l'association, le périphérique met fin à la connexion et termine la durée de l'événement.

Rapport d'association SCTP et de port

L'inspection SCTP est basée sur les associations plutôt que sur les flux. Comme le périphérique suit l'association complète comme une seule unité, il n'associe pas les ports de flux individuels aux champs de port traditionnels dans la sortie de journalisation. Par conséquent, lorsque vous affichez les détails de la connexion, vous pouvez observer les ports source et de destination affichés comme `0`. En effet, l'association est identifiée de manière unique par les adresses IP et l'ID d'association, plutôt que par les paires individuelles de ports source/destination.

Inspection dynamique SCTP

Comme pour le protocole TCP, le trafic SCTP est automatiquement inspecté au niveau de la couche 4 pour assurer un trafic bien structuré et une application limitée de la norme RFC 4960. Les éléments de protocole suivants sont inspectés et appliqués :

- Types de fragments, indicateurs et longueur.
- Étiquettes de vérification.
- Ports source et de destination pour empêcher les attaques par redirection d'association.
- Adresses IP.

L'inspection dynamique SCTP accepte ou rejette les paquets en fonction de l'état de l'association :

- Validation des séquences d'ouverture et de fermeture à 4 voies pour l'établissement initial de l'association.
- Vérification de la progression directe du TSN dans une association et un flux.
- Mettre fin à une association en voyant le chunk ABORT en raison d'une défaillance de pulsation. Les terminaux SCTP peuvent envoyer le chunk ABORT en réponse à des attaques de bombardement.

Si vous décidez que vous ne souhaitez pas ces vérifications d'application, vous pouvez configurer le contournement de l'état SCTP pour des classes de trafic spécifiques, comme expliqué dans la section Configurer les paramètres de connexion pour des classes de trafic spécifiques (tous les services), à la page 429.

Contrôle d'accès SCTP

Vous pouvez créer des règles d'accès pour le trafic SCTP. Ces règles sont similaires aux règles basées sur les ports TCP/UDP, où vous utilisez simplement **sctp** comme protocole et où les numéros de port sont des ports SCTP. Vous pouvez créer des objets ou des groupes de service pour SCTP, ou préciser directement les ports. Consultez les rubriques suivantes:

- Configurer des objets de service et des groupes de services, à la page 35
- Configurer les ACL étendues, à la page 56
- Configurer les règles d'accès, à la page 19

NAT SCTP

Vous pouvez appliquer la NAT d'objet réseau statique aux adresses dans les messages d'établissement d'association SCTP. Bien que vous puissiez configurer deux NAT statique, cela n'est pas recommandé, car la topologie de la partie destination de l'association SCTP est inconnue. Vous ne pouvez pas utiliser de NAT/PAT dynamique.

La NAT pour SCTP dépend de l'inspection dynamique SCTP plutôt que de l'inspection de la couche d'application SCTP. Ainsi, vous ne pouvez pas effectuer de trafic NAT si vous configurez le contournement de l'état SCTP.

Inspection de la couche application SCTP

Vous pouvez affiner vos règles d'accès en activant l'inspection et le filtrage SCTP sur les applications SCTP. Vous pouvez supprimer, consigner ou limiter de débit sélectivement des classes de trafic SCTP en fonction de l'identifiant de protocole de charge utile (PPID).

Si vous décidez d'effectuer un filtrage sur PPID, gardez les éléments suivants à l'esprit :

- Les PPID se trouvent dans des fragments de données, et un paquet donné peut avoir plusieurs fragments de données ou même un fragment de contrôle. Si un paquet comprend un fragment de contrôle ou plusieurs fragments de données, le paquet ne sera pas abandonné, même si l'action attribuée est abandonnée.
- Si vous utilisez le filtrage PPID pour abandonner ou limiter le débit des paquets, sachez que l'émetteur renvoyera tous les paquets abandonnés. Bien qu'un paquet pour un PPID à débit limité puisse passer lors de la prochaine tentative, un paquet pour un PPID abandonné sera de nouveau abandonné. Vous pouvez évaluer les conséquences ultérieures de ces abandons répétés sur votre réseau.

Limites de SCTP

La prise en charge de SCTP comprend les limites suivantes :

- Chaque nœud peut avoir jusqu'à trois adresses IP. Toutes les adresses au-delà de la limite de trois sont ignorées et ne sont pas incluses dans l'association. Les passages pour les adresses IP secondaires s'ouvrent automatiquement. Vous n'avez pas besoin d'écrire de règles de contrôle d'accès pour les autoriser.
- Les passages inutilisés expirent en 5 minutes.
- Les adresses IPv4 et IPv6 à double pile sur les terminaux multihébergés ne sont pas prises en charge.
- La NAT statique des objets réseau est le seul type de NAT pris en charge. De plus, NAT46 et NAT64 ne sont pas pris en charge.
- La fragmentation et le réassemblage des paquets SCTP sont effectués uniquement pour le trafic géré par l'inspection Diameter, M3UA et SCTP basée sur PPID.
- Les fragments ASCONF, qui sont utilisés pour ajouter ou supprimer dynamiquement des adresses IP dans SCTP, ne sont pas pris en charge.
- Le paramètre Hostname dans les messages INIT et INIT-ACK SCTP, qui est utilisé pour spécifier un nom d'hôte qui peut ensuite être résolu en une adresse IP, n'est pas pris en charge.
- SCTP/M3UA ne prend pas en charge le routage multichemin à coût égal (ECMP), qu'il soit configuré sur l'ASA ou ailleurs dans le réseau. Avec ECMP, les paquets peuvent être acheminés vers une destination sur plusieurs meilleurs chemins. Cependant, une réponse de paquet SCTP/M3UA à une destination unique doit revenir sur la même interface par laquelle elle est sortie. Même si la réponse peut provenir de n'importe quel serveur M3UA, elle doit toujours revenir sur la même interface par laquelle elle est sortie. Le signe de ce problème est que les paquets SCTP INIT-ACK sont abandonnés, ce que vous pouvez voir dans le compteur **show asp drop flow sctp-chunk-init-timeout** :

```
Flow drop:
SCTP INIT timed out (not receiving INIT ACK)(sctp-chunk-init-timeout)
```

Si vous rencontrez ce problème, vous pouvez le résoudre en configurant des routes statiques vers les serveurs M3UA ou en configurant le routage basé sur les politiques pour mettre en œuvre une conception de réseau qui garantit que les paquets INIT-ACK passent par la même interface que les paquets INIT.

Inspection Diameter

Diameter est un protocole d'authentification, d'autorisation et de comptabilité (AAA) utilisé dans les réseaux de télécommunications fixes et mobiles de nouvelle génération tels que EPS (Evolved Packet System) pour LTE (Long Term Evolution) et IMS (IP Multimedia Subsystem). Il remplace RADIUS et TACACS dans ces réseaux.

Diameter utilise TCP et SCTP comme couche de transport et sécurise les communications en utilisant TCP/TLS et SCTP/DTLS. Il peut également fournir le chiffrement d'objet de données, en option. Pour en savoir plus sur Diameter, consultez la RFC 6733.

Les applications Diameter effectuent des tâches de gestion de services telles que la décision d'accès de l'utilisateur, l'autorisation de service, la qualité de service et le taux de facturation. Bien que les applications Diameter puissent apparaître sur de nombreuses interfaces de plan de commande différentes dans l'architecture LTE, l'ASA inspecte les codes de commande Diameter et les paires attribut-valeur (AVP) pour les interfaces suivantes uniquement :

- S6a : Entité de gestion de la mobilité (MME) – Service d'abonnement local (HSS).
- S9 : Passerelle PDN (PDG) – serveur proxy/serveur AAA 3GPP.
- Rx : fonction des règles de politique et de facturation (PCRF) – fonction de contrôle de session d'appel (CSCF).

L'inspection Diameter ouvre les passages nécessaires pour permettre la communication avec les terminaux Diameter. L'inspection prend en charge 3GPP version 12 et est conforme à la norme RFC 6733. Vous pouvez l'utiliser pour TCP/TLS (en spécifiant un serveur proxy TLS lorsque vous activez l'inspection) et SCTP, mais pas SCTP/DTLS. Utilisez IPsec pour assurer la sécurité des sessions SCTP Diameter.

Vous pouvez éventuellement utiliser une liste des politiques d'inspection Diameter pour filtrer le trafic en fonction de l'ID d'application, des codes de commande et des AVP, afin d'appliquer des actions spéciales telles que l'abandon de paquets ou de connexions, ou leur journalisation. Vous pouvez créer un AVP personnalisé pour les applications Diameter nouvellement enregistrées. Le filtrage vous permet d'affiner le trafic que vous autorisez sur votre réseau.

Remarque Les messages Diameter pour les applications qui fonctionnent sur d'autres interfaces seront autorisés et transmis par défaut. Cependant, vous pouvez configurer une liste des politiques d'inspection Diameter pour abandonner ces applications par ID d'application, bien que vous ne puissiez pas spécifier d'actions en fonction des codes de commande ou des AVP pour ces applications non prises en charge.

Inspection M3UA

M3UA : MTP3 User Adaptation (M3UA) est un protocole client/serveur qui fournit une passerelle vers le réseau SS7 pour les applications IP qui communiquent avec la couche SS7 Message Transfer Part 3 (MTP3). M3UA permet d'exécuter les composants SS7 (comme ISUP) sur un réseau IP. M3UA est défini dans la RFC 4666.

M3UA utilise SCTP comme couche de transport. Le port SCTP 2905 est le port par défaut.

La couche MTP3 fournit des fonctions de réseau telles que le routage et l'adressage de nœud, mais utilise des codes de point pour identifier les nœuds. La couche M3UA échange les codes de point d'origine (OPC) et les codes de point de destination (DPC). C'est similaire à la façon dont IP utilise les adresses IP pour identifier les nœuds.

L'inspection M3UA fournit une conformité de protocole limitée. Vous pouvez éventuellement mettre en œuvre une vérification stricte de l'état du processus de serveur d'applications (ASP) et une validation supplémentaire des messages pour certains messages. Une vérification stricte de l'état de l'ASP est requise si vous souhaitez un basculement dynamique ou si vous souhaitez effectuer des opérations dans une grappe. Cependant, la vérification stricte de l'état ASP fonctionne uniquement en mode Override, elle ne fonctionne pas si vous êtes en mode Loadsharing ou Broadcast (selon la RFC 4666). L'inspection suppose qu'il y ait un et un seul ASP par terminal.

Vous pouvez éventuellement appliquer la politique d'accès en fonction des codes de point ou des indicateurs de service (SI). Vous pouvez également appliquer une limitation de débit en fonction de la classe et du type de message.

Conformité au protocole M3UA

L'inspection M3UA fournit l'application limitée du protocole suivante. L'inspection abandonne et journalise les paquets qui ne répondent pas aux exigences.

- En-tête du message commun. L'inspection valide tous les champs de l'en-tête commun.
  - Version 1 uniquement.
  - La longueur du message doit être correcte.
  - La classe de type de message avec une valeur réservée n'est pas autorisée.
  - Un ID de message non valide dans la classe de message n'est pas autorisé.
- Message de données de charge utile.
  - Un seul paramètre d'un type donné est autorisé.
  - Les messages de données sur le flux SCTP 0 ne sont pas autorisés.
- Le champ Affected Point Code doit être présent dans les messages suivants ou le message est abandonné : Destination disponible (DAVA), Destination non disponible (DUNA), Audit de l'état de destination (DAUD), Congestion de la signalisation (SCON), Partie utilisateur de destination non disponible (DUPU), Destination restreinte (DRST).
- Si vous activez la validation des balises de message pour les messages suivants, le contenu de certains champs est vérifié et validé. Les messages qui échouent à la validation sont abandonnés.
  - Destination User Part Unavailable (DUPU) : le champ Utilisateur/Cause doit être présent et ne doit contenir que des codes de cause et d'utilisateur valides.
  - Erreur : tous les champs obligatoires doivent être présents et contenir uniquement des valeurs autorisées. Chaque message d'erreur doit contenir les champs obligatoires pour ce code d'erreur.
  - Notification : les champs Type d'état et Informations sur l'état ne doivent contenir que des valeurs autorisées.

- Si vous activez la validation stricte de l'état du processus de serveur d'applications (ASP), le système conserve les états ASP des sessions M3UA et autorise ou abandonne les messages ASP en fonction du résultat de la validation. Si vous n'activez pas la validation stricte de l'état ASP, tous les messages ASP sont transmis sans inspection.

Limites d'inspection M3UA

Voici quelques limites relatives à l'inspection M3UA.

- La NAT n'est pas prise en charge pour les adresses IP intégrées dans les données M3UA.
- La validation stricte de l'état du processus de serveur d'applications (ASP) M3UA dépend de l'inspection avec état SCTP. Ne mettez pas en œuvre le contournement de l'état SCTP et la validation stricte ASP M3UA sur le même trafic.
- Une vérification stricte de l'état de l'ASP est requise si vous souhaitez un basculement dynamique ou si vous souhaitez effectuer des opérations dans une grappe. Cependant, la vérification stricte de l'état ASP ne fonctionne qu'en mode Override. Elle ne fonctionne pas si vous utilisez le mode Loadsharing ou Broadcast (selon la RFC 4666). L'inspection suppose qu'il y ait un et un seul ASP par terminal.

Aperçu de l'inspection de comptabilité RADIUS

L'objectif de l'inspection de comptabilité RADIUS est d'empêcher les attaques de surfacturation sur les réseaux GPRS qui utilisent des serveurs RADIUS. Bien que vous n'ayez pas besoin de la licence Carrier (exploitant) pour mettre en œuvre l'inspection de comptabilité RADIUS, elle n'a d'objet que si vous mettez en œuvre l'inspection GTP et que vous avez une configuration GPRS.

L'attaque par surfacturation dans les réseaux GPRS entraîne la facturation aux consommateurs de services qu'ils n'ont pas utilisés. Dans ce cas, un agresseur malveillant établit une connexion à un serveur et obtient une adresse IP du SGSN. Lorsque l'agresseur met fin à l'appel, le serveur malveillant continue de lui envoyer des paquets, qui sont abandonnés par le GGSN, mais la connexion du serveur reste active. L'adresse IP attribuée à l'agresseur malveillant est libérée et réattribuée à un utilisateur légitime qui sera ensuite facturé pour les services que l'agresseur utilisera.

L'inspection de comptabilité RADIUS empêche ce type d'attaque en vérifiant que le trafic vu par le GGSN est légitime. Avec la fonctionnalité de comptabilité RADIUS correctement configurée, l'ASA rompt une connexion en fonction de la correspondance de l'attribut Framed IP dans le message Radius Accounting Request Start avec le message Radius Accounting Request Stop. Lorsque le message Stop s'affiche avec l'adresse IP correspondante dans l'attribut Framed IP, l'ASA recherche toutes les connexions dont la source correspond à l'adresse IP.

Vous avez la possibilité de configurer une clé secrète prépartagée avec le serveur RADIUS afin que l'ASA puisse valider le message. Si le secret partagé n'est pas configuré, l'ASA vérifiera uniquement que l'adresse IP source fait partie des adresses configurées autorisées à envoyer les messages RADIUS.



Remarque Lors de l'utilisation de l'inspection de comptabilité RADIUS avec GPRS activé, l'ASA vérifie 3GPP-Session-Stop-Indicator dans les messages Accounting Request STOP afin de gérer correctement les contextes PDP secondaires. Plus précisément, l'ASA exige que les messages Accounting Request STOP comprennent l'attribut 3GPP-SGSN-Address avant de mettre fin aux sessions utilisateur et à toutes les connexions associées. Certains GGSN tiers peuvent ne pas envoyer cet attribut par défaut.

Licences pour l'inspection des protocoles de réseau mobile

L'inspection des protocoles suivants nécessite la licence indiquée dans le tableau ci-dessous.

- GTP
- SCTP
- Diamètre
- M3UA

Modèle	Exigence de licence
ASA virtuel, (tous les modèles)	Licence Carrier (exploitant) (activée par défaut)
Secure Firewall 3100	Licence d'opérateur
Firepower 4100	Licence d'opérateur
Firepower 9300	Licence Mobile Carrier
Tous les autres modèles	La licence Carrier (exploitant) n'est pas disponible sur les autres modèles. Vous ne pouvez pas inspecter ces protocoles.

Valeurs par défaut pour l'inspection GTP

L'inspection GTP n'est pas activée par défaut. Toutefois, si vous l'activez sans préciser votre propre liste d'inspection, une liste par défaut est utilisée et fournit le traitement suivant. Vous ne devez configurer une liste que si vous souhaitez des valeurs différentes.

- Les erreurs ne sont pas autorisées.
- Le nombre maximal de requêtes est de 200.
- Le nombre maximal de tunnels est de 500. Cela équivaut au nombre de contextes PDP (terminaux).
- Le délai d'expiration du terminal GTP est de 30 minutes. Les terminaux comprennent les réseaux GSN (GTPv0,1) et SGW/PGW (GTPv2).
- Le délai d'expiration du contexte PDP est de 30 minutes. Dans GTPv2, il s'agit du délai d'expiration du contexte du support.
- Le délai d'expiration de la demande est de 1 minute.
- Le délai d'expiration de signalisation est de 30 minutes.
- Le délai d'expiration de la tunnellisation est de 1 heure.
- Le délai d'expiration de réponse T3 est de 20 secondes.
- Les ID de message inconnus sont autorisés. Vous pouvez configurer les commandes **match message v1/v2 id range** pour supprimer et consigner toutes les commandes que vous ne prenez pas en charge ou

que vous souhaitez autoriser. Les messages sont considérés comme inconnus s'ils sont non définis ou définis dans les versions GTP que le système ne prend pas en charge.

Configurer l'inspection du réseau mobile

Les inspections pour les protocoles utilisés dans les réseaux mobiles ne sont pas activées par défaut. Vous devez les configurer si vous souhaitez prendre en charge les réseaux mobiles.

Procédure

Étape 1 (Facultatif) Configurer une liste des politiques d'inspection GTP, à la page 376.

Étape 2 (Facultatif) Configurer une liste des politiques d'inspection SCTP, à la page 380.

Étape 3 (Facultatif) Configurer une liste des politiques d'inspection Diameter, à la page 382.

Si vous souhaitez filtrer sur des paires attribut-valeur (AVP) qui ne sont pas encore prises en charge dans le logiciel, vous pouvez créer une AVP personnalisée à utiliser dans la liste des politiques d'inspection Diameter. Consultez Créer une paire attribut-valeur (AVP) de Diameter personnalisée, à la page 385.

Étape 4 (Facultatif) Si vous souhaitez inspecter le trafic Diameter TCP/TLS chiffré, créez le proxy TLS requis, comme décrit dans Inspection des sessions Diameter chiffrées, à la page 386

Étape 5 (Facultatif) Configurer une liste des politiques d'inspection M3UA, à la page 394

Étape 6 Configurer la politique de service d'inspection de réseau mobile , à la page 397.

Étape 7 (Facultatif) Configurer l'inspection de comptabilité RADIUS, à la page 398.

L'inspection de comptabilité RADIUS protège contre les attaques de surfacturation.

Configurer une liste des politiques d'inspection GTP

Si vous souhaitez appliquer des paramètres supplémentaires au trafic GTP et que la carte par défaut ne répond pas à vos besoins, créez et configurez une carte GTP.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **GTP**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste pour afficher son contenu. Cliquez sur **Customize** (Personnaliser) pour modifier la liste. Le reste de la procédure suppose que vous personnalisez ou ajoutez une liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Dans l'affichage **Security Level** (Niveau de sécurité) de la boîte de dialogue GTP Inspect Map (Liste d'inspection GTP), affichez la configuration actuelle de la liste.

La vue indique si la liste utilise les valeurs par défaut ou si vous l'avez personnalisée. Si vous devez personnaliser davantage les paramètres, cliquez sur **Details** (Détails) et poursuivez la procédure.

Astuces
Le bouton **IMSI Prefix Filtering** (Filtrage de préfixe IMSI) est un raccourci pour configurer le filtrage de préfixe IMSI, qui est expliqué plus loin dans cette procédure.

Étape 5 Cliquez sur l'onglet **Permit Parameters** (Paramètres d'autorisation) et configurez les options souhaitées.

- **Autoriser la réponse** : lorsque l'ASA effectue l'inspection GTP, l'ASA abandonne par défaut les réponses GTP des GSN ou des PGW qui n'ont pas été spécifiées dans la demande GTP. Cette situation se produit lorsque vous utilisez l'équilibrage de charge parmi un ensemble de terminaux GSN/PGW pour assurer l'efficacité et l'évolutivité de GPRS.

  Pour configurer le regroupement GSN/PGW et ainsi prendre en charge l'équilibrage de charge, créez un groupe d'objets réseau qui spécifie les terminaux GSN/PGW et sélectionnez-le en tant que **From Object Group** (Groupe d'objets source). De même, créez un groupe d'objets réseau pour le SGSN/SGW et sélectionnez-le comme «**To Object Group**» (Groupe d'objets de destination). Si le GSN/PGW qui répond appartient au même groupe d'objets que le GSN/PGW auquel la demande GTP a été envoyée et si le SGSN/SGW se trouve dans un groupe d'objets auquel le GSN/PGW qui répond est autorisé à envoyer une réponse GTP, l'ASA permet la réponse.

  Le groupe d'objets réseau peut identifier les terminaux par adresse d'hôte ou par le sous-réseau qui les contient.

- **Erreurs d'autorisation** : indique s'il faut autoriser tous les paquets, y compris les paquets GTP non valides ou les paquets qui échoueraient sinon à l'analyse et seraient abandonnés. Des paquets peuvent toujours être abandonnés en fonction des actions que vous définissez dans la liste des politiques.

Étape 6 Cliquez sur l'onglet **General Parameters** (Paramètres généraux) et configurez les options souhaitées :

- **Nombre maximal de demandes** : le nombre maximal de demandes GTP qui seront mises en file d'attente en attente d'une réponse.
- **Nombre maximal de tunnels** : le nombre maximal de tunnels GTP actifs autorisés. Cela équivaut au nombre de contextes PDP ou de terminaux. La valeur par défaut est 500. Les nouvelles demandes seront abandonnées une fois le nombre maximal de tunnels atteint.
- **Appliquer le délai d'inactivité** : s'il faut appliquer les délais d'inactivité pour les comportements suivants. Les délais d'expiration sont au format hh:mm:ss.
  - Terminal : période maximale d'inactivité avant le retrait d'un terminal GTP.
  - PDP-Context : période maximale d'inactivité avant la suppression du contexte PDP pour une session GTP. Dans GTPv2, il s'agit du contexte de support.

- Demande : période maximale d'inactivité après laquelle une demande est supprimée de la file d'attente de demande. Toutes les réponses ultérieures à une demande abandonnée seront également abandonnées.
- Signalisation : période maximale d'inactivité avant la suppression de la signalisation GTP.
- Délai d'attente de réponse T3 : délai d'attente maximal pour une réponse avant de retirer la connexion.
- Tunnel : période maximale d'inactivité du tunnel GTP avant son démontage.

Étape 7 Cliquez sur l'onglet **IMSI Prefix Filtering (Filtrage de préfixe IMSI)** et configurez le filtrage de préfixe IMSI si vous le souhaitez.

Par défaut, l'inspection GTP ne vérifie pas les combinaisons valides du code de pays mobile (MCC)/du code de réseau mobile (MNC). Si vous configurez le filtrage de préfixe IMSI, le MCC et le MNC dans l'IMSI du paquet reçu sont comparés aux combinaisons MCC/MNC configurées. Le système prend ensuite l'une des actions suivantes en fonction de l'option **Drop** (abandon) :

- **Drop not selected** (abandon non sélectionné) (par défaut) : le paquet est abandonné s'il ne correspond à aucune des combinaisons.
- **Drop selected** (abandon sélectionné) : le paquet est abandonné s'il correspond à au moins une combinaison.

Le code de pays mobile est une valeur non nulle à trois chiffres; ajoutez des zéros comme préfixe pour les valeurs à un ou à deux chiffres. Le code de réseau mobile est une valeur à deux ou trois chiffres.

Ajoutez toutes les combinaisons MCC et MNC que vous souhaitez autoriser ou abandonner. Par défaut, l'ASA ne vérifie pas la validité des combinaisons MNC et MCC. Vous devez donc vérifier la validité des combinaisons configurées. Pour en savoir plus sur les codes MCC et MNC, consultez la recommandation de l'UIT E.212, *Plan d'identification pour les stations mobiles terrestres*.

Étape 8 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

a) Effectuez l'une des actions suivantes :
   - Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
   - Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez le type de correspondance pour les critères : **Match** (Correspondance) (le trafic doit correspondre au critère) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au critère). Configurez ensuite le critère :
   - **Access Point Name** (Nom du point d'accès) : correspond au nom du point d'accès avec l'expression régulière ou la liste d'expressions régulières spécifiée. Par défaut, tous les messages avec des noms de point d'accès valides sont inspectés et n'importe quel nom est autorisé.
   - **Message ID** (ID du message) : correspond à l'ID du message, de 1 à 255. Vous pouvez spécifier une valeur ou une plage de valeurs. Vous devez préciser si le message est destiné à GTPv1 (qui comprend GTPv0) ou GTPv2. Par défaut, tous les ID de message valides sont autorisés.
   - **Message Length** (Longueur du message) : correspond aux messages dans lesquels la longueur de la charge utile UDP est comprise entre la longueur minimale et la longueur maximale spécifiées.

- **Version** : correspond à la version GTP, de 0 à 255. Vous pouvez spécifier une valeur ou une plage de valeurs. Par défaut, toutes les versions de GTP sont autorisées.
- **MSISDN** : correspond à l'élément d'information Mobile Station International Subscriber Directory Number (MSISDN) dans les messages Create PDP Context request, Create session request et Modify Bearer Response par rapport à l'expression régulière ou à la liste d'expressions régulières spécifiée. L'expression régulière peut identifier un MSISDN spécifique ou une plage de MSISDN en fonction du premier nombre x de chiffres. Le filtrage MSISDN est pris en charge pour GTPv1 et GTPv2 uniquement.
- **Selection Mode** (Mode de sélection) : correspond à l'élément d'information Selection Mode dans la demande Create PDP Context request. Le mode de sélection spécifie l'origine du nom de point d'accès (APN) dans le message et peut être l'un des suivants. Le filtrage en mode de sélection est pris en charge pour GTPv1 et GTPv2 uniquement.
  - 0 : vérifié. L'APN a été fourni par la station mobile ou le réseau, et l'abonnement est vérifié.
  - 1 : station mobile. L'APN a été fourni par la station mobile, et l'abonnement n'est pas vérifié.
  - 2 : réseau. L'APN a été fourni par le réseau, et l'abonnement n'est pas vérifié.
  - 3 : réservé, non utilisé.

c) Pour la correspondance d'ID de message, choisissez d'abandonner le paquet ou d'appliquer une limite de débit en paquets par seconde. L'action pour toutes les autres correspondances est d'abandonner le paquet. Pour toutes les correspondances, vous pouvez choisir d'activer la journalisation.

d) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 9 Cliquez sur l'onglet **Anti-Replay Protection** (Protection anti-replay) et configurez les options anti-replay.

- **Activer la fenêtre de relecture des paquets de données** : s'il faut activer l'anti-relecture en spécifiant une fenêtre glissante pour les messages GTP-U. La taille de la fenêtre glissante est en nombre de messages et peut être de 128, 256, 512 ou 1 024. Lorsque des messages valides s'affichent, la fenêtre se déplace vers les nouveaux numéros de séquence. Les numéros de séquence sont compris entre 0 et 65 535, avec encapsulation lorsqu'ils atteignent le maximum, et ils sont uniques par contexte PDP. Les messages sont considérés comme valides si leurs numéros de séquence se trouvent dans la fenêtre. L'anti-replay permet d'éviter le détournement de session ou les attaques DoS, qui peuvent se produire lorsqu'un pirate capture des paquets de données GTP et les rejoue.

Étape 10 Cliquez sur l'onglet **User-Spoofing** (Usurpation d'utilisateur) et configurez les options anti-usurpation d'utilisateur.

- **GTP Header Check** (Vérification de l'en-tête GTP) : indique s'il faut vérifier que la charge utile interne d'un paquet de données GTP est un paquet IP valide, et abandonner le paquet s'il a un en-tête non IP. Vous devez sélectionner cette option pour mettre en œuvre l'anti-usurpation d'adresse.
- **Anti-Spoofin**g (Anti-usurpation d'adresse) : indique s'il faut vérifier que l'adresse IP de l'utilisateur mobile dans l'en-tête IP de la charge utile interne correspond à l'adresse IP attribuée dans les messages de contrôle GTP tels que Create Session Response, et abandonner le message si les adresses IP ne correspondent pas. Les pirates peuvent se faire passer pour un autre client en utilisant une adresse IP différente de celle attribuée par GTP-C. L'anti-usurpation d'adresse vérifie si l'adresse GTP-U utilisée est bien celle qui a été attribuée à l'aide de GTP-C. Cette vérification prend en charge les types de PDN IPv4, IPv6 et IPv4v6.

