



CLI, livre 2 : Guide de configuration de la série Cisco Secure Firewall ASA Firewall CLI, 9.19

Dernière modification : 2026-07-24

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 NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

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

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

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

© 2026 Cisco Systems, Inc. Tous droits réservés.



TABLE DES MATIÈRES

PRÉFACE

À propos de ce guide xix

Objectifs du document xix

Documentation associée xix

Conventions de document xix

Communications, services et renseignements supplémentaires xxi

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 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 7

CHAPITRE 2

Objets pour le contrôle d'accès 9

Lignes directrices relatives aux objets 9

Configurer les objets. 10

Configurer les objets et groupes de réseau 10

Configurer un objet réseau 10

Configurer un groupe d'objets réseau 11

Configurer des objets de service et des groupes de services 12

Configurer un objet de service 12

Configurer un groupe de services	13
Configuration des objets et des groupes de service réseau	15
Lignes directrices relatives aux objets de service réseau	15
Configurer des serveurs DNS de confiance	16
Configurer les objets de service de réseau	17
Configurer les groupes d'objets de service réseau	19
Configurer les groupes d'utilisateurs locaux	20
Configurer les groupes d'objets de sécurité	22
Configurer les plages de temps	23
Surveillance des objets	24
Historique pour les objets	25
CHAPITRE 3	Listes de contrôle d'accès 27
À propos des ACL	27
Types d'ACL	27
Noms des ACL	29
Ordre des entrées de contrôle d'accès	29
Autoriser/refuser ou mettre en correspondance/aucune correspondance	30
Refus implicite du contrôle d'accès	30
Adresses IP utilisées pour les ACL étendues lorsque vous utilisez la NAT	30
ACE temporelles	31
Licences pour les ACL	32
Lignes directrices pour les ACL	32
Configurer les ACL	33
Options de base de configuration et de gestion de l'ACL	33
Configurer les ACL étendues	34
Ajouter une ACE étendue pour la correspondance basée sur les adresses IP ou les noms de domaine complets	35
Ajoutez une ACE étendue pour la correspondance basée sur le port	36
Ajouter une ACE étendue pour la correspondance basée sur ICMP	38
Ajouter une ACE étendue pour la correspondance basée sur l'utilisateur (pare-feu d'identité)	38
Ajouter une ACE étendue pour la correspondance basée sur un groupe de sécurité (Cisco TrustSec)	39
Exemples d'ACL étendues	40

Exemple de conversion d'adresses en objets pour les ACL étendues	41
Configurer les ACL standard	42
Configurer les ACL de type Web	42
Ajouter une ACE de type Web pour la correspondance d'URL	43
Ajouter une ACE de type Web pour la correspondance d'adresses IP	44
Exemples d'ACL de type Web	45
Configurer les ACL EtherType	46
Exemples d'ACL EtherType	47
Modifier les ACL dans une session de configuration isolée	48
Surveiller les ACL	49
Historique des ACL	50

CHAPITRE 4

Règles d'accès 53

Contrôle d'accès au réseau	53
Renseignements généraux sur les règles	54
Règles d'accès d'interface et règles d'accès globales	54
Règles entrantes et sortantes	54
Ordre des règles	55
Autorisations implicites	55
Refus implicite	56
NAT et critères d'accès	56
Interfaces de niveau de sécurité identiques et règles d'accès	56
Règles d'accès étendues	57
Règles de contrôle d'accès étendues pour le retour du trafic	57
Autoriser le trafic de diffusion et de multidiffusion	57
Règles d'accès de gestion	58
Règles EtherType	58
EtherTypes pris en charge et autres types de trafic	58
Règles EtherType pour le retour du trafic	59
Autoriser MPLS	59
Licences pour les règles d'accès	59
Lignes directrices relatives au contrôle d'accès	59
Configurer le contrôle d'accès	61
Configurer un groupe d'accès	61

Configurer les règles d'accès ICMP	62
Surveillance des règles d'accès	64
Évaluation des messages Syslog pour les règles d'accès	65
Exemples de configuration pour autoriser ou refuser l'accès au réseau	66
Historique des règles d'accès	67

CHAPITRE 5

ASA et Cisco TrustSec 71

À propos de Cisco TrustSec	71
À propos de la prise en charge de SGT et SXP dans Cisco TrustSec	72
Rôles dans la fonctionnalité Cisco TrustSec	73
Application de la politique de groupe de sécurité	74
Comment l'ASA applique les politiques basées sur les groupes de sécurité	75
Effets des modifications des groupes de sécurité sur l'ISE	76
Rôles de speaker et de listener sur l'ASA	77
Enregistrer l'ASA auprès de l'ISE	78
Créer un groupe de sécurité sur l'ISE	78
Générer le fichier PAC	79
Lignes directrices relatives à Cisco TrustSec	79
Configurer l'ASA pour s'intégrer à Cisco TrustSec	82
Configurer le serveur AAA pour l'intégration de Cisco TrustSec	83
Importer un fichier PAC	85
Configurer le protocole d'échange de sécurité	86
Ajouter un homologue de connexion SXP	88
Actualiser les données d'environnement	90
Configurer la politique de sécurité	90
Configurer l'imposition du balisage de groupe de sécurité de couche 2	92
Scénarios d'utilisation	92
Configurer une balise de groupe de sécurité sur une interface	94
Configurer manuellement les liaisons IP-SGT	95
Astuces de dépannage	