Si la station mobile obtient son adresse à l'aide de DHCP, l'adresse IP de l'utilisateur final dans GTPv2 est 0.0.0.0 (IPv4) ou *le préfixe*::0 (IPv6). Dans ce cas, le système met à jour l'adresse IP de l'utilisateur final avec la première adresse IP trouvée dans les paquets internes. Vous pouvez modifier le comportement par défaut des adresses obtenues par DHCP à l'aide des mots-clés suivants :

- **GTPV2-DHCP-ByPass** : ne mettez pas à jour l'adresse 0.0.0.0 ou *le préfixe*::0. Au lieu de cela, autorisez les paquets dont l'adresse IP de l'utilisateur final est 0.0.0.0 ou *le préfixe*::0. Cette option contourne la vérification anti-usurpation d'adresse lorsque DHCP est utilisé pour obtenir l'adresse IP.
- **GTPV2-DHCP-DROP** : ne mettez pas à jour l'adresse 0.0.0.0 ou *le préfixe*::0. Au lieu de cela, abandonnez tous les paquets dont l'adresse IP de l'utilisateur final est 0.0.0.0 ou *le préfixe*::0. Cette option empêche l'accès pour les utilisateurs qui utilisent DHCP pour obtenir l'adresse IP.

Étape 11 Cliquez sur l'onglet **Location-Logging** (journalisation de l'emplacement) et configurez les options de journalisation de l'emplacement.

- **Location Logging** (Journalisation de l'emplacement) : indique s'il faut consigner l'emplacement des abonnés pour suivre les modifications d'emplacement des stations mobiles. Le suivi des modifications d'emplacement peut vous aider à identifier les frais d'itinérance potentiellement frauduleux. Lorsque vous activez la journalisation des emplacements, le système génère des messages de journal système pour les emplacements nouveaux (message 324010) ou modifiés (message 324011) pour chaque identité internationale d'abonné mobile (IMSI).

  Sélectionnez l'option **Cell-ID** (ID de cellule) si vous souhaitez que les messages de journalisation comprennent l'identification globale de cellule (CGI) ou l'identifiant global de cellule E-UTRAN (ECGI) où l'utilisateur est actuellement enregistré.

Étape 12 Cliquez sur **OK** dans la boîte de dialogue de la liste d'inspection GTP.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection GTP.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer la politique de service d'inspection de réseau mobile , à la page 397.

Configurer une liste des politiques d'inspection SCTP

Pour appliquer d'autres actions au trafic SCTP en fonction de l'identifiant de protocole de charge utile (PPID) spécifique à l'application, comme la limitation de débit, créez une liste des politiques d'inspection SCTP à utiliser par la politique de service.

Remarque Les PPID se trouvent dans des fragments de données, et un paquet donné peut avoir plusieurs fragments de données ou même un fragment de contrôle. Si un paquet comprend un fragment de contrôle ou plusieurs fragments de données, le paquet ne sera pas abandonné, même si l'action attribuée est abandonnée. Par exemple, si vous configurez une liste des politiques d'inspection SCTP pour abandonner le PPID 26 et qu'un bloc de données PPID 26 est combiné dans un paquet avec un bloc de données PPID Diameter, ce paquet ne sera pas abandonné.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **SCTP**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste, puis cliquez sur **Edit** (Modifier).

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Abandonnez, limitez le débit ou journalisez le trafic en fonction du PPID dans les fragments de données SCTP.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez le type de correspondance pour les critères : **Match** (Correspondance) (le trafic doit correspondre au PPID) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au PPID).

Par exemple, si vous sélectionnez No Match (Aucune correspondance) pour le PPID Diameter, tous les PPID, à l'exception de Diameter, sont exclus de la carte de trafic.

c) Choisissez **Minimum Payload PID** (PID de charge utile minimal) et, éventuellement, **Maximum Payload PID** (PID de charge utile maximal) à faire correspondre.

Vous pouvez saisir les PPID par nom ou par numéro (0 à 4 294 967 295). Cliquez sur le bouton **...** dans chaque champ pour effectuer une sélection dans une liste de PPID. Si vous sélectionnez un PPID maximal, la correspondance s'applique à la plage de PPID

Vous pouvez trouver la liste actuelle des PPID SCTP à l'adresse http://www.iana.org/assignments/sctp-paramètres/sctp-paramètres.xhtml#sctp-paramètres-25.

d) Choisissez d'abandonner (et de journaliser), de journaliser ou de limiter le débit (en kilobits par seconde, kbps) des paquets correspondants.

e) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 5 Cliquez sur **OK** dans la boîte de dialogue SCTP Inspect Map (Liste d'inspection SCTP).

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection SCTP.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer la politique de service d'inspection de réseau mobile , à la page 397.

Configurer une liste des politiques d'inspection Diameter

Vous pouvez créer une liste des politiques d'inspection Diameter pour filtrer divers éléments de protocole Diameter. Vous pouvez ensuite supprimer ou journaliser sélectivement les connexions.

Pour configurer le filtrage de message Diameter, vous devez avoir une bonne connaissance de ces éléments de protocole tels qu'ils sont définis dans les RFC et les spécifications techniques. Par exemple, l'IETF dispose d'une liste des applications enregistrées, des codes de commande et des paires attribut-valeur à l'adresse http://www.iana.org/assignments/aaa-paramètres/aaa-paramètres.xhtml, bien que l'inspection Diameter ne prenne pas en charge tous éléments répertoriés. Consultez le site Web de 3GPP pour connaître leurs caractéristiques techniques.

Vous pouvez éventuellement créer une carte de trafic d'inspection Diameter pour définir les critères de filtrage des messages pour l'inspection Diameter. L'autre option consiste à définir les critères de filtrage directement dans la liste des politiques d'inspection Diameter. La différence entre la création d'une carte de trafic et la définition des critères de filtrage directement dans la liste d'inspection est que vous pouvez créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafics. Bien que cette procédure explique les cartes d'inspection, les critères de correspondance utilisés dans les cartes de trafic sont les mêmes que ceux expliqués à l'étape relative à l'onglet **Inspection**. Vous pouvez configurer les cartes de trafic Diameter en sélectionnant **Configuration** > **Firewall** > **Objects** > **Class Maps (Cartes de trafic)** > **Diameter** > **(Configuration** > **Pare-feu** > **Objets** > **cartes de trafic** > **Diameter**), ou en les créant lors de la configuration de la liste des politiques d'inspection.

Astuces Vous pouvez configurer des listes d'inspection lors de la création de politiques de service, en plus de la procédure expliquée ci-dessous. Le contenu de la liste est le même, quelle que soit la façon dont vous la créez.

Avant de commencer

Certaines options de correspondance de trafic utilisent des expressions régulières à des fins de correspondance. Si vous avez l'intention d'utiliser l'une de ces techniques, créez d'abord l'expression régulière ou la carte de trafic d'expressions régulières.

Procédure

Étape 1 **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **Diameter**

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.

- Sélectionnez une liste et cliquez sur **Edit** (Modifier) pour afficher son contenu.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Cliquez sur l'onglet **Parameters** (Paramètres) et choisissez les options souhaitées. si vous souhaitez consigner les messages contenant des éléments Diameter non pris en charge.

- **Unsupported Parameters** (Paramètres non pris en charge) : indique si vous souhaitez consigner les messages contenant des éléments Diameter non pris en charge. Vous pouvez consigner les éléments **Application ID** (ID d'application), **Command Code** (Code de commande) ou **Attribute Value Pair (AVP)** (Paire attribut-valeur (AVP)) qui ne sont pas directement pris en charge.
- **Strict Diameter Validation Parameters** (Paramètres de validation Diameter stricte) : active la conformité stricte du protocole Diameter à la RFC 6733. Par défaut, l'inspection garantit que les trames Diameter sont conformes à la RFC. Vous pouvez ajouter une validation de message liée à la session et une validation de machine d'état.

Étape 5 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

Vous pouvez définir les critères de correspondance du trafic en fonction des cartes de trafic Diameter, en configurant les correspondances directement dans la liste d'inspection, ou les deux.

a) Effectuez l'une des actions suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
- Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez **Single Match** (Correspondance unique) pour définir directement le critère, ou **Multiple Match** (Correspondances multiples), auquel cas vous sélectionnez la carte de trafic Diameter qui définit les critères.

c) Si vous définissez le critère ici, choisissez le type de correspondance : **Match** (Correspondance) (le trafic doit correspondre au critère) ou **No Match** (Aucune correspondance) (le trafic ne doit pas correspondre au critère). Configurez ensuite le critère comme suit :

- **Application ID** (ID d'application) : saisissez le nom ou le numéro de l'application Diameter (de 0 à 4 294 967 295). S'il y a une plage d'applications numérotées consécutivement que vous souhaitez mettre en correspondance, vous pouvez inclure un deuxième identifiant. Vous pouvez définir la plage par nom ou numéro d'application, et elle s'applique à tous les nombres entre le premier et le deuxième ID.

  Ces applications sont enregistrées auprès de l'IANA. Voici les applications principales prises en charge, mais vous pouvez filtrer d'autres applications.

  - **3gpp-rx-ts29214** (16777236)
  - **3gpp-s6a** (16777251)
  - **3gpp-s9** (16777267)
  - **common-message** (0). Il s'agit du protocole Diameter de base.

- **Command Code** (Code de commande) : saisissez le nom ou le numéro du code de commande Diameter (0 à 4 294 967 295). S'il existe une plage de codes de commande numérotés consécutivement à laquelle vous souhaitez mettre en correspondance, vous pouvez inclure un deuxième code. Vous

pouvez définir la plage par nom ou numéro de code de commande, et elle s'applique à tous les nombres entre le premier et le deuxième codes.

Par exemple, pour faire correspondre le code de commande de demande/réponse d'échange de capacité, CER/CEA, saisissez **cer-cea**.

- **Attribute Value Pair** (Paire attribut-valeur) : vous pouvez mettre en correspondance l'AVP par attribut uniquement, une plage d'AVP ou un AVP en fonction de la valeur de l'attribut. Pour **AVP Begin Value** (Valeur de début d'AVP), vous pouvez spécifier le nom d'un AVP personnalisé ou enregistré dans les spécifications techniques des RFC ou de 3GPP et directement pris en charge dans le logiciel. Cliquez sur le bouton **...** dans le champ pour choisir un élément dans une liste.

  Si vous souhaitez faire correspondre une plage d'AVP, spécifiez AVP **End Value** (Valeur de fin d'AVP) par numéro uniquement. Si vous souhaitez faire correspondre un AVP par sa valeur, vous ne pouvez pas spécifier de deuxième code.

  Vous pouvez affiner la correspondance en précisant l' **ID de fournisseur**facultatif, de 0 à 4 294 967 295. Par exemple, l'ID du fournisseur 3GPP est 10415, l'IETF est 0.

  Vous pouvez configurer la mise en correspondance de valeur uniquement si le type de données de l'AVP est pris en charge. Par exemple, vous pouvez spécifier une adresse IP pour un AVP qui a le type de données d'adresse. La liste des AVP affiche le type de données pour chacun. La façon dont vous spécifiez la valeur diffère en fonction du type de données AVP :

  - Diameter Identity, Diameter URI, Octet String : sélectionnez l'expression régulière ou les objets de liste d'expressions régulières pour correspondre à ces types de données.
  - Adresse : spécifiez l'adresse IPv4 ou IPv6 pour la correspondance. Par exemple, 10.100.10.10 ou 2001:DB8::0DB8:800:200C:417A.
  - Temps : précisez les dates et l'heure de début et de fin. Les deux sont requis. L'heure est au format 24 heures.
  - Numérique : spécifiez une plage de numéros. La plage de numéros valide dépend du type de données :
    - Integer32 : -2 147 483 647 à 2 147 483 647
    - Integer64 : -9 223 372 036 854 775 807 à 9 223 372 036 854 775 807
    - Unsigned32 : 0 à 4 294 967 295
    - Unsigned64 : 0 à 18 446 744 073 709 551 615
    - Float32 : représentation en point décimal avec une précision de 8 chiffres
    - Float64 : représentation en point décimal avec une précision de 16 chiffres

d) Choisissez l'action à entreprendre pour le trafic correspondant : abandonner le paquet, abandonner la connexion ou se connecter.
e) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 6 Cliquez sur **OK** dans la boîte de dialogue Diameter Inspect Map (Liste d'inspection Diameter).

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection Diameter.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer la politique de service d'inspection de réseau mobile , à la page 397.

Créer une paire attribut-valeur (AVP) de Diameter personnalisée

À mesure que de nouvelles paires attribut-valeur (AVP) sont définies et enregistrées, vous pouvez créer des AVP Diameter personnalisées pour les définir et les utiliser dans votre liste des politiques d'inspection Diameter. Vous obtiendriez les informations dont vous avez besoin pour créer l'AVP à partir de la RFC ou d'une autre source qui définit l'AVP.

Créez des AVP personnalisées uniquement si vous souhaitez les utiliser dans une liste des politiques d'inspection Diameter ou une carte de trafic pour la correspondance d'AVP.

Procédure

Étape 1 Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Listes d'inspection)** > **Diameter AVP (AVP Diameter)** .

Étape 2 Cliquez sur **Add** (Ajouter) pour créer une nouvelle entrée.

Lorsque vous modifiez un AVP, vous pouvez modifier la description uniquement.

Étape 3 Configurez les options suivantes :

- **Name**(nom) : le nom de l'AVP personnalisé que vous créez, jusqu'à 32 caractères. Vous vous référerez à ce nom dans une liste des politiques d'inspection ou une carte de trafic lors de la définition d'une correspondance de paire attribut-valeur.
- **Custom Code** (Code personnalisé) : valeur du code AVP personnalisé, de 256 à 4 294 967 295. Vous ne pouvez pas saisir une combinaison de code et d'identifiant de fournisseur qui est déjà définie dans le système.
- **Data Type** (Type de données) : type de données de l'AVP. Vous pouvez définir les types d'AVP suivants. Si le nouvel AVP est d'un type différent, vous ne pouvez pas créer d'AVP personnalisé pour celui-ci.
  - Adresse (pour les adresses IP)
  - Identité de Diameter
  - Identifiant de ressource uniforme (URI) Diameter
  - Nombre à virgule flottante 32 bits
  - Nombre à virgule flottante 64 bits
  - Nombre entier de 32 bits
  - Nombre entier de 64 bits
  - Chaîne d'octets
  - Durée
  - Entier non signé 32 bits

- Entier non signé 64 bits

- **Vendor ID** (ID du fournisseur) : facultatif. Le numéro d'ID du fournisseur qui a défini l'AVP, de 0 à 4 294 967 295. Par exemple, l'ID du fournisseur 3GPP est 10415, l'IETF est 0.
- **Description** : (facultatif.) Une description de l'AVP, jusqu'à 80 caractères.

Étape 4 Cliquez sur **OK**.

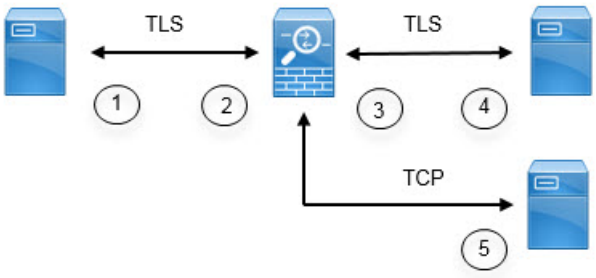
Inspection des sessions Diameter chiffrées

Si une application Diameter utilise des données chiffrées sur TCP, l'inspection ne peut pas voir à l'intérieur des paquets pour mettre en œuvre vos règles de filtrage de message. Ainsi, si vous créez des règles de filtrage et que vous souhaitez qu'elles s'appliquent également au trafic TCP chiffré, vous devez configurer un proxy TLS. Vous avez également besoin d'un proxy si vous souhaitez appliquer strictement le protocole sur le trafic chiffré. Cette configuration ne s'applique pas au trafic SCTP/DTLS.

Le proxy TLS agit en tant qu'homme du milieu. Il déchiffre le trafic, l'inspecte, puis le chiffre à nouveau et l'envoie à la destination prévue. Ainsi, les deux côtés de la connexion, le serveur Diameter et le client Diameter, doivent faire confiance à l'ASA et toutes les parties doivent avoir les certificats requis. Vous devez avoir une bonne compréhension des certificats numériques pour mettre en œuvre le proxy TLS. Veuillez lire le chapitre sur les certificats numériques dans le guide de configuration générale ASA.

L'illustration suivante montre la relation entre le client et le serveur Diameter, l'ASA et les exigences de certification pour établir la confiance. Dans ce modèle, un client Diameter est un MME (Mobility Management Entity) et non un utilisateur final. Le certificat de l'autorité de certification de chaque côté d'un lien est celui utilisé pour signer le certificat de l'autre côté du lien. Par exemple, le certificat de l'autorité de certification du proxy TLS de l'ASA est celui utilisé pour signer le certificat client Diameter/TLS.

Illustration 39 : Inspection TLS Diameter



1	Client TLS Diameter (MME) • Certificat d'identité du client • Certificat d'autorité de certification utilisé pour signer le certificat d'identité du serveur proxy TLS ASA	2	Serveur proxy TLS ASA • Certificat d'identité du serveur • Certificat d'autorité de certification utilisé pour signer le certificat d'identité du client TLS Diameter

3	Client proxy TLS ASA • Certificat d'identité du client (statique ou LDC) • Certificat d'autorité de certification utilisé pour signer le certificat d'identité du serveur TLS Diameter	4	Serveur TLS Diameter (proxy complet) • Certificat d'identité du serveur • Certificat d'autorité de certification utilisé pour signer le certificat d'identité du client proxy TLS ASA
5	Serveur TCP Diameter (déchargement TLS).	—	—

Vous avez les options suivantes pour configurer le proxy TLS pour l'inspection Diameter :

- Proxy TLS complet : chiffrez le trafic entre l'ASA et les clients Diameter, ainsi qu'entre l'ASA et le serveur Diameter. Vous avez les options suivantes pour établir la relation d'approbation avec le serveur TLS :
  - Utilisez un point de confiance client proxy statique. L'ASA présente le même certificat pour chaque client Diameter lors de la communication avec le serveur Diameter. Comme tous les clients se présentent de la même manière, le serveur Diameter ne peut pas fournir de services différentiels par client. D'autre part, cette option est plus rapide que la méthode LDC.
  - Utilisez des certificats dynamiques locaux (LDC). Avec cette option, l'ASA présente des certificats uniques par client Diameter lors de la communication avec le serveur Diameter. Le LDC conserve tous les champs du certificat d'identité du client reçu, à l'exception de sa clé publique et d'une nouvelle signature de l'ASA. Cette méthode donne au serveur Diameter une meilleure visibilité sur le trafic client, ce qui permet de fournir des services différentiels en fonction des caractéristiques du certificat client.
- Déchargement TLS : chiffrez le trafic entre l'ASA et le client Diameter, mais utilisez une connexion en texte clair entre l'ASA et le serveur Diameter. Cette option est viable si le serveur Diameter se trouve dans le même centre de données que l'ASA, où vous êtes certain que le trafic entre les périphériques ne quittera pas la zone protégée. L'utilisation du déchargement TLS peut améliorer les performances, car elle réduit la quantité de traitement de chiffrement requise. Il devrait s'agir de l'option la plus rapide. Le serveur Diameter peut appliquer des services différentiels en fonction de l'adresse IP du client uniquement.

Les trois options utilisent la même configuration pour la relation d'approbation entre l'ASA et les clients Diameter.

Remarque Le proxy TLS utilise TLSv1.0 - 1.2. Vous pouvez configurer la version TLS et la suite de chiffrement.

Les rubriques suivantes expliquent comment configurer le proxy TLS pour l'inspection Diameter.

Configurer la relation de confiance du serveur avec les clients Diameter

L'ASA agit en tant que serveur proxy TLS par rapport aux clients Diameter. Pour établir la relation de confiance mutuelle :

- Vous devez importer le certificat de l'autorité de certification (CA) utilisé pour signer le certificat du serveur de l'ASA dans le client Diameter. Il peut s'agir du magasin de certificats de l'autorité de

certification du client ou de tout autre emplacement utilisé par le client. Consultez la documentation du client pour obtenir les détails exacts de l'utilisation des certificats.

- Vous devez importer le certificat d'autorité de certification utilisé pour signer le certificat du client TLS Diameter afin que l'ASA puisse faire confiance au client.

La procédure suivante explique comment importer le certificat d'autorité de certification utilisé pour signer le certificat du client Diameter et importer un certificat d'identité à utiliser pour le serveur proxy TLS ASA. Au lieu d'importer un certificat d'identité, vous pouvez créer un certificat autosigné sur l'ASA. Sinon, vous pouvez importer ces certificats lorsque vous créez le serveur proxy TLS.

Procédure

Étape 1 Importez le certificat d'autorité de certification utilisé pour signer le certificat du client Diameter dans un point de confiance ASA.

Cette étape permet à l'ASA de faire confiance aux clients Diameter.

a) Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Certificate Management (Gestion des certificats)** > **CA Certificates (Certificats d'autorité de certification)**.
b) Cliquez sur **Add** (Ajouter) et saisissez un nom pour le point de confiance. 5917 Par exemple, **diameter-clients**.
c) Ajoutez le certificat.

Vous pouvez importer le certificat à partir d'un fichier, le coller au format PEM ou utiliser SCEP pour l'importer.

d) Cliquez sur **Install Certificate** (Installer le certificat).

Étape 2 Importez le certificat et créez un point de confiance pour le certificat d'identité et la paire de clés du serveur proxy ASA.

Cette étape permet aux clients Diameter de faire confiance à l'ASA.

a) Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Certificate Management (Gestion des certificats)** > **Identity Certificates (Certificats d'identité)**.
b) Cliquez sur **Add** (Ajouter) et saisissez un nom pour le point de confiance. 5917 Par exemple, **tls-proxy-server-tp**.
c) Sélectionnez **Import the identity certificate from a file** (Importer le certificat d'identité à partir d'un fichier), saisissez la phrase secrète de déchiffrement et sélectionnez le fichier (au format pkcs12).

Vous pouvez également créer un nouveau certificat.

d) Cliquez sur **Add Certificate** (Ajouter le certificat).

Configurer le proxy TLS complet avec un certificat client statique pour l'inspection Diameter

Si le serveur Diameter peut accepter le même certificat pour tous les clients, vous pouvez configurer un certificat client statique que l'ASA utilisera lors de la communication avec le serveur Diameter.

Avec cette configuration, vous devez établir la relation de confiance mutuelle entre l'ASA et les clients (comme expliqué dans Configurer la relation de confiance du serveur avec les clients Diameter, à la page 387), ainsi que l'ASA et le serveur Diameter. Voici les exigences de confiance de l'ASA et du serveur Diameter.

- Vous devez importer le certificat d'autorité de certification utilisé pour signer le certificat d'identité du serveur Diameter afin que l'ASA puisse valider le certificat d'identité du serveur pendant l'établissement de liaison TLS.
- Vous devez importer le certificat client, un certificat auquel le serveur Diameter fait également confiance. Si le serveur Diameter ne fait pas déjà confiance au certificat, importez le certificat d'autorité de certification utilisé pour le signer sur le serveur. Consultez la documentation du serveur Diameter pour en savoir plus.

Procédure

Étape 1 Sélectionnez **Configuration** > **Firewall** > **Unified Communications** > **TLS Proxy** > **(Configuration Pare-feu Communications unifiées proxy TLS)**.

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Attribuez un nom au proxy TLS, par exemple, **diameter-tls-statique-proxy**. Cliquez sur **Next** (suivant).

Étape 4 Sélectionnez le certificat d'identité du proxy TLS que vous avez ajouté dans Configurer la relation de confiance du serveur avec les clients Diameter, à la page 387. Cliquez sur **Next** (suivant).

Si vous n'avez pas encore créé le certificat d'identité, vous pouvez cliquer sur **Manage** (Gérer) pour l'ajouter. Vous pouvez également installer le certificat CA du client Diameter en cliquant sur **Install TLS Server's Certificate** (Installer le certificat du serveur TLS).

Vous pouvez également définir les algorithmes de sécurité (chiffrements) que le serveur peut utiliser en les déplaçant des algorithmes disponibles vers la liste des algorithmes actifs. Si vous ne spécifiez pas de chiffrement, les chiffrements par défaut du système sont utilisés.

Remarque
À des fins de test, ou si vous êtes certain de pouvoir faire confiance aux clients Diameter, vous pouvez ignorer cette étape et désélectionner l'option **Enable client authentication during TLS Proxy handshake** (Activer l'authentification du client pendant l'établissement de liaison du proxy TLS) dans la configuration du proxy TLS.

Étape 5 Sélectionnez **Specify the proxy certificate for TLS client** (Spécifier le certificat proxy pour le client TLS) et procédez comme suit :

a) Sélectionnez le certificat pour le client du proxy TLS ASA.

Si vous n'avez pas encore ajouté le certificat, cliquez sur **Manage** (Gérer) et ajoutez-le maintenant.

b) Si vous n'avez pas encore ajouté le certificat d'autorité de certification qui a été utilisé pour signer le certificat du serveur Diameter, cliquez sur **Install TLS Client's Certificate** (Installer le certificat du client TLS) et ajoutez-le.

c) (Facultatif) Définissez les algorithmes de sécurité (chiffrements) que le client peut utiliser en les déplaçant des algorithmes disponibles vers la liste des algorithmes actifs.

Si vous ne définissez pas les chiffrements que le proxy TLS peut utiliser, le proxy utilise la suite de chiffrement globale définie par les paramètres de chiffrement **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSL Settings (Paramètres SSL)**. Par défaut, le

niveau de chiffrement global est moyen, ce qui signifie que tous les chiffrements sont disponibles, à l'exception de NULL-SHA, DES-CBC-SHA et RC4-MD5. Précisez les chiffrements spécifiques au proxy TLS uniquement si vous souhaitez utiliser une suite différente de celle généralement disponible sur l'ASA.

d) Cliquez sur **Next** (suivant).

Étape 6 Cliquez sur **Finish** (Terminer), puis cliquez sur **Apply** (Appliquer).

Prochaine étape

Vous pouvez maintenant utiliser le proxy TLS dans l'inspection Diameter. Consultez Configurer la politique de service d'inspection de réseau mobile , à la page 397.

Configurer le proxy TLS complet avec des certificats dynamiques locaux pour l'inspection Diameter

Si le serveur Diameter a besoin de certificats uniques pour chaque client, vous pouvez configurer l'ASA pour générer des certificats dynamiques locaux (LDC). Ces certificats existent pour la durée de la connexion du client et sont ensuite supprimés.

Avec cette configuration, vous devez établir la relation de confiance mutuelle entre l'ASA et les clients (comme expliqué dans la section Configurer la relation de confiance du serveur avec les clients Diameter, à la page 387), ainsi que l'ASA et le serveur Diameter. La configuration est similaire à celle décrite dans Configurer le proxy TLS complet avec un certificat client statique pour l'inspection Diameter, à la page 388, sauf qu'au lieu d'importer un certificat client Diameter, vous configurez le LDC sur l'ASA. Voici les exigences de confiance de l'ASA et du serveur Diameter.

- Vous devez importer le certificat d'autorité de certification utilisé pour signer le certificat d'identité du serveur Diameter afin que l'ASA puisse valider le certificat d'identité du serveur pendant l'établissement de liaison TLS.
- Vous devez créer le point de confiance LDC. Vous devez exporter le certificat d'autorité de certification du serveur LDC et l'importer dans le serveur Diameter. L'étape d'exportation est expliquée ci-dessous. Consultez la documentation du serveur Diameter pour obtenir des renseignements sur l'importation des certificats.

Procédure

Étape 1 Sélectionnez **Configuration** > **Firewall** > **Unified Communications** > **TLS Proxy** > **(Configuration Pare-feu Communications unifiées proxy TLS)**.

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Attribuez un nom au proxy TLS, par exemple, **diameter-tls-ldc-proxy**.

Étape 4 Sélectionnez le certificat d'identité du proxy TLS que vous avez ajouté dans Configurer la relation de confiance du serveur avec les clients Diameter, à la page 387. Cliquez sur **Next** (suivant).

Si vous n'avez pas encore créé le certificat d'identité, vous pouvez cliquer sur **Manage** (Gérer) pour l'ajouter. Vous pouvez également installer le certificat CA du client Diameter en cliquant sur **Install TLS Server's Certificate** (Installer le certificat du serveur TLS).

Vous pouvez également définir les algorithmes de sécurité (chiffrements) que le serveur peut utiliser en les déplaçant des algorithmes disponibles vers la liste des algorithmes actifs. Si vous ne spécifiez pas de chiffrement, les chiffrements par défaut du système sont utilisés.

Remarque
À des fins de test, ou si vous êtes certain de pouvoir faire confiance aux clients Diameter, vous pouvez ignorer cette étape et désélectionner l'option **Enable client authentication during TLS Proxy handshake** (Activer l'authentification du client pendant l'établissement de liaison du proxy TLS) dans la configuration du proxy TLS.

Étape 5 Sélectionnez **Specify the internal Certificate Authority to sign for local dynamic certificates** (Spécifier l'autorité de certification interne devant signer les certificats dynamiques locaux) et procédez comme suit (ignorez tout texte lié aux téléphones IP).

Cette procédure suppose que vous créiez un nouveau certificat et une clé. Si vous avez déjà créé le certificat et la clé nécessaires, sélectionnez-les et passez à l'étape des algorithmes de sécurité.

a) Pour Local Dynamic Certificate Key Pair (Paire de clés de certificat dynamique local), cliquez sur **New** (Nouveau). (Vous devrez peut-être redimensionner la boîte de dialogue pour voir le bouton.)
b) Créez un certificat RSA à usage général avec un nouveau nom de paire de clés, tel que **ldc-signer-key**. Cliquez sur **Generate Now** (Générer maintenant) pour créer la clé.

   Vous êtes renvoyé à la boîte de dialogue Gérer les certificats d'identité.

c) Sélectionnez **Certificate** (Certificat) et cliquez sur **Manage** (Gérer) pour créer le certificat et la clé pour le client du proxy TLS ASA.
d) Cliquez sur **Add** (Ajouter) dans la boîte de dialogue Gérer les certificats d'identité.
e) Attribuez un nom au point de confiance, tel que **ldc-server**.
f) Sélectionnez **Ajouter un nouveau certificat d'identité**.
g) Pour **Key Pair** (Paire de clés), sélectionnez la même clé que vous avez créée pour la clé de certificat dynamique locale.
h) Pour **Certificate Subnet DN** (DN du sous-réseau du certificat), sélectionnez les attributs de nom distinctif dont vous avez besoin.

   Le nom usuel du périphérique est le nom par défaut. Vérifiez si l'application Diameter a des exigences spécifiques pour le nom du sujet.

i) Sélectionnez **Generate self-signed certificate** (Générer un certificat autosigné). Cette opération est obligatoire.
j) Sélectionnez **Act as a local certificate authority and issue dynamic certificates to TLS Proxy** (Agir en tant qu'autorité de certification locale et émettre des certificats dynamiques vers le proxy TLS). Cette option fait de ce certificat un émetteur LDC.
k) Cliquez sur **Add Certificate** (Ajouter le certificat).

   Vous êtes renvoyé à la boîte de dialogue Gérer les certificats d'identité.

l) Sélectionnez le certificat que vous venez de créer et cliquez sur **Export** (Exporter).

   Vous devez exporter le certificat pour pouvoir l'importer dans le serveur Diameter. Précisez un nom de fichier et un format PEM, puis cliquez sur **Export Certificate** (Exporter le certificat).

   Vous êtes renvoyé à la boîte de dialogue Gérer les certificats d'identité.

m) Avec le certificat toujours sélectionné, cliquez sur **OK**.

Vous êtes renvoyé à l'assistant de proxy TLS. Si le certificat n'est pas sélectionné dans le champ Certificate (Certificat), sélectionnez-le maintenant.

n) (Facultatif) Définissez les algorithmes de sécurité (chiffrements) que le client peut utiliser en les déplaçant des algorithmes disponibles vers la liste des algorithmes actifs.

Si vous ne définissez pas les chiffrements que le proxy TLS peut utiliser, le proxy utilise la suite de chiffrement globale définie par les paramètres de chiffrement **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSL Settings (Paramètres SSL)**. Par défaut, le niveau de chiffrement global est moyen, ce qui signifie que tous les chiffrements sont disponibles, à l'exception de NULL-SHA, DES-CBC-SHA et RC4-MD5. Précisez les chiffrements spécifiques au proxy TLS uniquement si vous souhaitez utiliser une suite différente de celle généralement disponible sur l'ASA.

o) Cliquez sur **Next** (suivant).

Étape 6 Cliquez sur **Finish** (Terminer), puis cliquez sur **Apply** (Appliquer).

Étape 7 Vous pouvez maintenant importer le certificat de l'autorité de certification LDC dans le serveur Diameter. Consultez la documentation du serveur Diameter pour connaître la procédure. Notez que les données sont au format Base64. Si votre serveur exige le format binaire ou DER, vous devrez utiliser les outils OpenSSL pour convertir les formats.

Prochaine étape

Vous pouvez maintenant utiliser le proxy TLS dans l'inspection Diameter. Consultez Configurer la politique de service d'inspection de réseau mobile , à la page 397.

Configurer le serveur mandataire TLS avec déchargement TLS pour l'inspection Diameter

Si vous êtes certain que le chemin réseau entre l'appareil de sécurité adaptable Cisco et le serveur Diameter est sécurisé, vous pouvez éviter le coût de performance du chiffrement des données entre l'appareil de sécurité adaptable Cisco et le serveur. Avec le déchargement TLS, le serveur proxy TLS chiffre/déchiffre les sessions entre le client Diameter et l'ASA, mais utilise du texte en clair avec le serveur Diameter.

Avec cette configuration, vous devez établir la relation d'approbation mutuelle entre l'appareil de sécurité adaptable Cisco et les clients uniquement, ce qui simplifie la configuration. Avant d'effectuer la procédure suivante, effectuez les étapes dans Configurer la relation de confiance du serveur avec les clients Diameter, à la page 387.

Procédure

Étape 1 Sélectionnez **Configuration** > **Firewall** > **Unified Communications** > **TLS Proxy** > **(Configuration** > **Pare-feu** > **Communications unifiées** > **Serveur proxy TLS)**.

Étape 2 Cliquez sur **Add** (ajouter).

Étape 3 Attribuez un nom au serveur proxy TLS, par exemple, **Diameter-tls-offload-proxy**.

Étape 4 Sélectionnez le certificat d'identité du serveur proxy TLS que vous avez ajouté dans Configurer la relation de confiance du serveur avec les clients Diameter, à la page 387. Cliquez sur **Next** (suivant).

Si vous n'avez pas encore créé le certificat d'identité, vous pouvez cliquer sur **Manage** (Gérer) pour l'ajouter. Vous pouvez également installer le certificat CA du client Diameter en cliquant sur **Install TLS Server's Certificate** (Installer le certificat du serveur TLS).

Vous pouvez également définir les algorithmes de sécurité (chiffrements) que le serveur peut utiliser en les déplaçant des algorithmes disponibles vers la liste des algorithmes actifs. Si vous ne spécifiez pas de chiffrement, les chiffrements par défaut du système sont utilisés.

Remarque
À des fins de test, ou si vous êtes certain de pouvoir faire confiance aux clients Diameter, vous pouvez ignorer cette étape et désélectionner l'option **Enable client authentication during TLS Proxy handshake** (Activer l'authentification du client pendant l'établissement de liaison du serveur proxy TLS) dans la configuration du serveur proxy TLS.

Étape 5 Sélectionnez **Configure the proxy client to use clear text to communicate with the remote TCP client** (Configurer le client du serveur proxy afin qu'il utilise du texte en clair pour communiquer avec le client TCP distant), puis cliquez sur **Next** (Suivant).

Étape 6 Cliquez sur **Finish** (Terminer), puis **Apply** (Appliquer).

Étape 7 Comme les ports Diameter sont différents pour TCP et TLS, configurez une règle NAT pour traduire le port TCP en port TLS pour le trafic passant du serveur Diameter vers le client.

Créez une règle NAT d'objet pour chaque serveur Diameter.

a) Choisissez **Configuration** > **Firewall** > **NAT** > **(Configuration** > **Pare-feu** > **NAT)**.
b) Cliquez sur **Add** > **Object NAT Rule** > **(Ajouter Règle NAT d'objet)**.
c) Configurez les propriétés de base :

- **Name** (Nom) : nom de l'objet, par exemple DiameterServerA.
- **Type** (pour l'objet : sélectionnez **Host** (Hôte).
- **IP Version** (Version IP) : IPv4 ou IPv6, selon le cas.
- **IP Address** (Adresse IP) : l'adresse IP du serveur Diameter, par exemple, 10.100.10.10.
- **Add Automatic Address Translation** (Ajouter une traduction automatique d'adresses) : assurez-vous de sélectionner cette option.
- **Type** (pour la règle NAT) : sélectionnez **Static** (Statique).
- **ranslated Addr** (Adresse traduite) : l'adresse IP du serveur Diameter. Il s'agirait de la même adresse IP de l'objet, par exemple, 10.100.10.10.

d) Cliquez sur **Advanced** (Avancé) et configurez les options **Interface** et **Service** suivantes :

- **Source Interface** (Interface source) : sélectionnez l'interface qui se connecte au serveur Diameter.
- **Destination Interface** (Interface de destination) : sélectionnez l'interface qui se connecte au client Diameter.
- **Protocol** (Protocole) : sélectionnez **TCP**.
- **Real Port** (Port réel) : saisissez 3868, qui est le numéro de port TCP Diameter par défaut.
- **Mapped Port** (Port mappé) : saisissez 5868, qui est le numéro de port TLS Diameter par défaut.

e) Cliquez sur **OK**, puis de nouveau sur **OK** dans la boîte de dialogue Add Network Object (Ajouter un objet réseau).

Prochaine étape

Vous pouvez maintenant utiliser le serveur proxy TLS dans l'inspection Diameter. Consultez Configurer la politique de service d'inspection de réseau mobile , à la page 397.

Configurer une liste des politiques d'inspection M3UA

Utilisez une liste des politiques d'inspection M3UA pour configurer le contrôle d'accès en fonction des codes de point. Vous pouvez également abandonner et limiter le débit des messages par classe et type.

Le format de code de point par défaut est ITU. Si vous utilisez un format différent, précisez le format requis dans la liste des politiques.

Si vous ne souhaitez pas appliquer de politique en fonction du code de point ou de la classe de message, vous n'avez pas besoin de configurer une liste des politiques M3UA. Vous pouvez activer l'inspection sans liste.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **M3UA**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste et cliquez sur **Edit** (Modifier) pour modifier la liste.

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de la modification d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Cliquez sur l'onglet **Parameters** (Paramètres) et configurez les options souhaitées :

- **SS7** : la variante de SS7 utilisée dans votre réseau : ITU, ANSI, Japon, Chine. Cette option détermine le format valide pour les codes de point. Après avoir configuré l'option et déployé une politique M3UA, vous ne pouvez pas la modifier, sauf si vous avez d'abord supprimé la politique. La variante par défaut est ITU.
- **Enable M3UA Application Server Process (ASP) state validation** (Activer la validation de l'état du processus de serveur d'applications [ASP] M3UA) : indique s'il faut effectuer une validation stricte de l'état du processus de serveur d'applications (ASP). Le système conserve les états ASP des sessions M3UA et autorise ou abandonne les messages ASP en fonction du résultat de la validation. Si vous n'activez pas la validation stricte de l'état ASP, tous les messages ASP sont transmis sans inspection. Une vérification stricte de l'état de l'ASP est requise si vous souhaitez un basculement dynamique ou si vous souhaitez effectuer des opérations dans une grappe. Cependant, la vérification stricte de l'état ASP ne fonctionne qu'en mode Override. Elle ne fonctionne pas si vous utilisez le mode Loadsharing ou Broadcast (selon la RFC 4666). L'inspection suppose qu'il y ait un et un seul ASP par terminal.

- **Enforce Timeout Endpoint (** > Appliquer le délai d'expiration du terminal) : délai d'inactivité pour supprimer les statistiques d'un terminal M3UA, au format hh:mm:ss. Pour n'avoir aucun délai d'expiration, spécifiez 0. La valeur par défaut est de 30 minutes (00:30:00).
- **Enforce Timeout** > **Session** (Appliquer le délai d'expiration de la session) : délai d'inactivité pour supprimer une session M3UA si vous activez la validation stricte de l'état ASP, au format hh:mm:ss. Pour n'avoir aucun délai d'expiration, spécifiez 0. La valeur par défaut est de 30 minutes (00:30:00). La désactivation de ce délai d'expiration peut empêcher le système de supprimer les sessions périmées.
- **Message Tag Validation** (Validation de la balise de message) : indique s'il faut vérifier et valider le contenu de certains champs pour le type de message précisé. Les messages qui échouent à la validation sont abandonnés. La validation diffère en fonction du type de message. Sélectionnez les messages que vous souhaitez valider.
  - Destination User Part Unavailable (DUPU) : le champ Utilisateur/Cause doit être présent et ne doit contenir que des codes de cause et d'utilisateur valides.
  - Erreur : tous les champs obligatoires doivent être présents et contenir uniquement des valeurs autorisées. Chaque message d'erreur doit contenir les champs obligatoires pour ce code d'erreur.
  - Notification : les champs Type d'état et Informations sur l'état ne doivent contenir que des valeurs autorisées.

Étape 5 Cliquez sur l'onglet **Inspections** et définissez les inspections spécifiques que vous souhaitez mettre en œuvre en fonction des caractéristiques du trafic.

a) Effectuez l'une des actions suivantes :
   - Cliquez sur **Add** (Ajouter) pour ajouter un nouveau critère.
   - Sélectionnez un critère existant et cliquez sur **Edit** (Modifier).

b) Choisissez le type de correspondance pour les critères : **Match** (le trafic doit correspondre au critère) ou **No Match** (le trafic ne doit pas correspondre au critère). Configurez ensuite le critère :
   - **Class ID** (ID de classe) : correspond à la classe et au type de message M3UA. Le tableau suivant répertorie les valeurs possibles. Consultez les RFC M3UA et la documentation pour obtenir des renseignements détaillés sur ces messages.

Classe de message M3UA	Type de message
0 (messages de gestion)	0-1
1 (messages de transfert)	1
2 (messages de gestion du réseau de signalisation SS7)	1-6
3 (messages de maintenance de l'état ASP)	1-6
4 (messages de maintenance du trafic ASP)	1 à 4
9 (messages de gestion des clés de routage)	1 à 4

- **OPC** : correspond au code de point d'origine, c'est-à-dire à la source du trafic. Le code de point est au format *zone-région-sp*, où les valeurs possibles pour chaque élément dépendent de la variante SS7 :
  - **ITU** : les codes de point sont de 14 bits au format 3-8-3. Les plages de valeurs sont [0-7]-[0-255]-[0-7].
  - **ANSI** : les codes de point sont de 24 bits au format 8-8-8. Les plages de valeurs sont [0-255]-[0-255]-[0-255].
  - **Japan** : les codes de point sont de 16 bits au format 5-4-7. Les plages de valeurs sont [0-31]-[0-15]-[0-127].
  - **China** : les codes de point sont de 24 bits au format 8-8-8. Les plages de valeurs sont [0-255]-[0-255]-[0-255].
- **DPC** : correspond au code du point de destination. Le code de point est au format *zone-région-sp*, comme expliqué pour **OPC**.
- **Service Indicator** (Indicateur de service) : correspond au numéro d'indicateur de service, de 0 à 15. Voici les indicateurs de service disponibles. Consultez les RFC et la documentation de M3UA pour obtenir des renseignements détaillés sur ces indicateurs de service.
  - 0—Messages de gestion du réseau de signalisation
  - 1—Messages de test et de maintenance du réseau de signalisation
  - 2—Messages spéciaux de test et de maintenance du réseau de signalisation
  - 3—SCCP
  - 4—Partie utilisateur téléphonique
  - 5—Partie utilisateur RNIS
  - 6—Partie utilisateur de données (messages liés aux appels et aux circuits)
  - 7—Partie utilisateur de données (messages d'enregistrement et d'annulation des installations)
  - 8—Réservé pour la partie utilisateur de test MTP
  - 9—Partie utilisateur RNIS à large bande
  - 10—Partie utilisateur RNIS par satellite
  - 11—Réservé
  - 12—Signalisation de type AAL 2
  - 13—Contrôle d'appel indépendant du support
  - 14—Protocole de contrôle de passerelle
  - 15—Réservé

c) Pour la correspondance Class ID (ID de classe), choisissez d'abandonner le paquet ou d'appliquer une limite de débit en paquets par seconde. L'action pour toutes les autres correspondances est d'abandonner le paquet. Pour toutes les correspondances, vous pouvez choisir d'activer la journalisation.

d) Cliquez sur **OK** pour ajouter l'inspection. Répétez le processus au besoin.

Étape 6 Cliquez sur **OK** dans la boîte de dialogue M3UA Inspect Map.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection M3UA.

Prochaine étape

Vous pouvez maintenant configurer une politique d'inspection pour utiliser la liste. Consultez Configurer la politique de service d'inspection de réseau mobile , à la page 397.

Configurer la politique de service d'inspection de réseau mobile

Les inspections pour les protocoles utilisés dans les réseaux mobiles ne sont pas activées dans la politique d'inspection par défaut, vous devez donc les activer si vous avez besoin de ces inspections. Vous pouvez simplement modifier la politique d'inspection globale par défaut pour ajouter ces inspections. Vous pouvez également créer une nouvelle politique de service comme vous le souhaitez, par exemple, une politique spécifique à l'interface.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**, et ouvrez une règle.

- Pour modifier la politique globale par défaut, sélectionnez la règle « inspection_default » dans le dossier Global, puis cliquez sur **« Edit »** (Modifier).
- Pour créer une nouvelle règle, cliquez sur **Add (Ajouter)** > **Add** > **Service Policy Rule** > **(Ajouter une règle de politique de service)**. Passez par l'assistant jusqu'à la page Rules (Règles).
- Si vous avez une règle d'inspection de réseau mobile ou une règle à laquelle vous ajoutez ces inspections, sélectionnez-la et cliquez sur **Edit** (Modifier).

Étape 2 Sur la page ou l'onglet de l'assistant Rule Actions (Actions name), sélectionnez l'onglet **Protocol Inspection** (Inspection de protocole).

Étape 3 (Pour modifier une politique en cours d'utilisation.) Si vous modifiez une politique en cours d'utilisation pour utiliser une liste des politiques d'inspection différente, vous devez désactiver les inspections, puis les réactiver avec le nouveau nom de liste des politiques d'inspection :

a) Décochez les cases pertinentes déjà sélectionnées : **GTP**, **SCTP**, **Diameter**, **M3UA**.
b) Cliquez sur **OK**.
c) Cliquez sur **Apply** (Appliquer).
d) Répétez ces étapes pour revenir à l'onglet Protocol Inspections (Inspections de protocole).

Étape 4 Sélectionnez les protocoles de réseau mobile souhaités : **GTP**, **SCTP**, **Diameter**, **M3UA**.

Étape 5 Si vous souhaitez une inspection autre que celle par défaut pour un ou plusieurs de ces protocoles, cliquez sur **Configure** (Configurer) à côté des options et procédez comme suit :

a) Choisissez d'utiliser la liste par défaut ou d'utiliser une liste des politiques d'inspection que vous avez configurée. Vous pouvez créer la liste à ce moment-ci.

b) (Diameter uniquement.) Pour activer l'inspection Diameter des messages chiffrés, sélectionnez **Enable Encrypted Traffic Inspection** (Activer l'inspection du trafic chiffré) et sélectionnez un proxy TLS à utiliser pour le déchiffrement.

Remarque
Si vous spécifiez un proxy TLS pour l'inspection Diameter et que vous appliquez la redirection de port NAT au trafic du serveur Diameter (par exemple, rediriger le trafic du serveur du port 5868 au port 3868), configurez l'inspection globalement ou sur l'interface d'entrée uniquement. Si vous appliquez l'inspection à l'interface de sortie, le trafic Diameter NATisé contourne l'inspection.

c) Cliquez sur **OK** dans la boîte de dialogue Select Inspect Map (Sélectionner une liste d'inspection).

Étape 6 Cliquez sur **OK** ou **Finish** (Terminer) pour enregistrer la règle de politique de service.

Configurer l'inspection de comptabilité RADIUS

L'inspection de comptabilité RADIUS n'est pas activée par défaut. Vous devez le configurer si vous souhaitez effectuer une inspection de la comptabilité RADIUS.

Procédure

Étape 1 Configurer une liste des politiques d'inspection de comptabilité RADIUS, à la page 398.

Étape 2 Configurer la politique de service d'inspection de comptabilité RADIUS, à la page 399.

Configurer une liste des politiques d'inspection de comptabilité RADIUS

Vous devez créer une liste des politiques d'inspection de comptabilité RADIUS) pour configurer les attributs nécessaires à l'inspection.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (listes d'inspection)** > **RADIUS Accounting (Comptabilité RADIUS)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle carte.
- Sélectionnez une liste, puis cliquez sur **Edit** (Modifier).

Étape 3 Pour les nouvelles listes, saisissez un nom (40 caractères maximum) et une description. Lors de l'édition d'une liste, vous pouvez modifier la description uniquement.

Étape 4 Cliquez sur l'onglet **Host Parameters** (paramètres de l'hôte) et ajoutez les adresses IP de chaque serveur RADIUS ou GGSN.

Vous pouvez éventuellement inclure une clé secrète afin que l'ASA puisse valider le message. Sans la clé, seule l'adresse IP est vérifiée. L'ASA reçoit une copie des messages de comptabilité RADIUS de ces hôtes.

Étape 5 Cliquez sur l'onglet **Other Parameters** (autres paramètres) et configurez les options souhaitées.

- **Send responses to the originator of the RADIUS accounting message** (Envoyer des réponses à l'initiateur du message de comptabilité RADIUS) : indique s'il faut envoyer des réponses à l'initiateur du message de comptabilité RADIUS.
- **Enforce user timeout** (Appliquer le délai d'inactivité des utilisateurs) : indique s'il faut mettre en œuvre un délai d'inactivité pour les utilisateurs, ainsi que la valeur de ce délai La valeur par défaut est de 1 heure.
- **Enable detection of GPRS accounting** (Activer la détection de la comptabilité GPRS) : indique s'il faut mettre en œuvre la protection contre la surcharge GPRS. L'ASA vérifie l'attribut 3GPP VSA 26-10415 dans les messages d'arrêt et de déconnexion de la demande de comptabilité afin de gérer correctement les contextes de PDP secondaires. Si cet attribut est présent, l'ASA supprime toutes les connexions dont l'adresse IP source correspond à l'adresse IP de l'utilisateur sur l'interface configurée.
- **Validate Attribute** (Valider l'attribut) : critères supplémentaires à utiliser lors de la création d'un tableau des comptes utilisateur lors de la réception des messages Accounting-Request Start. Ces attributs sont utiles lorsque l'ASA décide s'il faut supprimer les connexions.

  Si vous ne spécifiez pas d'attributs supplémentaires à valider, la décision est basée uniquement sur l'adresse IP dans l'attribut d'adresse IP encapsulée. Si vous configurez des attributs supplémentaires et que l'ASA reçoit un message de comptabilité de démarrage qui comprend une adresse en cours de suivi, mais que les autres attributs à valider sont différents, toutes les connexions commencées à l'aide des anciens attributs sont abandonnées, en supposant que l'adresse IP a été réassignée à un nouvel utilisateur.

  Les valeurs sont comprises entre 1 et 191, et vous pouvez entrer la commande plusieurs fois. Pour obtenir la liste des numéros d'attributs et leurs descriptions, consultez le site http://www.iana.org/assignments/radius-types.

Étape 6 Cliquez sur **OK**.

Vous pouvez maintenant utiliser la liste d'inspection dans une politique de service d'inspection de comptabilité RADIUS.

Configurer la politique de service d'inspection de comptabilité RADIUS

L'inspection de comptabilité RADIUS n'est pas activée dans la politique d'inspection par défaut. Vous devez donc l'activer si vous avez besoin de cette inspection. Comme l'inspection de comptabilité RADIUS s'adresse au trafic dirigé vers l'ASA, vous devez la configurer comme règle d'inspection de gestion plutôt que comme règle standard.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**, et ouvrez une règle.

- Pour créer une nouvelle règle, cliquez sur **Add (Ajouter) > Add Management Service Policy Rule (Ajouter une règle de politique de service de gestion)**. Passez par l'assistant jusqu'à la page Rules (Règles).
- Si vous avez une règle d'inspection de comptabilité RADIUS ou une règle de gestion à laquelle vous ajoutez l'inspection de comptabilité RADIUS, sélectionnez-la, cliquez sur **Edit** (Modifier), puis cliquez sur l'onglet **Rule Actions** (Actions de règle).

Étape 2 (Pour modifier une politique en cours d'utilisation) Si vous modifiez une politique en cours d'utilisation pour utiliser une liste des politiques d'inspection différente, vous devez désactiver l'inspection de comptabilité RADIUS, puis la réactiver avec le nouveau nom de liste des politiques d'inspection :

a) Sélectionnez **None** (Aucun) pour la liste de comptabilité RADIUS.
b) Cliquez sur **OK**.
c) Cliquez sur **Apply** (Appliquer).
d) Répétez ces étapes pour revenir à l'onglet Protocol Inspections (Inspections de protocole).

Étape 3 Choisissez la liste **RADIUS Accounting** (Comptabilité RADIUS) souhaitée. Vous pouvez créer la liste à ce moment-ci. Pour de plus amples renseignements, voir Configurer une liste des politiques d'inspection de comptabilité RADIUS, à la page 398.

Étape 4 Cliquez sur **OK** ou **Finish** (Terminer) pour enregistrer la règle de politique de service.

Surveillance de l'inspection du réseau mobile

Les rubriques suivantes expliquent comment surveiller l'inspection du réseau mobile.

Surveillance de l'inspection GTP

Pour afficher la configuration GTP, saisissez la commande **show service-policy inspect gtp** en mode d'exécution privilégié. Sélectionnez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**pour entrer ces commandes.

Utilisez la commande **show service-policy inspect gtp statistics** pour afficher les statistiques de l'inspection GTP. Voici un exemple de sortie :

```
firewall(config)# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support               0     msg_too_short             0
  unknown_msg                       0     unexpected_sig_msg        0
  unexpected_data_msg               0     ie_duplicated             0
  mandatory_ie_missing              0     mandatory_ie_incorrect    0
  optional_ie_incorrect             0     ie_unknown                0
  ie_out_of_order                   0     ie_unexpected             0
  total_forwarded                  67     total_dropped             1
  signalling_msg_dropped            1     data_msg_dropped          0
  signalling_msg_forwarded         67     data_msg_forwarded        0
  total created_pdp                33     total deleted_pdp         32
  total created_pdpmcb             31     total deleted_pdpmcb      30
  total dup_sig_mcbinfo             0     total dup_data_mcbinfo    0
  no_new_sgw_sig_mcbinfo            0     no_new_sgw_data_mcbinfo   0
  pdp_non_existent                  1
```

Vous pouvez obtenir des statistiques pour un terminal GTP spécifique en saisissant l'adresse IP dans la commande **show service-policy inspect gtp statistics** *ip_address*.

```
firewall(config)# show service-policy inspect gtp statistics 10.9.9.9
1 in use, 1 most used, timeout 0:30:00
 GTP GSN Statistics for 10.9.9.9, Idle 0:00:34, restart counter 0
  Tunnels Active                    0
  Tunnels Created                   1
  Tunnels Destroyed                 0
  Total Messages Received           1
                         Signalling Messages        Data Messages
  total received                   1                          0
  dropped                          0                          0
  forwarded                        1                          0
```

Utilisez la commande **show service-policy inspect gtp pdp-context** pour afficher les informations liées au contexte PDP. Pour GTPv2, il s'agit du contexte de support. Par exemple :

```
ciscoasa(config)# show service-policy inspect gtp pdp-context
4 in use, 5 most used

Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:52:01,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517056,  MS Addr 100.100.100.102,
SGW Addr 10.0.203.24,      Idle 0:00:05,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517057,  MS Addr 100.100.100.103,
SGW Addr 10.0.203.25,      Idle 0:00:04,   Timeout 3:00:00,   APN ssenoauth146

Version v2,   TID 0505420121517055,  MS Addr 100.100.100.101,
SGW Addr 10.0.203.23,      Idle 0:00:06,   Timeout 3:00:00,   APN ssenoauth146

ciscoasa(config)# show service-policy inspect gtp pdp-context detail
1 in use, 1 most used

Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:06:14,   Timeout 3:00:00,   APN ssenoauth146

    user_name (IMSI):  50502410121507    MS address: 2005:a00::250:56ff:fe96:eec
    nsapi: 5                linked nsapi: 5
    primary pdp: Y         sgsn is Remote
    sgsn_addr_signal: 10.0.203.22    sgsn_addr_data: 10.0.203.22
    ggsn_addr_signal: 10.0.202.22    ggsn_addr_data: 10.0.202.22
    sgsn control teid:     0x00000001    sgsn data teid:        0x000003e8
    ggsn control teid:     0x000f4240    ggsn data teid:        0x001e8480
    signal_sequence:               18     state:    Ready
...
```

Le contexte de PDP ou de support est identifié par l'ID de tunnel (TID), qui est une combinaison des valeurs d'IMSI et de NSAPI (GTPv0-1) ou d'IMSI et d'EBI (GTPv2). Un tunnel GTP est défini par deux contextes associés dans différents nœuds GSN ou SGW/PGW et est identifié par un ID de tunnel. Un tunnel GTP est nécessaire pour transférer les paquets entre un réseau de données de paquets externe et un utilisateur d'abonné mobile (MS).

Surveillance SCTP

Vous pouvez utiliser les commandes suivantes pour surveiller SCTP. Sélectionnez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**pour entrer ces commandes.

- **show service-policy inspect sctp**

  Affiche les statistiques d'inspection SCTP. Le compteur sctp-drop-override s'incrémente chaque fois qu'un PPID correspond à une action d'abandon, mais le paquet n'a pas été abandonné car il contenait des fragments de données avec des PPID différents. Par exemple :

```
ciscoasa# show service-policy inspect sctp
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: sctp sctp, packet 153302, lock fail 0, drop 20665, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0, sctp-drop-override 4910
        Match ppid 30 35
          rate-limit 1000 kbps, chunk 2354, dropped 10, bytes 21408, dropped-bytes 958

        Match: ppid 40
           drop, chunk 5849
        Match: ppid 55
           log, chunk 9546
```

- **show sctp** [**detail**]

  Affiche les témoins et les associations SCTP actuels. Ajoutez le mot-clé **detail** pour voir des informations détaillées sur les associations SCTP. La vue détaillée affiche également des informations sur le multi-homing, les flux multiples et le réassemblage de fragments.

```
ciscoasa# show sctp

AssocID: 71adeb15
Local:  192.168.107.12/50001 (ESTABLISHED)
Remote: 192.168.108.122/2905 (ESTABLISHED)
Secondary Conn List:
    192.168.108.12(192.168.108.12):2905 to 192.168.107.122(192.168.107.122):50001
    192.168.107.122(192.168.107.122):50001 to 192.168.108.12(192.168.108.12):2905
    192.168.108.122(192.168.108.122):2905 to 192.168.107.122(192.168.107.122):50001
    192.168.107.122(192.168.107.122):50001 to 192.168.108.122(192.168.108.122):2905
    192.168.108.12(192.168.108.12):2905 to 192.168.107.12(192.168.107.12):50001
    192.168.107.12(192.168.107.12):50001 to 192.168.108.12(192.168.108.12):2905
```

- **show conn protocol sctp**

  Affiche des renseignements sur les connexions SCTP actuelles.

- **show local-host** [**connection sctp** *start*[*-end*]]

  Affiche les informations sur les hôtes qui effectuent des connexions SCTP par l'intermédiaire de l'ASA, par interface. Ajoutez le mot-clé **connection sctp** pour voir uniquement les hôtes avec le nombre ou la plage spécifié de connexions SCTP.

- **show traffic**

  Affiche les statistiques de connexion SCTP et d'inspection par interface si vous activez la commande **sysopt traffic detailed-statistics**.

Surveillance de Diameter

Vous pouvez utiliser les commandes suivantes pour surveiller Diameter. Sélectionnez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**pour entrer ces commandes.

- **show service-policy inspect diameter**

  Affiche les statistiques d'inspection de Diameter. Par exemple :

```
ciscoasa# show service-policy inspect diameter
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: Diameter Diameter_map, packet 0, lock fail 0, drop 0, -drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0
        Class-map: log_app
            Log: 5849
         Class-map: block_ip
             drop-connection: 2
```

- **show diameter**

  Affiche les informations d'état pour chaque connexion Diameter. Par exemple :

```
ciscoasa# show diameter
Total active diameter sessions: 5
Session 3638
       ==========
       ref_count: 1 val = .; 1096298391; 2461;
           Protocol : diameter Context id : 0
           From inside:211.1.1.10/45169 to outside:212.1.1.10/3868
...
```

- **show conn detail**

  Affiche les informations de connexion. Les connexions Diameter sont marquées avec l'indicateur Q.

- **show tls-proxy**

  Affiche les informations sur le proxy TLS si vous en utilisez un dans l'inspection Diameter.

Surveillance M3UA

Vous pouvez utiliser les commandes suivantes pour surveiller M3UA. Sélectionnez **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**pour entrer ces commandes.

- **show service-policy inspect m3ua drops**

  Affiche les statistiques de rejet pour l'inspection M3UA.

- **show service-policy inspect m3ua endpoint** [*IP_address*]

  Affiche les statistiques pour les terminaux M3UA. Vous pouvez spécifier une adresse IP de terminal pour afficher les informations sur un terminal spécifique. Pour les systèmes à haute disponibilité ou en grappe, les statistiques sont fournies par unité et ne sont pas synchronisées entre les unités. Par exemple :

```
ciscoasa# sh service-policy inspect m3ua endpoint
```

```
M3UA Endpoint Statistics for 10.0.0.100, Idle : 0:00:06 :
                  Forwarded        Dropped          Total Received
All Messages      21                5                 26
DATA Messages     9                 5                 14
M3UA Endpoint Statistics for 10.0.0.110, Idle : 0:00:06 :
                  Forwarded        Dropped          Total Received
All Messages      21                8                 29
DATA Messages     9                 8                 17
```

- **show service-policy inspect m3ua session**

  Affiche les informations sur les sessions M3UA si vous activez la validation stricte de l'état du processus de serveur d'applications (ASP). Les informations comprennent l'ID d'association source, si la session est en échange unique ou double, et dans la mise en grappe, s'il s'agit d'une session de propriétaire de grappe ou d'une session de sauvegarde. Dans une grappe de 3 unités ou plus, vous pouvez voir des sessions de sauvegarde périmées si une unité quitte puis revient à la grappe. Ces sessions périmées sont supprimées lorsqu'elles expirent, sauf si vous avez désactivé le délai d'expiration de session.

```
Ciscoasa# show service-policy inspect m3ua session
0 in use, 0 most used
Flags: o - cluster owner session, b - cluster backup session
       d - double exchange      , s - single exchange
AssocID: cfc59fbe in Down state, idle:0:00:05, timeout:0:01:00, bd
AssocID: dac2e123 in Active state, idle:0:00:18, timeout:0:01:00, os
```

- **show service-policy inspect m3ua table**

  Affiche la table d'inspection M3UA en cours d'exécution, y compris les règles de classification.

- **show conn detail**

  Affiche les informations de connexion. Les connexions M3UA sont marquées du drapeau v.

Historique de l'inspection du réseau mobile

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Inspection GTPv2 et améliorations de l'inspection GTPv0/1	9.5(1)	L'inspection GTP peut désormais gérer GTPv2. En outre, l'inspection GTP pour toutes les versions prend désormais en charge les adresses IPv6. Nous avons modifié la boîte de dialogue **GTP Inspect Map (Liste d'inspection GTP)** > **Inspections** pour vous permettre de configurer la mise en correspondance d'ID de message distincts pour GTPv1 et GTPv2. Dans l'onglet **General Parameters** (Paramètres généraux), le délai d'expiration du **GSN** est maintenant le délai d'expiration du **terminal**.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Inspection SCTP	9.5(2)	Vous pouvez maintenant appliquer l'inspection de couche d'application au trafic du protocole SCTP (Stream Control Transmission Protocol) pour appliquer des actions en fonction de l'identifiant de protocole de charge utile (PPID). Nous avons ajouté ou modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Listes d'inspection)** > **SCTP** ; onglet **Rule Actions (Actions de règle)** > **Protocol Inspection (Inspection de protocole)** de l'assistant d'ajout/de modification **Configuration** > **Firewall (Pare-feu)** > **Service Policy (Politique de service)** .
Inspection Diameter	9.5(2)	Vous pouvez désormais appliquer l'inspection de couche d'application au trafic Diameter et appliquer des actions en fonction de l'ID d'application, du code de commande et du filtrage de paire attribut-valeur (AVP). Nous avons ajouté ou modifié les écrans suivants : **Configuration** > **Firewall** > **(Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Listes d'inspection)** > **Diameter** et **Diameter AVP (AVP Diameter)** ; onglet **Rule Actions (Actions de règle)** > **Protocol Inspection (Inspection de protocole)** de l'assistant d'ajout/de modification **Configuration** > **Firewall (Pare-feu)** > **Service Policy (Politique de service)** .
Améliorations de l'inspection Diameter	9.6(1)	Vous pouvez désormais inspecter Diameter sur le trafic TCP/TLS, appliquer une vérification stricte de la conformité du protocole et inspecter Diameter sur SCTP en mode grappe. Nous avons ajouté ou modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Listes d'inspection)** > **Diameter** ; onglet **Rule Actions (Actions de règle)** > **Protocol Inspection (Inspection du protocole)** de l'assistant d'ajout/de modification **Configuration** > **Firewall (Pare-feu)** > **Service Policy (Politique de service)** .
Inspection avec état SCTP en mode grappe	9.6(1)	L'inspection dynamique de paquets SCTP fonctionne désormais en mode grappe. Vous pouvez également configurer le contournement d'inspection dynamique de SCTP en mode grappe. Nous n'avons pas ajouté ni modifié d'écrans.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Inspection de l'adaptation de l'utilisateur MTP3 (M3UA)	9.6(2)	Vous pouvez désormais inspecter le trafic M3UA et appliquer des actions en fonction du code de point, de l'indicateur de service, ainsi que de la classe et du type de message. Nous avons ajouté ou modifié les pages suivantes : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspection Maps (Cartes d'inspection)** > **M3UA**; l'onglet **Rule Action (Action de règle)** > **Protocol Inspection (Inspection de protocole)** pour les règles de politique de service
Prise en charge de la réorganisation, du réassemblage et de la fragmentation des flux multiples SCTP. Prise en charge du multi-hébergement SCTP, où les terminaux SCTP ont plusieurs adresses IP.	9.7(1)	Le système prend désormais entièrement en charge la réorganisation, le réassemblage et la fragmentation des flux multiples SCTP, ce qui améliore l'efficacité des inspections Diameter et M3UA pour le trafic SCTP. Le système prend également en charge le multi-hébergement SCTP, où les terminaux ont plusieurs adresses IP chacun. Pour le multi-hébergement, le système ouvre des passages pour les adresses secondaires afin que vous n'ayez pas besoin d'écrire des critères d'accès pour les autoriser. Les terminaux SCTP doivent être limités à 3 adresses IP chacun. Nous n'avons pas modifié d'écrans ASDM.
Améliorations de l'inspection M3UA.	9.7(1)	L'inspection M3UA prend désormais en charge le basculement dynamique, la mise en grappe semi-distribuée et la connexion à plusieurs réseaux. Vous pouvez également configurer la validation stricte de l'état du processus du serveur d'application (ASP) et la validation de divers messages. Une validation stricte de l'état ASP est requise pour le basculement dynamique et la mise en grappe. Nous avons modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspection Maps (Cartes d'inspection)** > **M3UA** Boîtes de dialogue Add/Edit (Ajouter/modifier).
Prise en charge de la définition de la suite de chiffrement SSL du proxy TLS.	9.8(1)	Vous pouvez maintenant définir la suite de chiffrement SSL lorsque l'ASA agit en tant que serveur mandataire TLS. Auparavant, vous ne pouviez définir que les paramètres globaux pour l'ASA sur la page **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **SSL Settings (Paramètres SSL)** > **Encryption (Chiffrement)** . Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Unified Communications (Communications unifiées)** > **TLS Proxy (Mandataire TLS)**, boîtes de dialogue Add/Edit (Ajouter/modifier), page **Server Configuration** (Configuration du serveur).

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Améliorations de l'inspection GTP pour le filtrage des MSISDN et du mode de sélection, les attaques par rejeu et la protection contre l'usurpation d'adresse de l'utilisateur	9.10(1)	Vous pouvez maintenant configurer l'inspection GTP pour abandonner les messages de création d'un contexte PDP en fonction du numéro de répertoire international de l'abonné de la station mobile (MSISDN) ou du mode de sélection. Vous pouvez également mettre en œuvre une protection contre l'anti-relecture et l'usurpation d'adresse de l'utilisateur. Boîte de dialogue **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspection Maps (Cartes d'inspection)** > **GTP** > **Add/Edit (Ajouter/Modifier)**
Prise en charge de GTPv1 version 10.12.	9.12(1)	Le système prend désormais en charge GTPv1 version 10.12. Auparavant, le système prenait en charge la version 6.1. La nouvelle prise en charge comprend la reconnaissance de 25 messages GTPv1 supplémentaires et de 66 éléments d'information. De plus, il y a un changement de comportement. Désormais, tous les ID de message inconnus sont autorisés. Auparavant, les messages inconnus étaient abandonnés et enregistrés. Nous n'avons pas ajouté ni modifié d'écrans.
Journalisation de la localisation pour les stations mobiles (inspection GTP).	9.13(1)	Vous pouvez configurer l'inspection GTP pour enregistrer l'emplacement initial d'une station mobile et les modifications ultérieures de cet emplacement. Le suivi des modifications d'emplacement peut vous aider à identifier les frais d'itinérance potentiellement frauduleux. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **Inspect Maps (Cartes d'inspection)** > **GTP**
Prise en charge de GTPv2 et GTPv1 version 15.	9.13(1)	Le système prend désormais en charge GTPv2 3GPP 29.274 V15.5.0. Pour GTPv1, la prise en charge va jusqu'à 3GPP 29.060 V15.2.0. La nouvelle prise en charge comprend la reconnaissance de 2 messages supplémentaires et de 53 éléments d'information. Nous n'avons pas modifié d'écrans.
Possibilité de spécifier les préfixes IMSI à abandonner lors de l'inspection GTP.	9.16(1)	L'inspection GTP vous permet de configurer le filtrage de préfixes IMSI, pour identifier les combinaisons code de pays mobile/code de réseau mobile (MCC/MNC) à autoriser. Vous pouvez maintenant effectuer le filtrage IMSI sur les combinaisons MCC/MNC que vous souhaitez abandonner. De cette façon, vous pouvez répertorier les combinaisons indésirables et autoriser toutes les autres combinaisons par défaut. Nous avons modifié les écrans suivants : l'option Drop (Abandon) a été ajoutée à l'onglet IMSI Prefix Filtering (Filtrage des préfixes IMSI) pour les cartes d'inspection GTP.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de Secure Firewall 3100 pour la licence d'opérateur	9.18(1)	La licence d'opérateur permet l'inspection des protocoles Diameter, GTP/GPRS et SCTP. Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **Licensing (Licences)** > **Smart Licensing (Licences Smart)** .



PARTIE V

Gestion des connexions et détection des menaces

- Paramètres de connexion, à la page 411
- Qualité de service, à la page 441
- Détection des menaces, à la page 451



CHAPITRE 16

Paramètres de connexion

Ce chapitre décrit comment configurer les paramètres de connexion pour les connexions qui passent par l'ASA ou pour les connexions de gestion, qui vont à l'ASA.

- Que sont les paramètres de connexion ?, à la page 411
- Configurer les paramètres de connexion, à la page 412
- Supervision des connexions, à la page 434
- Historique des paramètres de connexion, à la page 435

Que sont les paramètres de connexion ?

Les paramètres de connexion comprennent une variété de fonctionnalités liées à la gestion des connexions de trafic, telles qu'un flux TCP dans ASA. Certaines fonctionnalités sont des composants nommés que vous configurez pour fournir des services spécifiques.

Les paramètres de connexion sont les suivants :

- **Délais d'expiration globaux pour divers protocoles** : Tous les délais d'expiration globaux ont des valeurs par défaut, vous devez donc les modifier uniquement si vous subissez une perte de connexion prématurée.
- **Délai d'expiration de la connexion par classe de trafic** : vous pouvez remplacer les délais d'expiration globaux pour des types de trafic spécifiques à l'aide des politiques de service. Tous les délais d'expiration de classes de trafic ont des valeurs par défaut, vous n'avez donc pas besoin de les définir.
- **Limites de connexion et interception TCP** : par défaut, il n'y a aucune limite au nombre de connexions pouvant passer par (ou vers) l'ASA. Vous pouvez définir des limites pour des classes de trafic particulières en utilisant des règles de politique de service pour protéger les serveurs contre les attaques par déni de service (DoS). En particulier, vous pouvez définir des limites sur les connexions amorces (celles qui n'ont pas terminé la prise de contact TCP), ce qui protège contre les attaques par inondation SYN. Lorsque les limites amorces sont dépassées, le composant TCP Intercept intervient pour les connexions mandataires et s'assure que les attaques sont limitées.
- **Détection des connexions mortes (DCD)** : si vous avez des connexions persistantes qui sont valides, mais souvent inactives, de sorte qu'elles sont fermées parce qu'elles dépassent les paramètres de délai d'inactivité, vous pouvez activer la détection des connexions mortes pour identifier les connexions inactives, mais valides, et les maintenir actives (en réinitialisant leurs temporisateurs d'inactivité). Chaque fois que les durées d'inactivité sont dépassées, la DCD sonde les deux côtés de la connexion pour voir si les deux côtés s'entendent pour dire que la connexion est valide. La sortie de la commande **show**

service-policy comprend des compteurs pour afficher le volume d'activité du DCD. Vous pouvez utiliser la commande **show conn detail** pour obtenir des renseignements sur l'initiateur et le répondeur, et indiquer la fréquence à laquelle chacun a envoyé des sondes.

- **Randomisation de la séquence TCP** : chaque connexion TCP possède deux numéros de séquence initial (ISN) : un généré par le client et l'autre par le serveur. Par défaut, ASA rend aléatoire l'ISN du SYN TCP passant à la fois dans les sens entrant et sortant. La gestion aléatoire empêche un agresseur de prédire le prochain ISN pour une nouvelle connexion et de détourner potentiellement la nouvelle session. Cependant, la répartition aléatoire des séquences TCP rompt en pratique les SACK TCP (accusé de réception sélectif), car les numéros de séquence que voit le client sont différents de ce que le serveur voit. Vous pouvez désactiver la répartition aléatoire par classe de trafic si vous le souhaitez.
- **Normalisation TCP** : le normaliseur TCP offre une protection contre les paquets anormaux. Vous pouvez configurer le traitement de certains types d'anomalies de paquets par classe de trafic.
- **Contournement d'état TCP** : vous pouvez contourner la vérification de l'état TCP si vous utilisez le routage dissymétrique dans votre réseau.
- **Contournement d'état SCTP** : vous pouvez contourner l'inspection avec état du protocole SCTP (Stream Control Transmission Protocol) si vous ne souhaitez pas de validation du protocole SCTP.
- **Décharge de flux** : vous pouvez identifier le trafic à décharger vers un chemin super rapide, où les flux sont commutés dans la carte réseau elle-même. Le déchargement peut vous aider à améliorer les performances des applications exigeantes en données, telles que les transferts de fichiers volumineux.
- **Décharge de flux IPsec** : après la configuration initiale d'une association de sécurité (SA) IPsec de site à site ou d'accès à distance, les connexions IPsec sont déchargées vers le réseau portail programmable sur site (FPGA) dans le périphérique, ce qui devrait améliorer les performances du périphérique . Cette fonctionnalité est activée par défaut sur les plateformes qui la prennent en charge.

Configurer les paramètres de connexion

Les limites de connexion, les délais d'expiration, la normalisation TCP, l'aléatorisation de séquence TCP et le décrément de la durée de vie (TTL) ont des valeurs par défaut qui sont appropriées à la plupart des réseaux. Vous ne devez configurer ces paramètres de connexion que si vous avez des exigences hors du commun, si votre réseau dispose de types de configuration spécifiques ou si vous subissez des pertes de connexion anormales en raison d'un délai d'inactivité prématuré.

Les autres fonctionnalités liées à la connexion ne sont pas activées. Vous configurez ces services sur des classes de trafic spécifiques uniquement, et non en tant que service général. Ces fonctionnalités comprennent les éléments suivants : interception TCP, contournement de l'état TCP, détection de connexion inactive (DCD), contournement de l'état SCTP, déchargement de flux.

La procédure générale suivante couvre la gamme des configurations possibles des paramètres de connexion. Choisissez et sélectionnez les éléments à mettre en œuvre en fonction de vos besoins.

Avant de commencer

Lorsqu'un paquet entre dans le périphérique, le pare-feu évalue d'abord les règles de contrôle d'accès et le NAT pour déterminer si une entrée de connexion doit être créée. Une entrée de connexion est créée, qu'une entrée ARP existe pour le prochain saut. Ainsi, l'existence d'une connexion ne signifie pas qu'un paquet dans la portée de la connexion l'a fait par l'intermédiaire du périphérique. Les paramètres de connexion tels que

les délais d'inactivité garantissent que les connexions indésirables ne persistent pas et n'utilisent pas les ressources du système.

Procédure

Étape 1 Configurer les délais d'expiration globaux, à la page 413. Ces paramètres modifient les délais d'inactivité par défaut pour divers protocoles pour tout le trafic qui passe par le périphérique. Si vous rencontrez des problèmes avec la réinitialisation des connexions en raison d'un délai d'expiration prématuré, essayez d'abord de modifier les délais d'expiration globaux.

Étape 2 Protéger les serveurs contre une attaque DoS par inondation SYN (interception de TCP), à la page 416. Utilisez cette procédure pour configurer l'interception TCP.

Étape 3 Personnaliser le traitement anormal des paquets TCP (listes TCP, normaliseur TCP), à la page 418, si vous souhaitez modifier le comportement de normalisation TCP par défaut pour des classes de trafic spécifiques.

Étape 4 Contourner les vérifications de l'état TCP pour le routage asymétrique (TCP State Bypass), à la page 421, si vous disposez de ce type d'environnement de routage.

Étape 5 Désactiver la gestion aléatoire de la séquence TCP, à la page 423, si l'aléatorisation par défaut brouille les données pour certaines connexions.

Étape 6 Délester les flux volumineux, à la page 425, si vous devez améliorer les performances dans un centre de données exigeant en informatique.

Étape 7 Configurer les paramètres de connexion pour des classes de trafic spécifiques (tous les services), à la page 429. Il s'agit d'une procédure « fourre-tout » pour les paramètres de connexion. Ces paramètres peuvent remplacer les valeurs globales par défaut pour des classes de trafic spécifiques à l'aide de règles de politique de service. Vous utilisez également ces règles pour personnaliser le normalisateur TCP, modifier l'aléatoire de séquence TCP, décrémenter la durée de vie des paquets et mettre en œuvre d'autres fonctionnalités facultatives.

Étape 8 Configurer les options TCP, à la page 433, si vous devez forcer les réinitialisations ou modifier un autre comportement TCP standard.

Configurer les délais d'expiration globaux

Vous pouvez définir les durées d'inactivité globales pour la connexion et les intervalles de traduction de divers protocoles. Si l'emplacement n'a pas été utilisé pendant la durée d'inactivité spécifiée, la ressource est remise dans le groupement (pool) libre.

La modification du délai d'expiration global définit un nouveau délai d'expiration par défaut, qui, dans certains cas, peut être remplacé pour des flux de trafic particuliers par le biais des politiques de service.

Pour les protocoles qui n'ont pas de paramètre de délai d'expiration configurable, comme GRE, le délai d'inactivité est de 2 minutes.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Global Timeouts (Délais d'expiration globaux)**.

Étape 2 Configurez les délais d'expiration en cochant les cases des délais d'expiration que vous souhaitez modifier et en saisissant la nouvelle valeur.

Toutes les durées sont affichées au format *hh*:*mm*:*ss*, avec une durée maximale de 1193:0:0 dans la plupart des cas. Dans tous les cas, à l'exception de Authentication absolute (Authentification absolue) et de Authentication inactivity (Inactivité de l'authentification), le fait de décocher les cases ramène le délai d'expiration à la valeur par défaut. Dans ces deux cas, le fait de décocher la case signifie une réauthentification à chaque nouvelle connexion.

Saisissez 0 pour désactiver le délai d'expiration.

- **Connexion**—Le temps d'inactivité jusqu'à ce qu'un emplacement de connexion soit libéré. Cette durée doit être d'au moins 5 minutes. La valeur par défaut est de 1 heure.
- **Half-Closed**—Le temps d'inactivité jusqu'à la fermeture d'une connexion TCP semi-fermée. Une connexion est considérée comme à moitié fermée si FIN et FIN-ACK ont été vus. Si seul le FIN a été vu, le délai d'expiration de connexion normal s'applique. La durée minimale est de 30 secondes. La valeur par défaut est 10 minutes.
- **UDP**—le temps d'inactivité avant la fermeture d'une connexion UDP. Cette durée doit être d'au moins 1 minute. La valeur par défaut est 2 minutes.
- **ICMP**—le temps d'inactivité après lequel les états ICMP généraux sont fermés. La valeur par défaut et minimale est de 2 secondes.
- **Erreur ICMP** : délai d'inactivité avant que l'ASA supprime une connexion ICMP après avoir reçu un paquet de réponse ECHO ICMP, entre 0:0:0 et 0:1:0 ou la valeur du délai d'expiration ICMP, selon la valeur la plus basse. La valeur par défaut est 0 (désactivé). Lorsque ce délai d'expiration est désactivé et que vous activez l'inspection ICMP, l'ASA supprime la connexion ICMP dès qu'une réponse d'écho est reçue; ainsi, toutes les erreurs ICMP générées pour la connexion (maintenant fermée) sont abandonnées. Ce délai d'expiration retarde la suppression des connexions ICMP afin que vous puissiez recevoir des erreurs ICMP importantes.
- **H.323**—le temps d'inactivité après lequel les connexions multimédias H.245 (TCP) et H.323 (UDP) sont fermées. La valeur par défaut est et minimale est de 5 minutes. Comme le même indicateur de connexion est défini sur les connexions multimédias H.245 et H.323, la connexion H.245 (TCP) partage le délai d'inactivité avec la connexion multimédia H.323 (RTP et RTCP).
- **H.225**—le temps d'inactivité avant la fermeture d'une connexion de signalisation H.225. La valeur par défaut est de 1 heure. Pour fermer une connexion immédiatement après l'élimination de tous les appels, un délai d'expiration de 1 seconde (0:0:1) est recommandé.
- **MGCP**—le temps d'inactivité après lequel une connexion de support MGCP est supprimée. La valeur par défaut est de 5 minutes, mais vous pouvez la fixer à 1 seconde.
- **MGCP PAT**—le temps d'inactivité après lequel une traduction de PAT MGCP est supprimée. La valeur par défaut est 5 minutes. La durée minimale est de 30 secondes.
- **TCP Proxy Reassembly**—le délai d'inactivité après lequel les paquets en mémoire tampon en attente de réassemblage sont abandonnés, entre 0:0:10 et 1193:0:0. La valeur par défaut est de 1 minute (0:1:0).
- **Floating Connection**—Lorsqu'il existe plusieurs routes vers un réseau avec différentes métriques, le système utilise celle ayant la meilleure métrique au moment de la création de la connexion. Si un meilleur routage devient disponible, ce délai d'expiration permet de fermer les connexions afin qu'une connexion puisse être rétablie pour utiliser le meilleur routage. La valeur par défaut est 0 (la connexion n'expire jamais). Pour permettre d'utiliser de meilleures routes, définissez le délai d'expiration à une valeur comprise entre 0:0:30 et 1193:0:0. Cette minuterie ne s'applique pas aux connexions par le biais

d'interfaces de tunnel virtuel (VTI). Si une connexion par l'intermédiaire d'un VTI est bloquée, vous devez l'effacer manuellement.

- **SCTP** : délai d'inactivité jusqu'à la fermeture d'une connexion SCTP (Stream Control Transmission Protocol), entre 0:1:0 et 1193:0:0. La valeur par défaut est 2 minutes. (0:2:0)
- **Stale Routes** (Routes périmées) — Durée de conservation d'une route périmée avant de la retirer de la base d'informations du routeur. Ces routes sont destinées aux protocoles de passerelle interne tels que OSPF. La valeur par défaut est de 70 secondes (00:01:10), la plage est comprise entre 00:00:10 et 00:01:40.
- **SUNRPC**—le temps d'inactivité jusqu'à ce qu'un emplacement SunRPC soit libéré. Cette durée doit être d'au moins 1 minute. La valeur par défaut est 10 minutes.
- **SIP**—le temps d'inactivité avant la fermeture d'une connexion de port de signalisation SIP. Cette durée doit être d'au moins 5 minutes. La valeur par défaut est de 30 minutes.
- **SIP Media**—le temps d'inactivité avant la fermeture d'une connexion de port de support SIP. Cette durée doit être d'au moins 1 minute. La valeur par défaut est 2 minutes. La minuterie de médias SIP est utilisée pour les paquets de médias SIP RTP/RTCP avec SIP UDP, plutôt que le délai d'inactivité d'UDP.
- **SIP Provisional Media**—la valeur du délai d'expiration pour les connexions multimédias provisoires SIP, entre 1 et 30 minutes. La valeur par défaut est 2 minutes.
- **SIP Invite**—le temps d'inactivité après lequel les passages pour les réponses PROVISOIRES et les xlates de médias seront fermés, entre 0:1:0 et 00:30:0. La valeur par défaut est de 3 minutes. (0:3:0).
- **SIP Disconnect**—le temps d'inactivité après lequel la session SIP est supprimée si 200 OK n'est pas reçu pour un message CANCEL ou BYE, entre 0:0:1 et 0:10:0. La valeur par défaut est 2 minutes. (0:2:0)
- **Authentication absolute**—la durée jusqu'à ce que la mémoire cache d'authentification expire et que les utilisateurs doivent s'authentifier à nouveau pour une nouvelle connexion. Cette minuterie est utilisée uniquement dans le mandataire direct, ce qui est une règle AAA. Cette durée doit être inférieure au délai d'expiration de l'intervalle de traduction. Le système attend que l'utilisateur établisse une nouvelle connexion pour demander à nouveau. Avant de désactiver la mise en cache pour forcer l'authentification à chaque nouvelle connexion, tenez compte des limites suivantes.
  - Ne définissez pas cette valeur à 0 si le FTP passif est utilisé sur les connexions.
  - Lorsque la valeur absolue de l'authentification est 0, l'authentification HTTPS peut ne pas fonctionner. Si un navigateur lance plusieurs connexions TCP pour téléverser une page Web après l'authentification HTTPS, la première connexion est autorisée, mais les connexions suivantes déclenchent l'authentification. Par conséquent, une page d'authentification s'affiche en permanence, même après une authentification réussie. Pour contourner ce problème, définissez le délai d'expiration absolu de l'authentification à 1 seconde. Cette solution de contournement ouvre une fenêtre d'occasion d'une seconde qui pourrait permettre aux utilisateurs non authentifiés de traverser le pare-feu s'ils proviennent de la même adresse IP source.
- **Authentication inactivity**—le temps d'inactivité jusqu'à ce que le cache d'authentification expire et que les utilisateurs doivent s'authentifier à nouveau pour une nouvelle connexion. Cette durée doit être inférieure à la valeur de l'intervalle de traduction. Ce délai est désactivé par défaut. Ce délai est désactivé par défaut. Cette minuterie est utilisée uniquement dans le mandataire direct, ce qui est une règle AAA.
- **Translation Slot**—le temps d'inactivité jusqu'à ce qu'un intervalle de traduction NAT soit libéré. Cette durée doit être d'au moins 1 minute. La valeur par défaut est de 3 heures.

- **PAT Translation Slot** (8.4(3) et versions ultérieures, sans inclure 8.5(1) et 8.6(1))—Le temps d'inactivité jusqu'à ce qu'un intervalle de traduction PAT soit libéré, entre 0:0:30 et 0:5:0. La valeur par défaut est de 30 secondes. Vous pourriez souhaiter augmenter le délai d'expiration si les routeurs en amont rejettent les nouvelles connexions utilisant un port PAT libéré, car la connexion précédente pourrait toujours être ouverte sur le périphérique en amont.
- **Connection Holddown** (Maintien de connexion) — Durée pendant laquelle le système doit maintenir une connexion lorsque la route utilisée par la connexion n'existe plus ou est inactive. Si le routage ne devient pas actif au cours de cette période d'attente, la connexion est libérée. Le but de la minuterie de maintien de connexion est de réduire l'effet du basculement des routes, où les routes peuvent apparaître et disparaître rapidement. Vous pouvez réduire le délai de maintien pour accélérer la convergence des routes. La valeur par défaut est de 15 secondes, et la plage est comprise entre 00:00:00 et 00:00:15.

Étape 3 Cliquez sur **Apply** (Appliquer).

Protéger les serveurs contre une attaque DoS par inondation SYN (interception de TCP)

Une attaque par déni de service par inondation SYN se produit lorsqu'un attaquant envoie une série de paquets SYN à un hôte. Ces paquets proviennent généralement d'adresses IP usurpées. Le flux constant de paquets SYN maintient la file d'attente SYN du serveur pleine, ce qui l'empêche de répondre aux demandes de connexion des utilisateurs légitimes.

Vous pouvez limiter le nombre de connexions amorces pour aider à prévenir les attaques par inondation SYN. Une connexion amorce est une demande de connexion qui n'a pas terminé l'établissement de liaison entre la source et la destination.

Lorsque le seuil de connexion embryonnaire d'une connexion est franchi, l'ASA agit comme un proxy pour le serveur et génère une réponse SYN-ACK à la requête SYN du client à l'aide de la méthode des cookies SYN, de sorte que la connexion ne soit pas ajoutée à la file d'attente SYN de l'hôte ciblé. Le témoin SYN est le numéro de séquence initial renvoyé dans le SYN-ACK qui est construit à partir du MSS, de l'horodatage et d'un hachage mathématique d'autres éléments pour créer principalement un code secret. Si l'ASA reçoit un ACK en retour du client avec le numéro de séquence correct et dans la fenêtre temporelle valide, il peut alors authentifier que le client est réel et autoriser la connexion au serveur. Le composant qui effectue le rôle de mandataire s'appelle TCP Intercept.

Le processus de bout en bout pour protéger un serveur contre une attaque par inondation SYN implique la définition des limites de connexion, l'activation des statistiques d'interception TCP, puis la surveillance des résultats.

Avant de commencer

- Veillez à ce que la limite de connexions amorces soit inférieure à la file d'attente TCP SYN sur le serveur que vous souhaitez protéger. Sinon, les clients valides ne peuvent plus accéder au serveur pendant une attaque SYN. Pour déterminer des valeurs raisonnables pour les limites amorces, analysez soigneusement la capacité du serveur, le réseau et l'utilisation du serveur.
- Selon le nombre de cœurs de CPU sur votre modèle d'ASA, le nombre maximal de connexions simultanées et de connexions embryonnaires peut dépasser les nombres configurés en raison de la façon dont chaque cœur gère les connexions. Dans le pire des cas, l'ASA autorise jusqu'à *n*-1 connexions supplémentaires et connexions embryonnaires, où *n* est le nombre de cœurs. Par exemple, si votre modèle comporte 4

cœurs, si vous configurez 6 connexions simultanées et 4 connexions amorces, vous pourriez en avoir 3 de chaque type. Pour déterminer le nombre de cœurs correspondant à votre modèle, saisissez la commande **show cpu core**.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (pare-feu)** > **Service Policy (politique de service)**.

Étape 2 Cliquez sur **Add (Ajouter) Add Service Policy Rule** (Ajouter une règle de politique de service).

Sinon, si vous avez déjà une règle pour les serveurs que vous souhaitez protéger, modifiez-la.

Étape 3 Choisissez d'appliquer la règle à une interface spécifique ou globalement à toutes les interfaces, puis cliquez sur **Next** (Suivant).

Étape 4 Pour Traffic Classification (Classification du trafic), sélectionnez **Source and Destination IP Addresses (uses ACL)** (Adresses IP source et de destination [utilise l'ACL]) et cliquez sur **Next** (Suivant).

Étape 5 Pour la règle d'ACL, saisissez les adresses IP des serveurs dans **Destination**, et précisez le protocole pour les serveurs. En règle générale, vous utilisez **any** pour la **Source**. Cliquez sur **Next** (Suivant) lorsque vous avez terminé.

Par exemple, si vous souhaitez protéger les serveurs Web 10.1.1.5 et 10.1.1.6, saisissez :

- Source = any
- Destination = 10.1.1.5, 10.1.1.6
- Destination Protocol (Protocole de destination) = tcp/http

Étape 6 Sur la page Rule Actions (Actions de règles), cliquez sur l'onglet **Paramètres de connexion** et complétez les options suivantes :

- **Embryonic Connections** (Connexions embryonnaires) : le nombre maximal de connexions TCP embryonnaires par hôte jusqu'à 2 000 000. La valeur par défaut est **0**, ce qui signifie que le nombre maximal de connexions embryonnaires est autorisé. Par exemple, vous pouvez la définir à 1 000.
- **Per Client Embryonic Connections** (Connexions embryonnaires par client) : le nombre maximal de connexions TCP embryonnaires simultanées pour chaque client jusqu'à 2 000 000. Lorsqu'une nouvelle connexion TCP est demandée par un client qui a déjà le nombre maximal de connexions embryonnaires par client ouvertes par l'intermédiaire de l'ASA, l'ASA empêche la connexion. Par exemple, vous pouvez la définir à 50.
- **TCP Syn Cookie MSS** (MSS des témoins SYN TCP) : la taille maximale de segment (MSS) du serveur pour la génération de témoins SYN pour les connexions embryonnaires lors de l'atteinte de la limite de connexions embryonnaires, de 48 à 65 535. La valeur par défaut est 1380. Ce paramètre n'a de sens que si vous configurez **Embryonic Connections** (Connexions embryonnaires) ou **Per Client Embryonic Connections** (Connexions embryonnaires par client).

Étape 7 Cliquez sur **Finish** (Terminer) pour enregistrer la règle et sur **Apply** (Appliquer) pour mettre à jour le périphérique.

Étape 8 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Threat Detection (Détection des menaces)**, et activez au moins les statistiques **TCP Intercept** (Interception TCP) dans le groupe Threat Detection Statistics (Statistiques de détection des menaces).

Vous pouvez simplement activer toutes les statistiques ou simplement activer l'interception TCP. Vous pouvez également ajuster la fenêtre et les débits de surveillance.

Étape 9 Choisissez **Home (Accueil)** > **Firewall Dashboard (Tableau de bord du pare-feu)**, et consultez le tableau de bord **Top Ten Protected Servers under SYN Attack** (Dix principaux serveurs protégés faisant l'objet d'une attaque SYN) pour surveiller les résultats.

Cliquez sur le bouton **Detail** (Détails) pour afficher les données d'échantillonnage de l'historique. L'ASA échantillonne le nombre d'attaques 30 fois au cours de l'intervalle de fréquence. Ainsi, pour la période par défaut de 30 minutes, des statistiques sont collectées toutes les 60 secondes.

Vous pouvez effacer les statistiques en saisissant la commande **clear threat-detection statistics tcp-intercept** à l'aide de **Tools (Outils) > Command Line Interface (Interface de ligne de commande).**

Personnaliser le traitement anormal des paquets TCP (listes TCP, normaliseur TCP)

Le normaliseur TCP identifie les paquets anormaux sur lesquels l'ASA peut agir lorsqu'ils sont détectés; par exemple, l'ASA peut autoriser, abandonner ou effacer les paquets. La normalisation TCP contribue à protéger l'ASA contre les attaques. La normalisation TCP est toujours activée, mais vous pouvez personnaliser le comportement de certaines fonctionnalités.

Pour personnaliser le normaliseur TCP, définissez d'abord les paramètres à l'aide d'une liste TCP. Vous pouvez ensuite appliquer la liste aux classes de trafic sélectionnées à l'aide des politiques de service.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **TCP Maps (Listes TCP)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle liste TCP. Attribuez un nom à la liste.
- Sélectionnez une liste, puis cliquez sur **Edit** (Modifier).

Étape 3 Dans le champ **Queue Limit** (Limite de file d'attente), saisissez le nombre maximal de paquets hors ordre qui peuvent être mis en mémoire tampon et mis en ordre pour une connexion TCP, entre 0 et 250 paquets.

La valeur par défaut est 0, ce qui signifie que ce paramètre est désactivé et que la limite de file d'attente du système par défaut est utilisée en fonction du type de trafic :

- Les connexions pour l'inspection d'application et TCP check-retransmission ont une limite de file d'attente de 3 paquets. Si l'ASA reçoit un paquet TCP avec une taille de fenêtre différente, la limite de la file d'attente est modifiée dynamiquement pour correspondre au paramètre annoncé.
- Pour les autres connexions TCP, les paquets hors ordre sont transmis sans être modifiés.

Si vous définissez la limite de file d'attente à 1 ou au-dessus, le nombre de paquets désordonnés autorisés pour tout le trafic TCP correspond à ce paramètre. Par exemple, pour l'inspection d'application et le trafic TCP check-retransmission, tous les paramètres annoncés des paquets TCP sont ignorés au profit du paramètre

Queue Limit (Limite de file d'attente). Pour les autres trafics TCP, les paquets hors ordre sont maintenant mis en mémoire tampon et mis en ordre au lieu d'être transmis sans modification.

Étape 4 Dans le champ **Timeout** (Délai d'expiration), définissez la durée maximale pendant laquelle les paquets hors ordre peuvent rester dans la mémoire tampon, entre 1 et 20 secondes.

S'ils ne sont pas mis en ordre et transmis dans le délai d'expiration, ils sont abandonnés. La valeur par défaut est de 4 secondes. Vous ne pouvez pas modifier le délai d'expiration d'un trafic si la limite de file d'attente est définie à 0; vous devez définir la limite à 1 ou plus pour que le délai d'expiration prenne effet.

Étape 5 Pour **Reserved Bits** (Bits réservés), sélectionnez comment gérer les paquets qui ont des bits réservés dans l'en-tête TCP : **Clear and allow** (Effacer et autoriser) (supprimer les bits avant d'autoriser le paquet), **Allow only (Autoriser uniquement**) (ne pas modifier les bits, la valeur par défaut) ou **Drop the packet** (Abandonner le paquet).

Étape 6 Sélectionnez l'une des options suivantes :

- **Clear urgent flag** (Effacer l'indicateur urgent) : efface l'indicateur URG dans un paquet avant de l'autoriser. L'indicateur URG est utilisé pour indiquer que le paquet contient des informations de priorité plus élevée que les autres données du flux. Le RFC de TCP est vague sur l'interprétation exacte de l'indicateur URG, donc les systèmes finaux gèrent les décalages urgents de différentes manières, ce qui peut rendre le système final vulnérable aux attaques.
- **Drop connection on window variation** (Abandonner la connexion en cas de variation de fenêtre) : abandonne une connexion dont la taille de fenêtre a été modifiée de manière inattendue. Le mécanisme de taille de fenêtre permet à TCP d'annoncer une grande fenêtre et d'annoncer ultérieurement une fenêtre beaucoup plus petite sans avoir accepté trop de données. À partir de la spécification TCP, la « réduction de la fenêtre » est fortement déconseillée.
- **Drop packets that exceed maximum segment size** (Abandonner les paquets qui dépassent la taille maximale de segment) : abandonne les paquets qui dépassent le MSS défini par l'homologue.
- **Check if transmitted data is the same as original** (Vérifier si les données transmises sont identiques aux données d'origine) : active les vérifications des données de retransmission, qui empêchent les retransmissions TCP incohérentes.
- **Drop packets which have past-window sequence** (Abandonner les paquets dont la séquence est au-delà de la fenêtre) : abandonne les paquets qui ont des numéros de séquence au-delà de la fenêtre, c'est-à-dire que le numéro de séquence d'un paquet TCP reçu est supérieur au bord droit de la fenêtre de réception TCP. Pour autoriser ces paquets, désélectionnez cette option et définissez **Queue Limit** (Limite de file d'attente) à 0 (désactivation de la limite de file d'attente).
- **Drop SYN Packets with data** (Abandonner les paquets SYN avec données) : abandonne les paquets SYN qui contiennent des données.
- **Enable TTL Evasion Protection** (Activer la protection contre l'évitement TTL) : la TTL maximale pour une connexion est déterminée par la TTL dans le paquet initial La TTL des paquets suivants peut diminuer, mais elle ne peut pas augmenter. Le système réinitialisera la TTL au plus bas TTL vu précédemment pour cette connexion. Cela empêche les attaques d'évitement TTL.

  Par exemple, un agresseur peut envoyer un paquet qui passe la politique avec un TTL très court. Lorsque le TTL passe à zéro, un routeur entre l'ASA et le terminal abandonne le paquet. C'est à ce stade que l'agresseur peut envoyer un paquet malveillant avec un TTL long qui apparaît à l'ASA comme une retransmission et qui est transmis. Pour l'hôte du terminal, cependant, il s'agit du premier paquet reçu par l'agresseur. Dans ce cas, un agresseur peut réussir sans que la sécurité empêche l'attaque.

- **Verify TCP Checksum** (Vérifier la somme de contrôle TCP) : vérifie la somme de contrôle TCP, en abandonnant les paquets qui échouent à la vérification.
- **Drop SYNACK Packets with data** (Abandonner les paquets SYNACK avec données) : abandonne les paquets TCP SYNACK qui contiennent des données.
- **Drop packets with invalid ACK** (Abandonner les paquets avec un ACK non valide) : abandonne les paquets avec un ACK non valide. Vous pourriez voir des adresses ACK non valides dans les instances suivantes :
  - Dans l'état de la réception SYN-ACK de la connexion TCP, si le numéro ACK d'un paquet TCP reçu n'est pas exactement identique au numéro de séquence du paquet TCP suivant, il s'agit d'un ACK non valide.
  - Chaque fois que le numéro d'accusé de réception d'un paquet TCP reçu est supérieur au numéro de séquence du prochain paquet TCP envoyé, il s'agit d'un ACK non valide.

Remarque
Les paquets TCP avec un ACK non valide sont automatiquement autorisés pour les connexions WAAS.

Étape 7 (Facultatif) Cliquez sur l'onglet **TCP Options** (Options TCP) et définissez l'action pour les paquets qui contiennent des options TCP.

Vous pouvez effacer les options avant d'autoriser les paquets, autoriser les paquets s'ils contiennent une seule option d'un type donné ou autoriser les paquets même s'ils ont plusieurs options d'un type donné. La valeur par défaut est d'autoriser les cinq options nommées tant qu'une option donnée ne s'affiche pas plus d'une fois par paquet (sinon le paquet est abandonné), tout en effaçant toutes les autres options. Vous pouvez également abandonner les paquets contenant l'option MD5 ou l'une des options numérotées. Notez que si une connexion TCP est inspectée, toutes les options sont effacées, à l'exception des options MSS et d'accusé de réception sélectif (SACK), quelle que soit votre configuration.

a) Sélectionnez l'action pour les options **d'accusé de réception sélectif**, **d'horodatage TCP** et **d'échelle de fenêtre**.

L'effacement de l'option d'horodatage désactive PAWS et RTT.

b) Sélectionnez l'action pour l'option **MSS** (Taille maximale du segment).

En plus des actions normales Allow (Autoriser), Allow multiple (Autoriser plusieurs) et Clear (Effacer), vous pouvez sélectionner **Specify Maximum** (Préciser la valeur maximale) et saisir la taille maximale de segment, de 68 à 65 535. Le MSS TCP par défaut est défini sur la page **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **TCP Options (Options TCP)** .

c) Choisissez si vous souhaitez définir l'option **Allow packets with the MD5 option** (Autoriser les paquets avec l'option MD5).

Si vous décochez la case, les paquets qui contiennent l'option MD5 sont abandonnés. Si vous sélectionnez l'option, vous pouvez appliquer les actions normales d'autoriser, autoriser plusieurs ou effacer.

d) Sélectionnez l'action pour les options par plage de numéros.

Les options numérotées 6 à 7, 9 à 18 et 20 à 255 sont effacées par défaut. Vous pouvez plutôt autoriser les options ou abandonner les paquets qui contiennent l'option. Vous pouvez spécifier différentes actions pour différentes plages d'options : saisissez simplement le nombre inférieur et supérieur pour la plage, sélectionnez l'action et cliquez sur **Add** (Ajouter). Pour configurer une action pour une seule option, saisissez le même nombre pour les plages inférieure et supérieure.

Pour supprimer une plage configurée, sélectionnez-la et cliquez sur **Delete** (Supprimer).

Étape 8 Cliquez sur **OK** puis sur **Apply** (Appliquer).

Vous pouvez maintenant utiliser la liste TCP dans une politique de service. La liste affecte le trafic uniquement lorsqu'elle est appliquée par le biais d'une politique de service.

Étape 9 Appliquez la liste TCP à une classe de trafic à l'aide d'une politique de service.

a) Choisissez **Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service)**.
b) Ajoutez ou modifiez une règle. Vous pouvez appliquer la règle globalement ou à une interface. Par exemple, pour personnaliser le traitement aberrant de paquets pour tout le trafic, créez une règle globale qui correspond à tout trafic. Passez à la page Rule Actions (Actions de règle).
c) Cliquez sur l'onglet **Connection Settings** (Paramètres de connexion).
d) Choisissez **Use TCP Map** (Utiliser la liste TCP) et sélectionnez la liste que vous avez créée.
e) Cliquez sur **Finish** (Terminer) ou **OK** (OK), puis sur **Apply** (Appliquer).

Contourner les vérifications de l'état TCP pour le routage asymétrique (TCP State Bypass)

Si vous disposez d'un environnement de routage asymétrique dans votre réseau, où le flux sortant et le flux entrant pour une connexion donnée peuvent passer par deux périphériques ASA différents, vous devez mettre en œuvre le contournement de l'état TCP sur le trafic concerné.

Cependant, le contournement de l'état TCP diminue la sécurité de votre réseau, vous devez donc appliquer le contournement sur les classes de trafic très spécifiques et limitées.

Les rubriques suivantes expliquent la problématique et sa solution plus en détail.

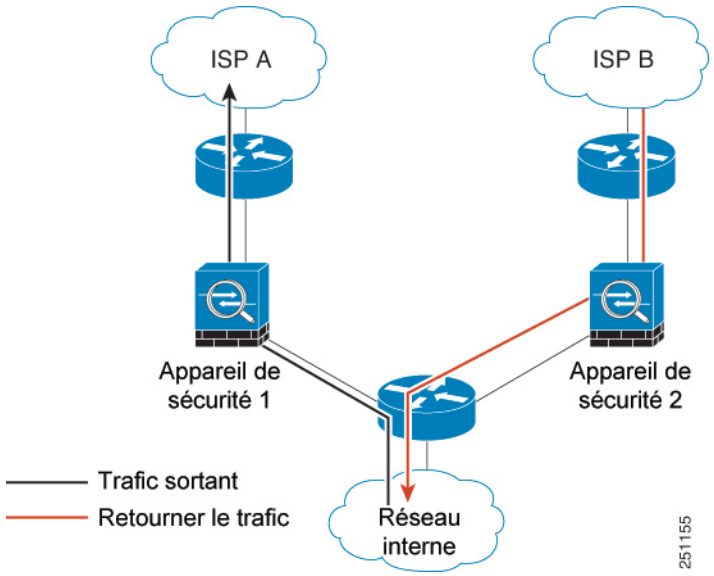
Le problème du routage asymétrique

Par défaut, tout le trafic qui passe par ASA est inspecté à l'aide de l'algorithme de sécurité adaptatif et est soit autorisé, soit abandonné en fonction de la politique de sécurité. ASA optimise la performance du pare-feu en vérifiant l'état de chaque paquet (nouvelle connexion ou connexion établie) et l'affecte au chemin de gestion de session (un nouveau paquet SYN de connexion), au chemin rapide (une connexion établie) ou au chemin de contrôle trajectoire du plan (inspection avancée).

Les paquets TCP qui correspondent à des connexions existantes sur le chemin rapide peuvent passer par l'ASA sans vérifier de nouveau tous les aspects de la politique de sécurité. Cette fonctionnalité maximise les performances. Cependant, la méthode d'établissement de la session dans le chemin rapide à l'aide du paquet SYN et les vérifications qui se produisent dans le chemin rapide (comme le numéro de séquence TCP) peuvent faire obstacle aux solutions de routage dissymétrique : les flux sortant et entrant d'une connexion doit passer par le même périphérique ASA.

Par exemple, une nouvelle connexion est dirigée vers le périphérique de sécurité 1. Le paquet SYN passe par le chemin de gestion de session et une entrée pour la connexion est ajoutée au tableau du chemin rapide. Si les paquets suivants de cette connexion passent par le périphérique de sécurité 1, les paquets correspondent à l'entrée du chemin rapide et sont transmis. Mais si les paquets suivants sont acheminés au périphérique de sécurité 2, où aucun paquet SYN n'a été soumis par le chemin de gestion de session, il n'y a pas d'entrée dans le chemin rapide pour la connexion et les paquets sont abandonnés. La figure suivante montre un exemple de routage symétrique dans lequel le trafic sortant passe par un ASA différent du trafic entrant :

Illustration 40 : Routage asymétrique



Si le routage asymétrique est configuré sur les routeurs en amont et que le trafic alterne entre deux périphériques ASA, vous pouvez configurer le contournement de l'état TCP pour un trafic spécifique. Le contournement de l'état TCP modifie la façon dont les sessions sont établies dans le chemin rapide et désactive les vérifications du chemin rapide. Cette fonctionnalité traite le trafic TCP de la même manière qu'elle traite une connexion UDP : lorsqu'un paquet non SYN correspondant aux réseaux spécifiés entre dans le périphérique ASA, et qu'il n'y a pas d'entrée de chemin rapide, le paquet passe par le chemin de gestion de session pour établir le connexion sur le chemin rapide. Une fois dans le chemin rapide, le trafic contourne les vérifications du chemin rapide.

Lignes directrices et limites du contournement d'état TCP

Fonctionnalités non prises en charge du contournement de l'état TCP

Les fonctionnalités suivantes ne sont pas prises en charge lorsque vous utilisez le contournement de l'état TCP :

- Inspection d'application : l'inspection nécessite que le trafic entrant et sortant passe par le même ASA, donc l'inspection n'est pas appliquée au trafic de contournement d'état TCP.
- Sessions authentifiées par AAA : lorsqu'un utilisateur s'authentifie auprès d'un ASA, le trafic revenant par l'autre ASA sera refusé, car l'utilisateur ne s'est pas authentifié auprès de cet ASA.
- Interception TCP, limite maximale de connexions explorées, répartition aléatoire des numéros de séquence TCP : l'ASA ne fait pas le suivi de l'état de la connexion, donc ces fonctionnalités ne sont pas appliquées.
- Normalisation TCP : le normalisateur TCP est désactivé.

Lignes directrices relatives à la NAT pour le contournement d'état TCP

Comme la session de traduction est établie séparément pour chaque périphérique, veillez à configurer la NAT statique sur les deux périphériques pour le trafic de contournement d'état TCP. Si vous utilisez la NAT

dynamique, l'adresse choisie pour la session sur le périphérique 1 sera différente de celle choisie pour la session sur le périphérique 2.

Configurer le contournement d'état TCP

Pour contourner la vérification de l'état TCP dans des environnements de routage symétrique, définissez avec soin une classe de trafic qui s'applique aux hôtes ou aux réseaux concernés uniquement, puis activez le contournement de l'état TCP sur la classe de trafic à l'aide d'une politique de service. Étant donné que le contournement réduit la sécurité du réseau, limitez son application autant que possible.

Avant de commencer

S'il n'y a aucun trafic sur une connexion donnée pendant 2 minutes, la connexion expire. Vous pouvez remplacer cette valeur par défaut en modifiant le **délai d'inactivité** pour la classe de trafic de contournement de l'état TCP. Les connexions TCP normales expirent par défaut après 60 minutes.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (pare-feu)** > **Service Policy (politique de service)**.

Étape 2 Cliquez sur **Add (Ajouter) Add Service Policy Rule** (Ajouter une règle de politique de service).

Sinon, si vous avez déjà une règle pour les hôtes, modifiez-la.

Étape 3 Choisissez d'appliquer la règle à une interface spécifique ou globalement à toutes les interfaces, puis cliquez sur **Next** (Suivant).

Étape 4 Pour Traffic Classification (Classification du trafic), sélectionnez **Source and Destination IP Addresses (uses ACL)** (Adresses IP source et de destination [utilise l'ACL]) et cliquez sur **Next** (Suivant).

Étape 5 Pour la règle d'ACL, saisissez les adresses IP des hôtes à chaque extrémité de la route dans **Source** et **Destination**, et spécifiez le protocole TCP. Cliquez sur **Next** (Suivant) lorsque vous avez terminé.

Par exemple, si vous souhaitez contourner la vérification de l'état TCP entre 10.1.1.1 et 10.2.2.2, saisissez :

- Source = 10.1.1.1
- Destination = 10.2.2.2
- Protocole de destination = tcp

Étape 6 Dans la page Rule Actions (Actions de règle), cliquez sur l'onglet **Connection Settings** (Paramètres de connexion) et sélectionnez **TCP State Bypass** (Contournement de l'état TCP).

Étape 7 Cliquez sur **Finish** (Terminer) pour enregistrer la règle et **Apply** (Appliquer) pour mettre à jour le périphérique.

Désactiver la gestion aléatoire de la séquence TCP

Chaque connexion TCP a deux numéros de séquence initiaux (ISN) : un généré par le client et un généré par le serveur. L'ASA effectue la randomisation de l'ISN du SYN TCP dans les sens entrant et sortant.

La distribution aléatoire de l'ISN de l'hôte protégé empêche un agresseur de prédire le prochain ISN pour une nouvelle connexion et de détourner potentiellement la nouvelle session. Cependant, la répartition aléatoire

des séquences TCP rompt en pratique les SACK TCP (accusé de réception sélectif), car les numéros de séquence que voit le client sont différents de ce que le serveur voit.

Vous pouvez désactiver la répartition aléatoire des numéros de séquence initial TCP si nécessaire, par exemple, parce que les données sont brouillées. Par exemple :

- Si un autre pare-feu en ligne effectue également la répartition aléatoire des numéros de séquence initiaux, il n'est pas nécessaire que les deux pare-feu effectuent cette action, même si cette action n'affecte pas le trafic.
- Si vous utilisez le protocole eBGP multi-sauts via l'ASA et que les homologues eBGP utilisent le protocole MD5. La randomisation rompt la somme de contrôle MD5.
- Si vous utilisez un périphérique WAAS qui exige que l'ASA ne randomise pas les numéros de séquence des connexions.
- Si vous activez le contournement matériel pour l'ISA 3000, les connexions TCP sont abandonnées lorsque l'ISA 3000 ne fait plus partie du chemin de données.

Remarque Nous vous déconseillons de désactiver la répartition aléatoire de la séquence TCP lors de l'utilisation de la mise en grappe. Il y a un faible risque que certaines sessions TCP ne soient pas établies, car le paquet SYN/ACK sera abandonné.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (pare-feu)** > **Service Policy (politique de service)** .

Étape 2 Cliquez sur **Add (Ajouter) Add Service Policy Rule** (Ajouter une règle de politique de service).

Sinon, si vous avez déjà une règle pour le trafic ciblé, modifiez-la.

Étape 3 Choisissez d'appliquer la règle à une interface spécifique ou globalement à toutes les interfaces, puis cliquez sur **Next** (Suivant).

Étape 4 Pour la classification du trafic, identifiez le type de correspondance de trafic. La correspondance de classe doit concerner le trafic TCP; vous pouvez identifier des hôtes spécifiques (avec une liste de contrôle d'accès), faire une correspondance de port TCP ou simplement faire correspondre n'importe quel trafic. Cliquez sur **Next** (Suivant) et configurez les hôtes dans la liste de contrôle d'accès ou définissez les ports, puis cliquez à nouveau sur **Next** (Suivant).

Par exemple, si vous souhaitez désactiver l'aléatoireisation du numéro de séquence TCP pour tout le trafic TCP dirigé vers l'adresse 10.2.2.2, saisissez :

- Source = any
- Destination = 10.2.2.2
- Protocole de destination = tcp

Étape 5 Sur la page Rule Actions (Actions de règles), cliquez sur l'onglet **Connection Settings (paramètres de connexion)** et décochez **la case de hasarder le numéro de séquence**.

Étape 6 Cliquez sur **Finish** (Terminer) pour enregistrer la règle et **Apply** (Appliquer) pour mettre à jour le périphérique.

Délester les flux volumineux

Si vous déployez l'ASA sur les périphériques pris en charge dans un centre de données, vous pouvez identifier le trafic sélectionné à décharger vers un chemin ultra-rapide, où le trafic est commuté dans la carte réseau elle-même. Le déchargement peut vous aider à améliorer les performances des applications exigeantes en données, telles que les transferts de fichiers volumineux.

- Les sites de recherche en informatique à haute performance (HPC), où l'ASA est déployé entre les stations de stockage et les stations d'informatique à haute performance. Lorsqu'un site de recherche effectue une sauvegarde à l'aide du transfert de fichiers FTP ou de la synchronisation de fichiers sur NFS, l'importance du trafic de données affecte tous les contextes sur l'ASA. Le déchargement du transfert de fichiers FTP et de la synchronisation des fichiers sur NFS réduit l'impact sur le reste du trafic.
- La négociation à haute fréquence (HFT), où l'ASA est déployé entre les postes de travail et l'Exchange, principalement à des fins de conformité. La sécurité n'est généralement pas un problème, mais la latence est une préoccupation majeure.

Avant d'être déchargé, l'ASA applique d'abord un traitement de sécurité normal, tel que les règles d'accès et l'inspection, lors de l'établissement de la connexion. L'ASA effectue également le démontage de la session. Mais une fois une connexion établie, si elle peut être déchargée, le traitement ultérieur se produit dans la carte réseau plutôt que dans l'ASA.

Les flux déchargés continuent de recevoir une inspection dynamique limitée, comme la vérification des indicateurs TCP de base et des options, et la vérification des sommes de contrôle si vous la configurez. Le système peut sélectivement transmettre les paquets au système de pare-feu pour un traitement plus approfondi si nécessaire.

Pour identifier les flux qui peuvent être déchargés, vous créez une règle de politique de service qui applique le service de déchargement de flux. Un flux correspondant est ensuite déchargé s'il répond aux conditions suivantes :

- Adresses IPv4 uniquement.
- TCP, UDP, GRE uniquement.
- Trames standard ou Ethernet balisées 802.1Q uniquement.
- (Mode transparent uniquement.) Le déchargement de multidiffusion est disponible pour les groupes de ponts qui contiennent deux et seulement deux interfaces.

Les flux inverses pour les flux déchargés sont également déchargés.

Limites de déchargement de flux

Tous les flux ne peuvent pas être déchargés. Même après le déchargement, il est possible de désactiver le déchargement d'un flux dans certaines conditions. Voici quelques-unes des limites :

Limites du périphérique

La fonctionnalité est prise en charge sur les périphériques suivants :

- Secure Firewall 3100 (statique uniquement)

- Firepower 4100/9300

Flux qui ne peuvent pas être déchargés

Les types de flux suivants ne peuvent pas être déchargés.

- Flux qui n'utilise pas l'adressage IPv4, comme l'adressage IPv6.
- Flux pour tout protocole autre que TCP, UDP et GRE.



Remarque Les connexions PPTP GRE ne peuvent pas être déchargées.

- Flux qui nécessitent une inspection. Dans certains cas, comme FTP, le canal de données secondaire peut être déchargé bien que le canal de contrôle ne puisse pas être déchargé.
- Connexions VPN IPsec et TLS/DTLS qui se terminent sur le périphérique.
- Flux de multidiffusion en mode routé.
- Flux de multidiffusion en mode transparent pour les groupes de ponts qui comportent trois interfaces ou plus.
- Flux d'interception TCP.
- Flux de contournement d'état TCP Vous ne pouvez pas configurer le déchargement de flux et le contournement de l'état TCP sur le même trafic.
- Flux mandataires AAA de type cut-through.
- Vpath, flux liés à VXLAN.
- Flux balisés avec les groupes de sécurité.
- Flux inverses qui sont transférés à partir d'un nœud de grappe différent, en cas de flux dissymétriques dans une grappe.
- Flux centralisés en grappe, si le propriétaire du flux n'est pas l'unité de contrôle.

Restrictions supplémentaires

- Le déchargement de flux et la détection de connexion inactive (DCD) ne sont pas compatibles. Ne configurez pas la DCD sur les connexions qui peuvent être déchargées.
- si plusieurs flux correspondant aux conditions de déchargement de flux sont mis en file d'attente pour être déchargés en même temps au même emplacement sur le matériel, seul le premier flux est déchargé. Les autres flux sont traités normalement. C'est ce qu'on appelle une *collision*. Utilisez la commande **show flow-offload flow** dans l'interface de ligne de commande pour afficher les statistiques de cette situation.
- Bien que les flux déchargés passent par les interfaces FXOS, les statistiques pour ces flux ne s'affichent pas sur l'interface de périphérique logique. Par conséquent, les compteurs d'interface de périphérique logique et les débits de paquets ne reflètent pas les flux déchargés.

Conditions d'inversion du déchargement

Après le déchargement d'un flux, les paquets qu'il contient sont renvoyés au système d'exploitation du pare-feu pour traitement ultérieur s'ils remplissent les conditions suivantes :

- Ils comprennent les options TCP autres que l'horodatage.
- Ils sont fragmentés.
- Ils sont soumis au routage à chemins multiples à coûts égaux (ECMP), et les paquets entrants sont déplacés d'une interface à une autre.
- Une modification de la table de routage s'applique au flux. Un paquet est renvoyé au périphérique pour déterminer la nouvelle route.

Configurer le déchargement de flux

Pour configurer le déchargement de flux, vous devez activer le service, puis créer des politiques de service pour identifier le trafic admissible au déchargement. Pour le Firepower 4100/9300 : lorsque vous activez le service pour la première fois, vous devez redémarrer. .

Procédure

Étape 1 Activez le service de déchargement de flux.

Pour le Firepower 4100/9300 : lorsque vous activez le service pour la première fois, vous devez redémarrer.

Si un redémarrage est requis, des considérations particulières s'appliquent aux grappes ou aux paires de basculement si vous souhaitez effectuer un changement sans interruption :

- Mise en grappe : saisissez d'abord la commande sur le nœud de contrôle, mais ne redémarrez pas le nœud de contrôle immédiatement. Au lieu de cela, redémarrez d'abord chaque nœud de la grappe, puis revenez au nœud de contrôle et redémarrez-le. Vous pouvez ensuite configurer la politique de service de déchargement sur le nœud de contrôle.
- Basculement : saisissez d'abord la commande sur l'unité active, sans la redémarrer immédiatement. Au lieu de cela, redémarrez l'unité en veille, puis redémarrez l'unité active. Vous pouvez ensuite configurer la politique de service de déchargement sur l'unité active.

a) Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Offload Engine (Moteur de déchargement)**.
b) Cochez **Enable Offload Engine** (Activer le moteur de déchargement).
c) Cliquez sur **Apply**.
d) Cliquez sur **Save** (Enregistrer) pour enregistrer vos modifications dans la configuration de démarrage.
e) (Firepower 4100/9300) Sélectionnez **Tools (Outils)** > **System Reload** (Redémarrage du système) pour redémarrer le périphérique.

Étape 2 Créez la règle de politique de service qui identifie le trafic admissible au déchargement.

a) Choisissez **Configuration** > **Firewall (pare-feu)** > **Service Policy (politique de service)**.
b) Cliquez sur **Add (Ajouter) Add Service Policy Rule** (Ajouter une règle de politique de service).

Sinon, si vous avez déjà une règle pour les hôtes, modifiez-la.

c) Choisissez d'appliquer la règle à une interface spécifique ou globalement à toutes les interfaces, puis cliquez sur **Next** (Suivant).
d) Pour Traffic Classification (Classification du trafic), la mise en correspondance par liste d'accès (**Source and Destination IP Addresses (uses ACL) (Adresses IP source et de destination (utilise une ACL**))) ou par port (**TCP or UDP or SCTP Destination Port**) constitue généralement les options les plus courantes. Sélectionnez une option et cliquez sur **Next** (Suivant).
e) Saisissez les critères d'ACL ou de port. Cliquez sur **Next** (Suivant) lorsque vous avez terminé.

   Par exemple, si vous souhaitez rendre tout le trafic TCP sur le sous-réseau 10.1.1.0/255.255.255.224 admissible au déchargement, saisissez :

   - Source = 10.1.1.0/255.255.255.224 (ou 10.1.1.0/27)
   - Destination = any
   - Protocole de destination = tcp

f) Sur la page Rule Actions (actions de règles), cliquez sur l'onglet **Connection Settings (paramètres de connexion)** et sélectionnez **Flow Offload (déchargement de flux)**.
g) Cliquez sur **Finish** (Terminer) pour enregistrer la règle et sur **Apply** (Appliquer) pour mettre à jour le périphérique.

Décharge de flux IPsec

Vous pouvez configurer des modèles de périphérique de prise en charge pour utiliser le déchargement de flux IPsec. Après la configuration initiale d'une association de sécurité (SA), d'un VPN de site à site ou d'un VPN d'accès à distance IPsec, les connexions IPsec sont déchargées vers le FPGA (field programmable gate RAID) dans le périphérique, ce qui devrait améliorer les performances du périphérique.

Les opérations déchargées sont spécifiquement liées au traitement de pré déchiffrement et de déchiffrement à l'entrée, et au traitement de pré chiffrement et de chiffrement à la sortie. Le logiciel système gère le flux interne pour appliquer vos politiques de sécurité.

Le déchargement de flux IPsec est activé par défaut et s'applique aux types de périphériques suivants :

- Secure Firewall 3100

Limites du déchargement de flux IPsec

Les flux IPsec suivants ne sont pas déchargés :

- Tunnels IKEv1. Seuls les tunnels IKEv2 seront déchargés. IKEv2 prend en charge les chiffrements plus forts.
- Flux pour lesquels une régénération basée sur le volume est configurée.
- Flux pour lesquels la compression est configurée.
- Flux des modes de transport. Seuls les flux en mode tunnel seront déchargés.
- Format AH. Seul le format ESP/NAT-T sera pris en charge.
- Les flux dont la post-fragmentation est configurée.

- Flux qui ont une taille de fenêtre d'anti-relecture autre que 64 bits et l'anti-relecture n'est pas désactivé.
- Les flux pour lesquels le filtre de pare-feu est activé.
- Mode à contextes multiples.

Configurer le déchargement de flux IPsec

Le déchargement de flux IPSec est activé par défaut sur les plateformes matérielles qui prennent en charge la fonctionnalité. Cependant, l'optimisation de sortie n'est pas activée par défaut, vous devez donc la configurer si vous souhaitez cette fonctionnalité.

Avant de commencer

Le déchargement de flux IPsec est configuré globalement. Vous ne pouvez pas le configurer pour les flux de trafic sélectionnés.

Utilisez la forme **no** de ces commandes pour désactiver les fonctionnalités.

Pour voir l'état actuel de la configuration, utilisez la commande **show flow-offload ipsec info**.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **IPsec Offload (Déchargement IPsec)**.

Étape 2 Sélectionnez **IPsec Offload** (Déchargement IPsec) pour activer le déchargement de flux IPsec.

Étape 3 Sélectionnez **Egress Optimization For IPSec Offload** (Optimisation de sortie pour le déchargement IPsec) pour optimiser le chemin d'accès aux données afin d'améliorer les performances pour les flux de tunnel unique.

La configuration pour l'optimisation de sortie est distincte du déchargement de flux. Cependant, même si elle est activée, elle n'a d'incidence que si vous activez également le déchargement de flux IPsec.

Configurer les paramètres de connexion pour des classes de trafic spécifiques (tous les services)

Vous pouvez configurer différents paramètres de connexion pour des classes de trafic spécifiques à l'aide des politiques de service. Utilisez les politiques de service pour :

- Personnalisez les limites de connexion et les délais d'expiration utilisés pour la protection contre les attaques DoS et SYN-flooding.
- Implémentez la détection de connexion inactive pour que les connexions valides, mais inactives, restent actives.
- Désactivez l'aléatoirisation du numéro de séquence TCP dans les cas où vous n'en avez pas besoin.
- Personnalisez la manière dont le normalisateur TCP protège contre les paquets TCP anormaux.

- Implémentez le contournement de l'état TCP pour le trafic soumis à un routage asymétrique. Le trafic de contournement n'est pas soumis à l'inspection.
- Implémentez le contournement de l'état SCTP (Stream Control Transmission Protocol) pour désactiver l'inspection dynamique SCTP.
- Mettez en œuvre le déchargement de flux pour améliorer les performances sur les plateformes matérielles prises en charge.
- Décrémentez la durée de vie (TTL) des paquets afin que l'ASA s'affiche dans la sortie traceroute.



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 TTL = 1, donc la décrémentation de la durée de vie peut avoir des conséquences inattendues pour les appareils ASA en mode transparent. Les paramètres de décrément de la durée de vie n'ont pas d'incidence sur le processus OSPF lorsque l'ASA fonctionne en mode routé.

Vous pouvez configurer n'importe quelle combinaison de ces paramètres pour une classe de trafic donnée, à l'exception du contournement de l'état TCP et de la personnalisation du normaliseur TCP, qui s'excluent mutuellement.



Astuces Cette procédure montre une politique de service pour le trafic qui passe par l'ASA. Vous pouvez également configurer la connexion maximale et la connexion embryonnaire maximale pour le trafic de gestion (vers le périphérique).

Avant de commencer

Si vous souhaitez personnaliser le normalisateur TCP, créez la liste TCP requise avant de continuer.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**, et ouvrez une règle.

- Pour créer une nouvelle règle, cliquez sur **Add (Ajouter) > Add Service Policy Rule (Ajouter une règle de politique de service)**. Passez par l'assistant jusqu'à la page Règles.
- Si vous avez une règle pour laquelle vous modifiez les paramètres de connexion, sélectionnez-la et cliquez sur **Edit** (Modifier).

Étape 2 Sur la page ou l'onglet Rule Actions (Actions de règles) de l'assistant, sélectionnez l'onglet **Connection Settings** (Paramètres de connexion).

Étape 3 Pour définir le nombre maximal de connexions, configurez les valeurs suivantes dans la zone Maximum Connections (Nombre maximal de connexions) :

Par défaut, il n'y a aucune limite à la connexion. Si vous mettez en œuvre des limites, le système doit commencer à les suivre, ce qui peut augmenter l'utilisation du processeur et de la mémoire et entraîner des problèmes opérationnels pour les systèmes soumis à une charge élevée, en particulier dans une grappe.

- **Maximum TCP, UDP and SCTP Connections**—(TCP, UDP, SCTP.) Le nombre maximal de connexions simultanées pour tous les clients dans la classe de trafic, jusqu'à 2 000 000. La valeur par défaut est 0, ce qui signifie que le nombre maximal de connexions possibles est autorisé. Pour les connexions TCP, ce nombre s'applique aux connexions établies uniquement.
- **Embryonic Connections** (Connexions embryonnaires) : spécifie le nombre maximal de connexions TCP embryonnaires par hôte jusqu'à 2 000 000. Une connexion amorce est une demande de connexion qui n'a pas terminé l'établissement de liaison entre la source et la destination. La valeur par défaut est **0**, ce qui signifie que le nombre maximal de connexions embryonnaires est autorisé. En définissant une limite non nulle, vous activez l'interception de TCP, qui protège les systèmes internes contre les attaques DoS perpétrées en inondant une interface de paquets SYN du protocole TCP. Définissez également les options par client pour vous protéger contre l'inondation SYN.
- **Per Client Connections (Connexions par client)** — (TCP, UDP, SCTP.) Spécifie le nombre maximal de connexions simultanées pour chaque client jusqu'à 2 000 000. Lorsqu'une nouvelle connexion est tentée par un client qui a déjà ouvert le nombre maximal de connexions par client, l'ASA rejette la connexion et abandonne le paquet. Pour les connexions TCP, cela inclut les connexions établies, à moitié ouvertes et à moitié fermées.
- **Per Client Embryonic Connections** (Connexions embryonnaires par client) — Spécifie le nombre maximal de connexions TCP embryonnaires simultanées pour chaque client jusqu'à 2 000 000. Lorsqu'une nouvelle connexion TCP est demandée par un client qui a déjà le nombre maximal de connexions embryonnaires par client ouvertes par l'intermédiaire de l'ASA, l'ASA empêche la connexion.
- **TCP Syn Cookie MSS** (MSS des témoins SYN TCP) — La taille maximale de segment (MSS) du serveur pour la génération de témoins SYN pour les connexions embryonnaires lors de l'atteinte de la limite de connexions embryonnaires, de 48 à 65 535. La valeur par défaut est 1380. Ce paramètre n'a de sens que si vous configurez **Embryonic Connections** ou **Per Client Embryonic Connections**.

Étape 4 Pour configurer les délais d'expiration de connexion, configurez les valeurs suivantes dans la zone TCP Timeout (Délai d'expiration TCP) :

- **Embryonic Connection Timeout** (Délai d'expiration de la connexion embryonnaire) — Le temps d'inactivité jusqu'à ce qu'un logement de connexion TCP embryonnaire (à moitié ouvert) soit libéré. Saisissez 0:0:0 pour désactiver le délai d'expiration pour la connexion. La valeur par défaut est de 30 secondes.
- **Half Closed Connection Timeout** (Délai d'expiration de la connexion à moitié fermée) —Le délai d'inactivité jusqu'à la fermeture d'une connexion à moitié fermée, entre 0:5:0 (pour 9.1(1) et antérieur) ou 0:0:30 (pour 9.1(2) et ultérieur) et 1 193:0:0. La valeur par défaut est 0:10:0. Les connexions à moitié fermées ne sont pas affectées par la détection des connexions inactives (DCD). De plus, l'ASA n'envoie pas de réinitialisation lorsqu'il interrompt les connexions à moitié fermées.
- **Idle Connection Timeout (Délai d'inactivité de la connexion)** — Le délai d'inactivité jusqu'à ce qu'un logement de connexion (de *n'importe quel* protocole, pas seulement TCP) soit libéré. Saisissez 0:0:0 pour désactiver le délai d'expiration pour la connexion. Cette durée doit être d'au moins 5 minutes. La valeur par défaut est de 1 heure.

- **Send reset to TCP endpoints before timeout** (Envoyer une réinitialisation aux terminaux TCP avant l'expiration) — Indique si l'ASA doit envoyer un message de réinitialisation TCP aux terminaux de la connexion avant de libérer le logement de connexion.
- **Dead Connection Detection (DCD)** (Détection des connexions inactives [DCD]) — Indique s'il faut activer Dead Connection Detection (DCD). Avant de faire expirer une connexion inactive, l'ASA sonde les hôtes finaux pour déterminer si la connexion est valide. Si les deux hôtes répondent, la connexion est conservée, sinon la connexion est libérée. Définissez le nombre maximal de tentatives (par défaut est 5, la plage est comprise entre 1 et 255) et l'intervalle de nouvelle tentative, qui est la période d'attente après chaque sonde DCD sans réponse avant d'envoyer une autre sonde (0:0:1 à 24:0:0, la valeur par défaut est 0:0:15). Lorsque vous utilisez le mode transparent du pare-feu, vous devez configurer des routes statiques pour les points terminaux. Vous ne pouvez pas configurer le DCD sur les connexions qui sont également déchargées, alors assurez-vous que le DCD et les classes de trafic de déchargement de flux ne se chevauchent pas.Utilisez la commande **show conn detail** pour suivre le nombre de sondes DCD envoyées par l'initiateur et le répondeur.

  Pour les systèmes qui fonctionnent dans une configuration de grappe ou haute disponibilité, nous vous recommandons de ne pas définir l'intervalle à moins d'une minute (0:1:0). Si la connexion doit être déplacée entre les systèmes, les modifications requises prennent plus de 30 secondes et la connexion peut être supprimée avant que la modification ne soit effectuée.

Étape 5 Pour désactiver les numéros de séquence aléatoires, décochez **Randomize Sequence Number** (Rendre le numéro de séquence aléatoire).

La distribution aléatoire de l'ISN de l'hôte protégé empêche un agresseur de prédire le prochain ISN pour une nouvelle connexion et de détourner potentiellement la nouvelle session.

Étape 6 Pour personnaliser le comportement du normaliseur TCP, cochez **Use TCP Map** (Utiliser une liste TCP) et choisissez une liste TCP existante dans la liste déroulante (le cas échéant), ou ajoutez-en une nouvelle en cliquant sur **New** (Nouveau).

Étape 7 Pour décrémenter le délai de vie (TTL) des paquets qui correspondent à la classe, cochez **Decrement time to live for a connection** (Décrémenter le temps de vie d'une connexion).

Le décrément de TTL est nécessaire pour que l'ASA s'affiche dans les routes de trace en tant que l'un des sauts. Vous devez également augmenter la limite de débit pour les messages ICMP Unreachable sur **Configuration > Device Management (Gestion des périphériques) > Management Access (Accès à la gestion) > ICMP**.

Étape 8 Pour activer le contournement de l'état TCP, cochez **TCP State Bypass** (Contournement de l'état TCP).

Étape 9 Pour activer le contournement de l'état SCTP, cochez **SCTP State Bypass** (Contournement de l'état SCTP).

Implémentez le contournement de l'état SCTP pour désactiver l'inspection dynamique SCTP. Pour en savoir plus, consultez Inspection dynamique SCTP, à la page 370.

Étape 10 (ASA sur le Châssis Firepower 4100/9300 , FXOS 1.1.3 ou version ultérieure, uniquement.) Pour activer le déchargement de flux, cochez **Flow Offload** (Déchargement de flux).

Le trafic éligible est déchargé vers un chemin ultra-rapide, où les flux sont commutés dans la carte réseau elle-même. Vous devez également activer le service de déchargement. Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Offload Engine (Moteur de déchargement)**.

Étape 11 Cliquez sur **OK** ou **Finish** (Terminer).

Configurer les options TCP

Vous pouvez configurer des options pour contrôler certains aspects du comportement TCP. Les paramètres par défaut pour ces réglages sont appropriés pour la plupart des réseaux.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Advanced** > **TCP Options** > **(Options TCP avancées)**.

Étape 2 Configurez le comportement de réinitialisation TCP par interface.

a) Sélectionnez l'interface que vous souhaitez modifier et cliquez sur **Edit** (Modifier).

b) Sélectionnez les options souhaitées :

- **Send reset reply for denied inbound TCP packets** (Envoyer une réponse de réinitialisation pour les paquets TCP entrants refusés). Envoyez des réinitialisations TCP pour toutes les sessions TCP entrantes qui tentent de transiter par l'ASA et sont refusées par l'ASA en fonction des listes d'accès ou des paramètres AAA. L'ASA envoie également des réinitialisations pour les paquets qui sont autorisés par une liste d'accès ou AAA, mais qui n'appartiennent pas à une connexion existante et sont refusés par le pare-feu dynamique. Le trafic entre les interfaces de même niveau de sécurité est également affecté. Lorsque cette option n'est pas activée, l'ASA rejette silencieusement les paquets refusés.

c) Cliquez sur **OK**.

Étape 3 Configurez les autres options TCP :

- **Send reset reply for denied outside TCP packets** (Envoyer une réponse de réinitialisation pour les paquets TCP externes refusés). Envoie des réinitialisations pour les paquets TCP qui se terminent à l'interface la moins sécurisée et qui sont refusés par l'ASA en fonction des listes d'accès ou des paramètres AAA. L'ASA envoie également des réinitialisations pour les paquets qui sont autorisés par une liste d'accès ou AAA, mais qui n'appartiennent pas à une connexion existante et qui sont refusés par le pare-feu dynamique. Lorsque cette option n'est pas activée, l'ASA rejette silencieusement les paquets des connexions refusées.

  Nous vous recommandons d'utiliser cette option avec l'interface PAT. Cela permet à l'ASA de terminer les connexions IDENT provenant d'un serveur SMTP ou FTP externe. La réinitialisation active de ces connexions évite le délai d'expiration de 30 secondes.

- **Force maximum segment size for TCP connection to be X bytes** (Forcer la taille de segment maximale de la connexion TCP à X octets). Définissez la taille de segment TCP maximale en octets, entre 48 et tout nombre maximal : Par défaut, la MTU est de 1380 octets. Vous pouvez désactiver cette fonctionnalité en mettant les octets à 0.

- **Force minimum segment size for TCP connection to be X bytes** (Forcer la taille de segment minimale de la connexion TCP à X octets). Remplace la taille maximale du segment pour qu'elle ne soit pas inférieure au nombre d'octets spécifié, entre 48 et 65 535 octets. Cette fonctionnalité est désactivée par défaut (définie sur 0).

- **Force TCP connection to linger in TIME_WAIT state for at least 15 seconds after TCP close-down** (Forcer la connexion TCP à persister dans l'état TIME_WAIT pendant au moins 15 secondes après la fermeture du TCP). Force chaque connexion TCP à persister dans un état TIME_WAIT raccourci d'au moins 15 secondes après la dernière séquence de fermeture TCP normale. Vous pouvez utiliser cette

fonctionnalité si une séquence de fin TCP par défaut de l'application d'hôte terminal est une fermeture simultanée.

- **TCP Maximum unprocessed segments (Nombre maximal de segments TCP non traités).** Vous pouvez définir le nombre maximal de segments TCP non traités, de 6 à 24. La valeur par défaut est 6. Si vous constatez que les téléphones SIP ne se connectent pas au gestionnaire d'appels, vous pouvez essayer d'augmenter le nombre maximal de segments TCP non traités.

Étape 4 Cliquez sur **Apply** (Appliquer).

Supervision des connexions

Utilisez les pages suivantes pour surveiller les connexions :

- Utilisez **Home (Accueil)** > **Firewall Dashboard** > **(Tableau de bord Pare-feu)**, puis consultez **Top Ten Protected Servers (Dix principaux serveurs protégés) dans le tableau de bord SYN Attack (Attaque SYN)** pour surveiller TCP Intercept. Cliquez sur le bouton **Detail** (Détails) pour afficher les données d'échantillonnage de l'historique. Le système ASA échantillonne le nombre d'attaques 30 fois au cours de l'intervalle de fréquence. Ainsi, pour la période par défaut de 30 minutes, des statistiques sont collectées toutes les 60 secondes.
- Utilisez **Monitoring (Surveillance)** > **Properties (Propriétés)** > **Connections (Connexions)** pour afficher les connexions actuelles.
- Utilisez **Monitoring (Surveillance)** > **Properties (Propriétés)** > **Connection Graphs (Graphiques de connexion)** pour surveiller les performances.

De plus, vous pouvez saisir les commandes suivantes à l'aide de **Tools (Outils)** > **Command Line Interface (Interface de ligne de commande)**.

- **show conn** [**detail**]

  Affiches des renseignements sur la connexion. Les informations détaillées utilisent des indicateurs pour indiquer des caractéristiques de connexion spéciales. Par exemple, l'indicateur « b » désigne un trafic soumis au contournement d'état TCP.

  Lorsque vous utilisez le mot-clé **detail**, vous pouvez voir des informations sur la sonde de détection de connexion inactive (DCD), qui indiquent la fréquence à laquelle la connexion a été sondée par l'initiateur et le répondeur. Par exemple, les détails d'une connexion compatible avec DCD ressembleraient à ce qui suit :

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828,
cluster sent/rcvd bytes 0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

- **show flow-offload** {**info** [**detail**] | **cpu** | **flow** [**count** | **detail**] | **statistics**}

Affiche des renseignements sur le déchargement de flux, notamment l'état général, l'utilisation du processeur pour le déchargement, le nombre et les détails des flux déchargés, ainsi que les statistiques des flux déchargés.

- **show service-policy**

  Affiche les statistiques de politique de service, y compris les statistiques de détection de connexion inactive (DCD).

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**]

  Affichez les 10 principaux serveurs protégés et soumis à des attaques. Le mot-clé **all** affiche les données d'historique de tous les serveurs suivis. Le mot-clé **detail** affiche les données d'échantillonnage de l'historique. L'ASA échantillonne le nombre d'attaques 30 fois au cours de l'intervalle de fréquence. Ainsi, pour la période par défaut de 30 minutes, des statistiques sont collectées toutes les 60 secondes.



Remarque Dans la configuration de l'ASA, les connexions embryonnaires (demandes de connexion qui n'ont pas encore terminé le processus de négociation en trois temps) sont fermées rapidement et ne sont pas synchronisées entre les périphériques actif et en veille. Cette conception garantit l'efficacité et la sécurité du système à haute disponibilité. Pour cette raison, une différence dans le nombre de connexions entre les deux ASA est normale.

Historique des paramètres de connexion

Nom de la caractéristique	Versions de plateforme	Description
contournement de l'état du TCP	8.2(1)	Cette fonctionnalité a été introduite. La commande suivante a été introduite : **set connection advanced-options tcp-state-bypass**.
Délai d'expiration de connexion pour tous les protocoles	8.2(2)	Le délai d'inactivité a été modifié pour s'appliquer à tous les protocoles, pas seulement au TCP. L'écran suivant a été modifié : Configuration > Firewall (Pare-feu) > Service Policies (Politiques de service) > Rule Actions (Actions de règle) > Connection Settings (Paramètres de connexion).
Délai d'expiration pour les connexions utilisant une route statique de sauvegarde	8.2(5)/8.4(2)	Lorsqu'il existe plusieurs routes statiques vers un réseau avec différentes métriques, l'ASA utilise celle ayant la meilleure métrique au moment de la création de la connexion. Si un meilleur routage devient disponible, ce délai d'expiration permet de fermer les connexions afin qu'une connexion puisse être rétablie pour utiliser le meilleur routage. La valeur par défaut est 0 (la connexion n'expire jamais). Pour profiter de cette fonctionnalité, modifiez le délai d'expiration pour une nouvelle valeur. Nous avons modifié l'écran suivant : Configuration > Firewall (Pare-feu) > Advanced (Avancé) > Global Timeouts (Délais d'expiration globaux).

Nom de la caractéristique	Versions de plateforme	Description
Délai d'expiration configurable pour PAT xlate	8.4(3)	Lorsqu'un PAT xlate expire (par défaut après 30 secondes) et que l'ASA réutilise le port pour une nouvelle traduction, certains routeurs en amont peuvent rejeter la nouvelle connexion, car la connexion précédente peut toujours être ouverte sur le périphérique en amont. Le délai d'expiration de PAT xlate est maintenant configurable, à une valeur comprise entre 30 secondes et 5 minutes. Nous avons modifié l'écran suivant : Configuration > Firewall (Pare-feu) > Advanced (Avancé) > Global Timeouts (Délais d'expiration globaux). *Cette fonctionnalité n'est pas disponible dans les versions 8.5(1) ou 8.6(1).*
Augmentation des limites de connexion maximales pour les règles de politique de service	9.0(1)	Le nombre maximal de connexions pour les règles de politique de service a été augmenté de 65 535 à 2 000 000. Nous avons modifié l'écran suivant : Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service) > Connection Settings (Paramètres de connexion).
Réduction de la valeur minimale du délai d'expiration à moitié fermé à 30 secondes	9.1(2)	La valeur minimale du délai d'expiration à moitié fermé pour le délai d'expiration global et le délai d'expiration de connexion a été réduite de 5 minutes à 30 secondes pour fournir une meilleure protection DoS. Nous avons modifié les écrans suivants : Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service) > Connection Settings (Paramètres de connexion); Configuration (Configuration) > Firewall (Pare-feu) > Advanced (Avancé) > Global Timeouts (Délais d'expiration globaux).
Délai d'expiration de la connexion pour la convergence des routes.	9.4(3) 9.6(2)	Vous pouvez maintenant configurer la durée pendant laquelle le système doit maintenir une connexion lorsque le routage utilisé par la connexion n'existe plus ou est inactif. Si le routage ne devient pas actif au cours de cette période d'attente, la connexion est libérée. Vous pouvez réduire le délai de maintien pour accélérer la convergence des routes. Cependant, la valeur par défaut de 15 secondes est appropriée pour la plupart des réseaux afin d'éviter l'oscillation des routes. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Global Timeouts (Délais d'expiration globaux)**.
Délai d'inactivité SCTP et contournement de l'état SCTP	9.5(2)	Vous pouvez définir un délai d'inactivité pour les connexions SCTP. Vous pouvez également activer le contournement de l'état SCTP pour désactiver l'inspection avec état SCTP sur une classe de trafic. Nous avons modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Global Timeouts (Délais d'expiration globaux)** ; assistant **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**, onglet **Connection Settings (Paramètres de connexion)**.

Nom de la caractéristique	Versions de plateforme	Description
Décharge de flux pour l'ASA sur le Firepower 9300	9.5(2.1)	Vous pouvez identifier les flux qui doivent être déchargés de l'ASA et commutés directement dans la carte réseau (sur le Firepower 9300). Cela offre des performances améliorées pour les flux de données volumineux dans les centres de données. Cette fonctionnalité nécessite FXOS 1.1.3. Nous avons ajouté ou modifié les écrans suivants : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Offload Engine (Moteur de déchargement)**, l'onglet **Rule Actions (Actions de règles)** > **Connection Settings (Paramètres de connexion)** lors de l'ajout ou de la modification des règles sous **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**.
Prise en charge du déchargement de flux pour l'ASA sur le Firepower 4100.	9.6(1)	Vous pouvez identifier les flux qui doivent être déchargés de l'ASA et commutés directement dans la carte réseau pour le Firepower 4100. Cette fonctionnalité requiert FXOS 1.1.4. Il n'y a aucune nouvelle commande ni écran ASDM pour cette fonctionnalité.
Prise en charge du déchargement de flux pour les connexions de multidiffusion en mode transparent.	9.6(2)	Vous pouvez désormais décharger les connexions de multidiffusion à basculer directement dans la carte d'interface réseau sur les périphériques Firepower 4100 et 9300 en mode transparent. Le déchargement de multidiffusion est disponible pour les groupes de ponts qui contiennent deux et seulement deux interfaces. Il n'y a aucune nouvelle commande ni écran ASDM pour cette fonctionnalité.

Nom de la caractéristique	Versions de plateforme	Description
Modifications dans la gestion des options TCP.	9.6(2)	Vous pouvez désormais spécifier des actions pour les options TCP MSS et MD5 dans l'en-tête TCP d'un paquet lors de la configuration d'une carte TCP. De plus, la gestion par défaut des options MSS, horodatage, taille de fenêtre et accusé de réception sélectif a été modifiée. Auparavant, ces options étaient autorisées, même s'il y avait plus d'une option d'un type donné dans l'en-tête. Désormais, les paquets sont abandonnés par défaut s'ils contiennent plusieurs options d'un type donné. Par exemple, précédemment, un paquet avec 2 options d'horodatage était autorisé, il sera maintenant abandonné. Vous pouvez configurer une carte TCP pour autoriser plusieurs options du même type pour MD5, MSS, accusé de réception sélectif, horodatage et taille de fenêtre. Pour l'option MD5, la valeur par défaut précédente était d'effacer l'option, tandis que la valeur par défaut est maintenant de l'autoriser. Vous pouvez également abandonner les paquets contenant l'option MD5. Pour l'option MSS, vous pouvez définir la taille de segment maximum dans la carte TCP (par classe de trafic). La valeur par défaut pour toutes les autres options TCP reste la même : elles sont effacées. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Objects (Objets)** > **TCP Maps (Cartes TCP)** Add/Edit dialog box (Boîte de dialogue Ajouter/modifier).
Délai d'expiration de route obsolète pour les protocoles de passerelle intérieure	9.7(1)	Vous pouvez maintenant configurer le délai d'expiration pour supprimer des routes obsolètes pour les protocoles de passerelle intérieure tels que OSPF. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Global Timeouts (Délais d'expiration globaux)**.
Délai d'expiration global pour les erreurs ICMP	9.8(1)	Vous pouvez maintenant définir le délai d'inactivité avant que l'ASA ne supprime une connexion ICMP après avoir reçu un paquet de réponse d'écho ICMP. Lorsque ce délai d'expiration est désactivé (par défaut) et que vous activez l'inspection ICMP, l'ASA supprime la connexion ICMP dès qu'une réponse d'écho est reçue; ainsi, toutes les erreurs ICMP générées pour la connexion (maintenant fermée) sont abandonnées. Ce délai d'expiration retarde la suppression des connexions ICMP afin que vous puissiez recevoir des erreurs ICMP importantes. Nous avons modifié l'écran suivant : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **Global Timeouts (Délais d'expiration globaux)**.
Délai d'inactivité par défaut pour le contournement d'état TCP	9.10(1)	Le délai d'inactivité par défaut pour les connexions de contournement d'état TCP est désormais de 2 minutes au lieu de 1 heure.

Nom de la caractéristique	Versions de plateforme	Description
Informations sur l'initiateur et le répondeur pour la détection des connexions inactives (DCD) et prise en charge du DCD dans une grappe.	9.13(1)	Si vous activez la détection des connexions inactives (DCD), vous pouvez utiliser la commande **show conn detail** pour obtenir des informations sur l'initiateur et le répondeur. La détection des connexions inactives vous permet de maintenir une connexion inactive, et la sortie **show conn** vous indique la fréquence à laquelle les points terminaux ont été sondés. En outre, DCD est désormais pris en charge dans une grappe. Nouveaux écrans ou modifiés : aucun.
Configurer la taille maximale de segment (MSS) pour les connexions amorces.	9.16(1)	Vous pouvez configurer une politique de service afin de définir la taille maximale de segment (MSS) du serveur pour la génération de témoins SYN pour les connexions amorces lors de l'atteinte de la limite de connexions amorces. Cela est important pour les politiques de service dans lesquelles vous définissez également des nombres maximums de connexions amorces. Écrans nouveaux ou modifiés : **Paramètres de connexion** de l'assistant d'ajout ou de modification d'une politique de service.
Configurer le délai d'inactivité global de l'initialisation de l'appel SIP	9.16(x)	Vous pouvez configurer le délai d'inactivité après lequel une session SIP dans l'état d'appel Call_Init (après la réception du message d'invitation initial) sera supprimée, c'est-à-dire lorsqu'aucune réponse n'est reçue, entre 0:0:1 et 1193:0:0. La valeur par défaut est de 32 secondes (0:00:32).
Décharge de flux IPsec.	9.18(1)	Sur la Secure Firewall 3100, les flux IPsec sont déchargés par défaut. Après la configuration initiale d'une association de sécurité (SA), d'un VPN de site à site ou d'un VPN d'accès à distance IPsec, les connexions IPsec sont déchargées vers le FPGA (field programmable gate RAID) dans le périphérique, ce qui devrait améliorer les performances du périphérique. Écrans ajoutés ou modifiés : **Configuration** > **Firewall (Pare-feu)** > **Advanced (Avancé)** > **IPsec Offload (Déchargement IPsec)**



CHAPITRE 17

Qualité de service

Avez-vous déjà pris part à un appel téléphonique longue distance nécessitant une connexion par satellite? La conversation peut être interrompue par de brèves pauses, mais perceptibles, à des intervalles irréguliers. Ces pauses correspondent au délai, appelé latence, entre l'envoi et la réception des paquets sur le réseau. Certains trafics réseau, comme la voix et la vidéo, ne peuvent tolérer des temps de latence élevés. La qualité de service (QoS) est une fonctionnalité qui vous permet de donner la priorité au trafic critique, d'empêcher la saturation de la bande passante et de gérer les goulots d'étranglement du réseau pour éviter les pertes de paquets.

Les rubriques suivantes décrivent comment appliquer des politiques QoS.

- À propos de QoS, à la page 441
- Lignes directrices pour la QoS, à la page 443
- Configurer QoS, à la page 444
- Surveiller la QoS, à la page 448
- Historique QoS, à la page 450

À propos de QoS

Vous devez considérer que dans un environnement réseau en constante évolution, la QoS n'est pas un déploiement unique, mais un élément continu et essentiel de la conception du réseau.

Cette section décrit les caractéristiques de QoS disponibles sur l'ASA.

Fonctionnalités QoS prises en charge

L'ASA prend en charge les fonctionnalités QoS suivantes :

- Régulation : pour éviter que le trafic classé ne monopolise la bande passante du réseau, vous pouvez limiter la bande passante maximale utilisée par classe. Consultez Police, à la page 442 pour de plus amples renseignements.
- Mise en file prioritaire : pour le trafic critique qui ne peut pas tolérer la latence, comme la voix sur IP (VoIP), vous pouvez identifier le trafic pour la mise en file d'attente à faible latence (LLQ) afin qu'il soit toujours transmis avant les autres trafics. Consultez File d'attente prioritaire, à la page 442.

Qu'est-ce qu'un compartiment de jetons?

Un compartiment à jetons est utilisé pour gérer un mécanisme qui régule les données dans un flux, par exemple un contrôleur de trafic. Un compartiment de jetons n'a pas de politique de suppression ou de priorité. u contraire, un compartiment à jetons rejette les jetons et laisse au flux le soin de gérer sa file d'attente de transmission si le flux surcharge le régulateur.

Un compartiment à jetons est une définition formelle d'un débit de transfert. Il comporte trois composants : une taille de rafale, un débit moyen et un intervalle de temps. Bien que le débit moyen soit généralement représenté sous forme de bits par seconde, deux valeurs peuvent être dérivées de la troisième par la relation indiquée comme suit :

débit moyen = taille de rafale/intervalle de temps

Voici quelques définitions de ces termes :

- Débit moyen : également appelé débit d'information validé (CIR), il spécifie la quantité de données qui peut être envoyée ou transmise par unité de temps en moyenne.
- Taille de la rafale : également appelée taille de rafale validée (Bc), elle spécifie en octets par rafale la quantité du trafic qui peut être envoyée dans une unité de temps donnée pour ne pas créer de problèmes de planification.
- Intervalle de temps : également appelé intervalle de mesure, il spécifie le quantum de temps en secondes par rafale.

Dans la métaphore du compartiment à jetons, les jetons sont placés dans le compartiment à un certain débit. Le compartiment lui-même a une capacité spécifiée. Si le compartiment se remplit à sa capacité, les jetons nouvellement entrants sont rejetés. Chaque jeton est l'autorisation pour la source d'envoyer un certain nombre de bits dans le réseau. Pour envoyer un paquet, le régulateur doit supprimer du compartiment un nombre de jetons égal en représentation à la taille du paquet.

S'il n'y a pas assez de jetons dans le compartiment pour envoyer un paquet, le paquet attend jusqu'à ce que le paquet soit rejeté ou marqué. Si le compartiment est déjà plein de jetons, les jetons entrants débordent et ne sont pas disponibles pour les futurs paquets. Ainsi, à tout moment, la plus grande rafale qu'une source peut envoyer dans le réseau est à peu près proportionnelle à la taille du compartiment.

Police

La régulation est un moyen de s'assurer que le trafic ne dépasse pas le débit maximal (en bits/seconde) que vous avez configuré, garantissant ainsi qu'aucune classe de trafic ne peut prendre le contrôle de toute la ressource. Lorsque le trafic dépasse le débit maximal, l'ASA abandonne le trafic excédentaire. La régulation définit également la plus grande rafale de trafic autorisée.

File d'attente prioritaire

La mise en file d'attente prioritaire LLQ vous permet de hiérarchiser certains flux de trafic (comme le trafic sensible à la latence comme la voix et la vidéo) avant d'autres trafics. La mise en file d'attente prioritaire utilise une file d'attente de priorité LLQ sur une interface (voir Configurer la file d'attente prioritaire pour une interface, à la page 446), tandis que tout autre trafic passe dans la file d'attente « au mieux ». Comme les files d'attente ne sont pas de capacité infinie, elles peuvent atteindre leur capacité maximale et déborder. Lorsqu'une file d'attente est remplie, tous les paquets supplémentaires ne peuvent pas entrer dans la file d'attente et sont abandonnés. C'est ce qu'on appelle *abandon de file d'attente*. Pour éviter que la file d'attente

ne se remplisse, vous pouvez augmenter la taille du tampon de file d'attente. Vous pouvez également affiner le nombre maximal de paquets autorisés dans la file d'attente de transmission. Ces options vous permettent de contrôler la latence et la robustesse de la mise en file d'attente prioritaire. Les paquets dans la file d'attente LLQ sont toujours transmis avant les paquets dans la file d'attente au mieux.

Comment les fonctionnalités QoS interagissent

Vous pouvez configurer chacune des fonctionnalités QoS seule si vous le souhaitez pour l'ASA. Souvent, cependant, vous configurez plusieurs fonctionnalités QoS sur l'ASA afin de pouvoir hiérarchiser certains trafics, par exemple, et empêcher d'autres trafics de provoquer des problèmes de bande passante. Vous pouvez configurer :

Mise en file prioritaire (pour un trafic spécifique) + régulation (pour le reste du trafic).

Vous ne pouvez pas configurer la mise en file d'attente prioritaire et la régulation pour le même ensemble de trafic.

Préservation DSCP (DiffServ)

Les marquages DSCP (DiffServ) sont conservés sur tout le trafic passant par l'ASA. L'ASA ne marque/remarque pas localement le trafic classé. Par exemple, vous pourriez désactiver les bits DSCP de transfert accéléré (EF) de chaque paquet pour déterminer s'il nécessite un traitement « priorité » et faire en sorte que l'ASA dirige ces paquets vers le LLQ.

Lignes directrices pour la QoS

Directives relatives au mode contextuel

Pris en charge en mode contexte unique uniquement Ne prend pas en charge le mode contexte multiple.

Directives sur le mode pare-feu

Pris en charge uniquement en mode de pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.

Directives IPv6

Ne prend pas en charge IPv6.

Directives et limites additionnelles

- La QoS est appliquée de manière unidirectionnelle; seul le trafic qui entre (ou en sort, selon la fonctionnalité QoS) de l'interface à laquelle vous appliquez la liste des politiques est touché.
- Pour le trafic prioritaire, vous ne pouvez pas utiliser la carte de trafic **par défaut**.
- Pour la mise en file d'attente prioritaire, la file d'attente prioritaire doit être configurée pour une interface physique.
- Pour la régulation, le trafic vers le boîtier n'est pas pris en charge.
- Pour la régulation, le trafic vers et depuis un tunnel VPN contourne la régulation d'interface.

- Pour la régulation, lorsque vous faites correspondre une carte de trafic de groupe de tunnels, seule la régulation sortante est prise en charge.

Configurer QoS

Utilisez la séquence suivante pour mettre en œuvre la QoS sur l'ASA.

Procédure

Étape 1 Déterminer les limites de la file d'attente et de l'anneau TX pour une file d'attente prioritaire, à la page 444.

Étape 2 Configurer la file d'attente prioritaire pour une interface, à la page 446.

Étape 3 Configurer une règle de service pour la mise en file d'attente prioritaire et la régulation, à la page 447.

Déterminer les limites de la file d'attente et de l'anneau TX pour une file d'attente prioritaire

Utilisez les feuilles de travail suivantes pour déterminer les limites de la file d'attente prioritaire et de l'anneau TX.

Feuille de travail sur la limite de la file d'attente

La feuille de travail suivante montre comment calculer la taille de la file d'attente prioritaire. Comme les files d'attente ne sont pas de taille infinie, elles peuvent se remplir et déborder. Lorsqu'une file d'attente est remplie, tous les paquets supplémentaires ne peuvent pas entrer dans la file d'attente et sont abandonnés (appelés *rejet de file d'attente*). Pour éviter que la file d'attente ne soit remplie, vous pouvez ajuster la taille du tampon de file d'attente en fonction de Configurer la file d'attente prioritaire pour une interface, à la page 446.

Conseils sur la feuille de travail :

- Bande passante sortante : par exemple, une connexion DSL peut avoir une vitesse de liaison ascendante de 768 kbit/s. Vérifiez auprès de votre fournisseur.
- Taille moyenne des paquets : déterminez cette valeur à partir d'un codec ou d'une taille d'échantillonnage. Par exemple, pour le protocole VoIP sur VPN, vous pouvez utiliser 160 octets. Nous vous recommandons d'utiliser 256 octets si vous ne savez pas quelle taille utiliser.
- Délai : le délai dépend de votre application. Par exemple, le délai maximal conseillé pour le protocole VoIP est de 200 ms. Nous vous recommandons d'utiliser 500 ms si vous ne savez pas quel délai utiliser.

Tableau 13 : Feuille de travail sur la limite de la file d'attente

1	_____ *Bande passante sortante (Mbit/s ou kbit/s)*	Mbit/s	x	**125**	=	_____ *Nombre d'octets/ms*		
		kbit/s	x	**0,125**	=	_____ *Nombre d'octets/ms*		
2	_____ *Nombre d'octets/ms de l'étape 1*		÷	_____ *Taille moyenne des paquets (octets)*	x	_____ *Retard (ms)*	=	_____ *Limite de la file d'attente (Nombre de paquets)*

Feuille de calcul des limites de l'anneau TX

La feuille de travail suivante montre comment calculer la limite de la boucle TX. Cette limite détermine le nombre maximal de paquets autorisés dans le pilote de transmission Ethernet avant que le pilote ne repousse les files d'attente sur l'interface pour leur permettre de mettre les paquets en mémoire tampon jusqu'à ce que la congestion se résorbe. Ce paramètre garantit que l'anneau de transmission matériel impose une quantité limitée de latence supplémentaire pour un paquet de priorité élevée.

Conseils sur la feuille de travail :

- Bande passante sortante : par exemple, le protocole DSL peut avoir une vitesse de liaison ascendante de 768 kbit/s. Vérifiez auprès de votre fournisseur.
- Taille maximale du paquet : en général, la taille maximale est de 1 538 octets ou de 1 542 octets pour Ethernet étiqueté. Si vous autorisez les trames étendues (si elles sont prises en charge pour votre plateforme), la taille des paquets pourrait être plus grande.
- Délai : le délai dépend de votre application. Par exemple, pour contrôler la gigue pour le VoIP, vous devez utiliser 20 ms.

Tableau 14 : Feuille de travail sur la limite de la boucle TX

1	_____ *Bande passante sortante (Mbit/s ou kbit/s)*	Mbit/s	x	**125**	=	_____ *Nombre d'octets/ms*		
		kbit/s	x	**0,125**	=	_____ *Nombre d'octets/ms*		
2	_____ *Nombre d'octets/ms de l'étape 1*		÷	_____ *Taille maximale des paquets (octets)*	x	_____ *Retard (ms)*	=	_____ *Limite de l'anneau TX (nombre de paquets)*

Configurer la file d'attente prioritaire pour une interface

Si vous activez la mise en file d'attente prioritaire pour le trafic sur une interface physique, vous devez également créer la file d'attente prioritaire sur chaque interface. Chaque interface physique utilise deux files d'attente : l'une pour le trafic prioritaire et l'autre pour tout autre trafic. Pour l'autre trafic, vous pouvez éventuellement configurer la régulation.

Procédure

Étape 1 Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced** > **(Avancé)** > **Priority Queue** (File d'attente prioritaire), puis cliquez sur **Add** (Ajouter).

Étape 2 Configurez les options suivantes :

- **Interface** : nom de l'interface physique sur laquelle vous souhaitez activer la file d'attente prioritaire ou, pour l'ASASM, le nom de l'interface VLAN.
- **Queue Limit** (Limite de file d'attente) : nombre moyen de paquets de 256 octets que l'interface précisée peut transmettre dans un intervalle de 500 ms. La plage est comprise entre 0 et 2048, et 2048 est la valeur par défaut.

  Un paquet qui reste plus de 500 ms dans un nœud de réseau peut déclencher un délai d'expiration dans l'application de bout en bout. Un tel paquet peut être rejeté dans chaque nœud de réseau.

  Comme les files d'attente ne sont pas de taille infinie, elles peuvent se remplir et déborder. Lorsqu'une file d'attente est remplie, tous les paquets supplémentaires ne peuvent pas entrer dans la file d'attente et sont abandonnés (appelés *« rejet de file d'attente »*). Pour éviter que la file d'attente ne soit remplie, vous pouvez utiliser cette option pour augmenter la taille du tampon de file d'attente.

  La limite supérieure de la plage de valeurs pour cette option est déterminée dynamiquement au moment de l'exécution. Les facteurs clés sont la mémoire nécessaire pour prendre en charge les files d'attente et la mémoire disponible sur le périphérique.

  La valeur Queue Limit (Limite de file d'attente) que vous spécifiez affecte à la fois la file d'attente à faible latence de priorité plus élevée et la file d'attente d'effort optimal.
- **Transmission Ring Limit** (Limite de l'anneau de transmission) : profondeur des files d'attente prioritaires, soit le nombre maximal de paquets de 1 550 octets que l'interface précisée peut transmettre dans un intervalle de 10 ms. La plage est comprise entre 3 et 511, et 511 est la valeur par défaut.

  Ce paramètre garantit que l'anneau de transmission matériel n'imposera pas plus de 10 ms de latence supplémentaire pour un paquet de priorité élevée.

  Cette option définit le nombre maximal de paquets à faible latence ou de priorité normale autorisés dans le pilote de transmission Ethernet avant que le pilote ne renvoie les paquets vers les files d'attente de l'interface pour leur mise en mémoire tampon jusqu'à ce que la congestion se résorbe.

  La limite supérieure de la plage de valeurs est déterminée dynamiquement au moment de l'exécution. Les facteurs clés sont la mémoire nécessaire pour prendre en charge les files d'attente et la mémoire disponible sur le périphérique.

  La valeur Transmission Ring Limit (Limite de l'anneau de transmission) que vous spécifiez affecte à la fois la file d'attente à faible latence de priorité plus élevée et la file d'attente d'effort optimal.

Étape 3 Cliquez sur **OK**, puis sur **Apply**(appliquer).

Configurer une règle de service pour la mise en file d'attente prioritaire et la régulation

Vous pouvez configurer la mise en file d'attente prioritaire et la régulation pour différentes cartes de trafic dans la même liste des politiques. Consultez Comment les fonctionnalités QoS interagissent, à la page 443 pour obtenir des renseignements sur les configurations QoS valides.

Avant de commencer

- Vous ne pouvez pas utiliser la carte de trafic **class-default** pour le trafic prioritaire.
- Pour la régulation, le trafic vers le boîtier n'est pas pris en charge.
- Pour la régulation, le trafic vers et depuis un tunnel VPN contourne la régulation d'interface.
- Pour la régulation, lorsque vous faites correspondre une carte de trafic de groupe de tunnels, seule la régulation sortante est prise en charge.
- Pour le trafic prioritaire, identifiez uniquement le trafic sensible à la latence.
- Pour réguler le trafic, vous pouvez choisir de réguler tout autre trafic ou de limiter le trafic à certains types.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy Rules (Règles de politique de service)**, et ouvrez une règle.

Vous pouvez configurer QoS dans le cadre d'une nouvelle règle de politique de service ou modifier une politique de service existante.

Étape 2 Poursuivez dans l'assistant jusqu'à la page Rules (Règles), en sélectionnant l'interface (ou globale) et les critères de correspondance du trafic en cours de route.

Pour réguler le trafic, vous pouvez choisir de réguler tout le trafic que vous ne priorisez pas, ou vous pouvez limiter le trafic à certains types.

Astuces
Si vous utilisez une liste de contrôle d'accès pour la correspondance du trafic, la régulation est appliquée dans la direction spécifiée dans la liste de contrôle d'accès uniquement. C'est-à-dire que le trafic allant de la source à la destination est régulé, mais pas l'inverse.

Étape 3 Dans la boîte de dialogue Rule Actions (Actions de règle), cliquez sur l'onglet **QoS** (QoS).

Étape 4 .Sélectionnez **Enable priority for this flow** (Activer la priorité pour ce flux).

Si cette règle de politique de service s'applique à une interface individuelle, ASDM crée automatiquement la file d'attente prioritaire pour l'interface (Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > Priority Queue (File d'attente prioritaire) ; pour plus d'informations, consultez Configurer

la file d'attente prioritaire pour une interface, à la page 446). Si cette règle s'applique à la politique globale, vous devez ajouter manuellement la file d'attente prioritaire à une ou plusieurs interfaces *avant* de configurer la règle de politique de service.

Étape 5 Sélectionnez **Enable policing** (Activer la régulation), puis cochez les cases **Input policing** (Régulation en entrée) ou **Output policing** (Régulation en sortie) (ou les deux) pour activer le type de régulation du trafic spécifié. Pour chaque type de régulation de trafic, configurez les options suivantes :

- **conform-rate** : limite de débit pour cette classe de trafic, de 8 000 à 2 000 000 000 bits par seconde. Par exemple, pour limiter le trafic à 5 Mbit/s, saisissez 5 000 000.
- **Conform Action** (Action conforme) : action à prendre lorsque le trafic est inférieur au débit de régulation et à la taille de rafale. Vous pouvez abandonner ou transmettre le trafic. La valeur par défaut est de transmettre le trafic.
- **Exceed Action** (Action de dépassement) : action à prendre lorsque le trafic dépasse le débit de régulation et la taille de rafale. Vous pouvez abandonner ou transmettre des paquets qui dépassent le débit de régulation et la taille de rafale. La valeur par défaut est d'abandonner les paquets en excédent.
- **Burst Rate** (Débit de rafale) : nombre maximal d'octets instantanés autorisés dans une rafale soutenue avant de passer à la valeur de débit conforme, entre 1 000 et 512 000 000 octets. Calculez la taille de rafale comme 1/32 du débit conforme en octets. Par exemple, la taille de rafale pour un débit de 5 Mbit/s serait de 156 250. La valeur par défaut est de 1 500, mais le système peut recalculer toute valeur que vous saisissez au besoin.

Étape 6 Cliquez sur **Finish** (Terminer), puis sur **Apply** (Appliquer).

Surveiller la QoS

Les rubriques suivantes expliquent comment surveiller la QoS.

Pour surveiller la QoS dans ASDM, vous pouvez entrer des commandes dans l'outil de l'interface de ligne de commande.

Statistiques de régulation QoS

Pour afficher les statistiques QoS pour la régulation du trafic, utilisez la commande **show service-policy police**.

```
hostname# show service-policy police

Global policy:
 Service-policy: global_fw_policy

Interface outside:
 Service-policy: qos
  Class-map: browse
   police Interface outside:
    cir 56000 bps, bc 10500 bytes
    conformed 10065 packets, 12621510 bytes; actions: transmit
    exceeded 499 packets, 625146 bytes; actions: drop
    conformed 5600 bps, exceed 5016 bps
  Class-map: cmap2
```

```
  police Interface outside:
   cir 200000 bps, bc 37500 bytes
   conformed 17179 packets, 20614800 bytes; actions: transmit
   exceeded 617 packets, 770718 bytes; actions: drop
   conformed 198785 bps, exceed 2303 bps
```

Statistiques de priorité QoS

Pour afficher les statistiques des politiques de service qui mettent en œuvre la commande **priority**, utilisez la commande **show service-policy priority**.

```
hostname# show service-policy priority
Global policy:
 Service-policy: global_fw_policy
Interface outside:
 Service-policy: qos
  Class-map: TG1-voice
   Priority:
    Interface outside: aggregate drop 0, aggregate transmit 9383
```

« Aggregate drop » (abandon agrégé) désigne l'abandon agrégé dans cette interface; « Aggregate transmit » (transmission agrégée) désigne le nombre agrégé de paquets transmis dans cette interface.

Statistiques de file d'attente prioritaire QoS

Pour afficher les statistiques de file d'attente prioritaire pour une interface, utilisez la commande **show priority-queue statistics**. Les résultats affichent les statistiques de la file d'attente best-effort (BE) et de la file d'attente à faible latence (LLQ). L'exemple suivant montre l'utilisation de la commande **show priority-queue statistics** pour l'interface nommée test.

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type         = BE
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0

Queue Type         = LLQ
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0
hostname#
```

Dans ce rapport statistique :

- « Paquets abandonnés » désigne le nombre total de paquets qui ont été abandonnés dans cette file d'attente.
- « Paquets transmis » désigne le nombre total de paquets qui ont été transmis dans cette file d'attente.

- « Paquets mis en file d'attente » désigne le nombre total de paquets qui ont été mis en file d'attente dans cette file d'attente.
- La « Longueur actuelle de la file d'attente » désigne la profondeur actuelle de cette file d'attente.
- La « Longueur maximale de la file d'attente » désigne la profondeur maximale jamais enregistrée dans cette file d'attente.

Historique QoS

Nom de la caractéristique	Versions de plateforme	Description
Mise en file et régulation prioritaires	7.0(1)	Nous avons introduit la mise en file d'attente prioritaire et la régulation QoS. Nous avons introduit les écrans suivants : Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > Priority Queue (File d'attente prioritaire) Configuration (Configuration) > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service)
Mise en forme et mise en file d'attente prioritaire hiérarchique	7.2(4)/8.0(4)	Nous avons lancé la mise en forme QoS et la mise en file prioritaire hiérarchique. Nous avons modifié l'écran suivant : Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service).
Prise en charge de dix Gigabit Ethernet pour une file d'attente de priorité standard sur l'ASA 5585-X	8.2(3)/8.4(1)	Nous avons ajouté la prise en charge d'une file d'attente prioritaire standard sur les interfaces Ten Gigabit Ethernet pour l'ASA 5585-X.



CHAPITRE 18

Détection des menaces

Les rubriques suivantes décrivent comment configurer les statistiques de détection des menaces et l'analyse de la détection des menaces.

- Détection des menaces, à la page 451
- Lignes directrices pour la détection des menaces, à la page 454
- Paramètres par défaut pour la détection des menaces, à la page 454
- Configurer la détection des menaces, à la page 455
- Surveillance de la détection des menaces, à la page 458
- Historique de la détection des menaces, à la page 459

Détection des menaces

La détection des menaces sur l'ASA fournit une défense de première ligne contre les attaques. La détection des menaces fonctionne aux couches 3 et 4 pour développer une référence pour le trafic sur le périphérique, en analysant les statistiques sur les pertes de paquets et en accumulant les rapports « top » en fonction des modèles de trafic. En comparaison, un module qui fournit des services IPS ou IPS de nouvelle génération identifie et atténue les vecteurs d'attaque jusqu'à la couche 7 sur le trafic autorisé par l'ASA, et ne peut pas voir le trafic déjà abandonné par l'ASA. Ainsi, la détection des menaces et l'IPS peuvent fonctionner ensemble pour fournir une défense contre les menaces plus complète.

La détection des menaces comprend les éléments suivants :

- Différents niveaux de collecte de statistiques pour diverses menaces.

  Les statistiques de détection des menaces peuvent vous aider à gérer les menaces qui pèsent sur votre ASA; par exemple, si vous activez la détection des menaces par analyse, l'affichage des statistiques peut vous aider à analyser la menace. Vous pouvez configurer deux types de statistiques de détection des menaces :

  - Statistiques de détection des menaces de base : comprennent des informations sur l'activité des attaques pour le système dans son ensemble. Les statistiques de détection des menaces de base sont activées par défaut et n'ont aucune incidence sur les performances. Consultez Statistiques de détection des menaces de base, à la page 452.

  - Statistiques avancées de détection des menaces : permettent de suivre l'activité au niveau de l'objet, afin que l'ASA puisse signaler l'activité des hôtes, des ports, des protocoles ou des ACL individuels. Les statistiques de détection avancée des menaces peuvent avoir un impact majeur sur les

performances, en fonction des statistiques recueillies, de sorte que seules les statistiques d'ACL sont activées par défaut. Consultez Statistiques de détection avancée des menaces, à la page 452.

- La fonction de détection des menaces par analyse détermine quand un hôte effectue une analyse. Vous pouvez éventuellement bloquer tout hôte identifié comme constituant une menace d'analyse. Consultez Détection des menaces par analyse, à la page 453.

Statistiques de détection des menaces de base

À l'aide des statistiques de détection des menaces de base, l'ASA surveille le taux d'abandons de paquets et les événements de sécurité pour les raisons suivantes :

- Déni par les listes de contrôle d'accès.
- Mauvais format de paquet (comme invalid-ip-header ou invalid-tcp-hdr-length).
- Limites de connexion dépassées (limites de ressources à l'échelle du système et limites définies dans la configuration).
- Attaque DoS détectée (comme un SPI non valide, échec de vérification de pare-feu avec état).
- Échec des vérifications de base du pare-feu. Cette option est un débit combiné qui inclut tous les abandons de paquets liés au pare-feu dans cette liste. Il n'inclut pas les abandons non liés au pare-feu, tels que la surcharge d'interface, les échecs de paquets lors de l'inspection de l'application et les attaques par analyse détectées.
- Paquets ICMP suspects détectés.
- Paquets ayant échoué à l'inspection de l'application.
- Surcharge de l'interface.
- Attaque par analyse détectée. Cette option surveille les attaques par analyse; par exemple, le premier paquet TCP n'est pas un paquet SYN, ou la connexion TCP a échoué dans l'établissement de liaison à 3 voies. La détection des menaces d'analyse complète prend ces informations de taux d'attaque d'analyse et agit en classant les hôtes comme agresseurs et en les contournant automatiquement, par exemple.
- Session incomplète détectée, comme l'attaque TCP SYN détectée ou la session UDP sans retour de données détectée.

Lorsque l'ASA détecte une menace, il envoie immédiatement un message de journal système (733100). L'ASA suit deux types de taux : le taux moyen d'événements sur un intervalle, et le taux d'événements en rafale sur un intervalle de rafale plus court. L'intervalle de débit en rafale est de 1/30 de l'intervalle de débit moyen ou de 10 secondes, selon le plus élevé des deux. Pour chaque événement reçu, l'ASA vérifie les limites de débit moyen et de rafale; si les deux débits sont dépassés, l'ASA envoie deux messages système distincts, avec un maximum d'un message pour chaque type de débit par période de rafale.

La détection des menaces de base affecte les performances uniquement en cas d'abandon ou de menace potentielle; même dans ce scénario, l'incidence sur les performances est négligeable.

Statistiques de détection avancée des menaces

Les statistiques de détection avancée des menaces affichent les débits de trafic autorisés et abandonnés pour les objets individuels tels que les hôtes, les ports, les protocoles ou les listes de contrôle d'accès.

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

Détection des menaces par analyse

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

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

Si le taux de menace d'analyse est dépassé, l'ASA envoie un message syslog (733101) et bloque éventuellement l'agresseur. L'ASA suit deux types de taux : le taux moyen d'événements sur un intervalle, et le taux d'événements en rafale sur un intervalle de rafale plus court. Le taux d'événements en rafale est de 1/30 de l'intervalle de débit moyen ou de 10 secondes, selon le plus élevé des deux. Pour chaque événement détecté et considéré comme faisant partie d'une attaque par analyse, l'ASA vérifie les limites de débit moyen et de rafale. Si l'un ou l'autre de ces débits est dépassé pour le trafic envoyé par un hôte, cet hôte est considéré comme un agresseur. Si l'un ou l'autre de ces débits est dépassé pour le trafic reçu par un hôte, cet hôte est considéré comme une cible.

Le tableau suivant répertorie les limites de débit par défaut pour la détection des menaces d'analyse.

Tableau 15 : Limites de débit par défaut pour la détection des menaces par analyse

Débit moyen	Taux de rafale
5 abandons/s au cours des 600 dernières secondes.	10 abandons/s au cours des 20 dernières secondes.
5 abandons/s au cours des 3 600 dernières secondes.	10 abandons/s au cours de la dernière période de 120 secondes.

Mise en garde La fonction de détection des menaces par analyse peut affecter de manière significative les performances et la mémoire de l'ASA pendant qu'elle crée et recueille une structure de données et des informations basées sur l'hôte et le sous-réseau.

Lignes directrices pour la détection des menaces

Lignes directrices relatives au contexte de sécurité

À l'exception des statistiques sur les menaces avancées, la détection des menaces est prise en charge en mode unique uniquement. En mode multiple, les statistiques d'interception TCP sont les seules statistiques prises en charge.

Types de trafic surveillés

- Pour les statistiques, seul le trafic traversant la boîte est surveillé; le trafic vers le boîtier n'est pas surveillé.
- Le trafic refusé par une liste de contrôle d'accès ne déclenche pas la détection des menaces par analyse; seul le trafic autorisé par l'ASA et qui crée un flux est affecté par la détection des menaces d'analyse.

Paramètres par défaut pour la détection des menaces

Les statistiques de détection des menaces de base sont activées par défaut.

Le tableau suivant répertorie les paramètres par défaut. Vous pouvez afficher tous ces paramètres par défaut à l'aide de la commande **show running-config all threat-detection** dans Outils > Interface de ligne de commande.

Pour les statistiques avancées, par défaut, les statistiques pour les listes de contrôle d'accès sont activées.

Tableau 16 : Paramètres par défaut de détection de base des menaces

Raison de l'abandon du paquet	Paramètres de déclenchement	
	Taux moyen	**Taux de rafale**
• Attaque par déni de service détectée	100 abandons/s au cours des 600 dernières secondes.	400 abandons/s au cours de la dernière période de 20 secondes.
• Mauvais format de paquet • Limite de connexion dépassée • Paquets ICMP suspects détectés	80 abandons/s au cours des 3 600 dernières secondes.	320 abandons/s au cours de la dernière période de 120 secondes.
Attaque par analyse détectée.	5 abandons/s au cours des 600 dernières secondes.	10 abandons/s au cours des 20 dernières secondes.
	4 abandons/s au cours des 3 600 dernières secondes.	8 abandons/s au cours des 120 dernières secondes.
Session incomplète détectée, comme une attaque TCP SYN détectée ou une session UDP sans retour de données détectée (combinées)	100 abandons/s au cours des 600 dernières secondes.	200 abandons/s au cours des 20 dernières secondes.
	80 abandons/s au cours des 3 600 dernières secondes.	160 abandons/s au cours des 120 dernières secondes.

Raison de l'abandon du paquet	Paramètres de déclenchement	
	Taux moyen	**Taux de rafale**
Refus par les listes de contrôle d'accès	400 abandons/s au cours des 600 dernières secondes.	800 abandons/s au cours des 20 dernières secondes.
	320 abandons/s au cours des 3 600 dernières secondes.	640 abandons/s au cours des 120 dernières secondes.
• Échec des vérifications de base du pare-feu • Paquets ayant échoué à l'inspection de l'application.	400 abandons/s au cours des 600 dernières secondes.	1 600 abandons/s au cours des 20 dernières secondes.
	320 abandons/s au cours des 3 600 dernières secondes.	1 280 abandons/s au cours des 120 dernières secondes.
Surcharge d'interface	2 000 abandons/s au cours des 600 dernières secondes.	8 000 abandons/s au cours des 20 dernières secondes.
	1 600 abandons/s au cours des 3 600 dernières secondes.	6 400 abandons/s au cours de la dernière période de 120 secondes.

Configurer la détection des menaces

Les statistiques de détection des menaces de base sont activées par défaut et peuvent être le seul service de détection des menaces dont vous avez besoin. Utilisez la procédure suivante si vous souhaitez mettre en œuvre des services de détection des menaces supplémentaires.

Procédure

Étape 1 Configurer les statistiques de base sur la détection des menaces, à la page 455.

Les statistiques de détection de base des menaces comprennent les activités qui peuvent être liées à une attaque, comme une attaque DoS.

Étape 2 Configurer les statistiques de détection avancée des menaces, à la page 456.

Étape 3 Configurer l'analyse de détection des menaces, à la page 457.

Configurer les statistiques de base sur la détection des menaces

Les statistiques de détection des menaces de base sont activées par défaut. Vous pouvez les désactiver ou les réactiver si vous les avez désactivées.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Threat Detection (Détection des menaces)**

Étape 2 Sélectionnez ou désélectionnez **la fonction Enable Basic Threat Détection (activer la détection des menaces de base)** comme vous le souhaitez.

Étape 3 Cliquez sur **Apply** (Appliquer).

Configurer les statistiques de détection avancée des menaces

Vous pouvez configurer l'ASA pour collecter des statistiques détaillées. Par défaut, les statistiques pour les listes de contrôle d'accès sont activées. Pour activer d'autres statistiques, procédez comme suit.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Threat Detection (Détection des menaces)**

Étape 2 Dans la zone Scanning Threat Statistics (Statistiques des menaces d'analyse), choisissez l'une des options suivantes :

- **Enable All Statistics (Activer toutes les statistiques)**.
- **Disable All Statistics (Désactiver toutes les statistiques)**.
- **Enable Only Following Statistics (Activer uniquement les statistiques suivantes)**.

Étape 3 Si vous avez choisi **Enable Only Following Statistics (Activer uniquement les statistiques suivantes)**, sélectionnez une ou plusieurs des options suivantes :

- **Hosts (Hôtes)** : active les statistiques de l'hôte. Les statistiques sur l'hôte s'accumulent tant que l'hôte est actif et dans la base de données de l'hôte de menace d'analyse. L'hôte est supprimé de la base de données (et les statistiques effacées) après 10 minutes d'inactivité.
- **Access Rules (Règles d'accès)** (activé par défaut) : active les statistiques pour les règles d'accès.
- **Port** : active les statistiques pour les ports TCP et UDP.
- **Protocol** : active les statistiques pour les protocoles IP non TCP/UDP.
- **TCP-Intercept** : active les statistiques pour les attaques interceptées par TCP Intercept (pour activer l'interception TCP, consultez Protéger les serveurs contre une attaque DoS par inondation SYN (interception de TCP), à la page 416).

Étape 4 Pour les statistiques d'hôte, de port et de protocole, vous pouvez modifier le nombre d'intervalles de débit collectées. Dans la zone Intervalles de débit, choisissez **1 heure**, **1 et 8 heures**, ou **1, 8 et 24 heures** pour chaque type de statistique. L'intervalle par défaut est **1 heure**, ce qui réduit l'utilisation de la mémoire.

Étape 5 Pour les statistiques d'interception TCP, vous pouvez définir les options suivantes dans la zone de détection des menaces d'interception TCP :

- **Monitoring Window Size** : définit la taille de la fenêtre de surveillance de l'historique, entre 1 et 1 440 minutes. La valeur par défaut est de 30 minutes. L'ASA échantillonne le nombre d'attaques 30 fois au cours de l'intervalle de débit ; ainsi, pour la période par défaut de 30 minutes, des statistiques sont collectées toutes les 60 secondes.
- **Burst Threshold Rate** : définit le seuil de génération de messages syslog, entre 25 et 2 147 483 647. La valeur par défaut est de 400 par seconde. Lorsque le débit en rafale est dépassé, le message syslog 733104 est généré.
- **Average Threshold Rate** : définit le seuil de débit moyen pour la génération de messages syslog, entre 25 et 2 147 483 647. La valeur par défaut est de 200 par seconde. Lorsque le débit moyen est dépassé, le message syslog 733105 est généré.

Cliquez sur **Set Default** (Rétablir les valeurs par défaut) pour rétablir les valeurs par défaut.

Étape 6 Cliquez sur **Apply** (Appliquer).

Configurer l'analyse de détection des menaces

Vous pouvez configurer la détection des menaces par analyse pour identifier les agresseurs et, éventuellement, les contourner.

Vous pouvez configurer l'ASA pour envoyer des messages de journal système sur un agresseur ou vous pouvez banir automatiquement l'hôte. Par défaut, le message de journal système 730101 est généré lorsqu'un hôte est identifié comme agresseur. Assurez-vous d'exclure les adresses du bannissement lorsque vous attendez beaucoup de messages de la part de l'hôte. Par exemple, si vous avez activé la multidiffusion PIM, exemptez les routeurs PIM ou les messages PIM seront abandonnés.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Threat Detection (Détection des menaces)**

Étape 2 Sélectionnez **Enable Scanning Threat Detection** (Activer la détection des menaces par analyse).

Étape 3 (Facultatif) Pour mettre fin automatiquement à une connexion d'hôte lorsque l'ASA identifie l'hôte comme un agresseur, sélectionnez **Shun Hosts detected by scanning threat** (Bloquer les hôtes détectés par la détection des menaces par analyse) et complétez ces options si vous le souhaitez :

- Pour exempter les adresses IP d'hôte d'être contournées, saisissez une adresse ou le nom d'un objet réseau dans le champ **Réseaux exclus du contournement**. Il est possible d'entrer des adresses multiples, séparées par des virgules. Pour choisir un réseau dans la liste des objets d'adresse IP, cliquez sur le bouton **...** .
- Pour définir la durée d'un bannissement pour un hôte attaquant, sélectionnez **Définir la durée du bannissement** et saisissez une valeur comprise entre 10 et 2 592 000. La durée par défaut est de 3 600 secondes (1 heure). Pour rétablir la valeur par défaut, cliquez sur **Set Default** (Rétablir les valeurs par défaut).

Étape 4 Cliquez sur **Apply** (Appliquer).

Surveillance de la détection des menaces

Les rubriques suivantes expliquent comment surveiller la détection des menaces et afficher les statistiques de trafic.

Surveillance des statistiques de détection de base des menaces

Choisissez **Home (Accueil) > Firewall Dashboard (Tableau de bord du pare-feu) > Traffic Overview (Aperçu du trafic)** pour afficher les statistiques de détection des menaces de base.

Surveillance des statistiques de détection avancée des menaces

Vous pouvez surveiller les statistiques avancées sur les menaces à l'aide des tableaux de bord suivants :

- **Accueil > Tableau de bord du pare-feu > 10 principaux critères d'accès** : affiche les critères d'accès les plus sollicités. Les autorisations et les refus ne sont pas distingués dans ce graphique. Vous pouvez suivre le trafic refusé dans le graphique **Aperçu du trafic > Taux de paquets abandonnés**.
- **Accueil > Tableau de bord du pare-feu > Statistiques d'utilisation** : les onglets **10 principales sources** et **10 principales destinations** affichent les statistiques sur les hôtes. En raison de l'algorithme de détection des menaces, une interface utilisée comme combinaison de basculement et de lien d'état peut apparaître dans les 10 principaux hôtes; il s'agit du comportement attendu, et vous pouvez ignorer cette adresse IP dans l'affichage.

  L'onglet **Top 10 Services** (10 principaux services) affiche les statistiques pour les ports et les protocoles (les deux doivent être activés pour l'affichage) et affiche les statistiques combinées des types de ports TCP/UDP et de protocoles IP. TCP (protocole 6) et UDP (protocole 17) ne sont pas inclus dans l'affichage pour les protocoles IP; cependant, les ports TCP et UDP sont inclus dans l'affichage pour les ports. Si vous n'activez les statistiques que pour l'un de ces types, port ou protocole, vous ne pourrez afficher que les statistiques activées.
- **Accueil > Tableau de bord du pare-feu > Les dix principaux serveurs protégés sous l'attaque SYN** : affiche les statistiques d'interception TCP. Cliquez sur le bouton **Detail** (Détails) pour afficher les données d'échantillonnage de l'historique. L'ASA échantillonne le nombre d'attaques 30 fois au cours de l'intervalle de débit ; ainsi, pour la période par défaut de 30 minutes, des statistiques sont collectées toutes les 60 secondes.

Historique de la détection des menaces

Nom de la caractéristique	Versions de plateforme	Description
Statistiques de détection de base et avancée des menaces, détection des menaces par analyse	8.0(2)	Statistiques de détection de base et avancée des menaces, la détection des menaces d'analyse a été introduite. Les écrans suivants ont été introduits : **Configuration > Firewall (Pare-feu) > Threat Detection (Détection des menaces)**, **Home (Accueil) > Firewall Dashboard (Tableau de bord du pare-feu) > Traffic Overview (Aperçu du trafic)**, **Home (Accueil) > Firewall Dashboard (Tableau de bord du pare-feu) > Top 10 Access Rules (10 principales règles d'accès)**, **Home (Accueil) > Firewall Dashboard (Tableau de bord du pare-feu) > Top Usage Status (État de l'utilisation la plus élevée)**, **Home (Accueil) > Firewall Dashboard (Tableau de bord du pare-feu) > Top 10 Protected Servers Under SYN Attack (10 principaux serveurs protégés sous attaque SYN)**.
Durée du bannissement	8.0(4)/8.1(2)	Vous pouvez maintenant définir la durée du blocage, L'écran suivant a été modifié : **Configuration > Firewall (Pare-feu) > Threat Detection (Détection des menaces)**.
Statistiques TCP Intercept	8.0(4)/8.1(2)	Les statistiques TCP Intercept ont été introduites. Les écrans suivants ont été introduits ou modifiés : **Configuration > Firewall (Pare-feu) > Threat Detection (Détection des menaces)**, **Home (Accueil) > Firewall Dashboard (Tableau de bord du pare-feu) > Top 10 Protected Servers Under SYN Attack (10 principaux serveurs protégés sous attaque SYN)**.
Personnaliser les intervalles de débit des statistiques d'hôte	8.1(2)	Vous pouvez maintenant personnaliser le nombre d'intervalles de débit pour lesquels les statistiques sont recueillies. Le nombre de débits par défaut a été modifié de 3 à 1. L'écran suivant a été modifié : **Configuration > Firewall (Pare-feu) > Threat Detection (Détection des menaces)**.
L'intervalle de débit de rafale a été modifié à 1/30 du débit moyen.	8.2(1)	Dans les versions précédentes, l'intervalle de débit en rafale était de 1/60 du débit moyen. Pour maximiser l'utilisation de la mémoire, l'intervalle d'échantillonnage a été réduit à 30 pendant le débit moyen.
Personnaliser les intervalles de débit des statistiques de port et de protocole	8.3(1)	Vous pouvez maintenant personnaliser le nombre d'intervalles de débit pour lesquels les statistiques sont recueillies. Le nombre de débits par défaut a été modifié de 3 à 1. L'écran suivant a été modifié : **Configuration > Firewall (Pare-feu) > Threat Detection (Détection des menaces)**.

Nom de la caractéristique	Versions de plateforme	Description
Amélioration de l'utilisation de la mémoire	8.3(1)	L'utilisation de la mémoire pour la détection des menaces a été améliorée.

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.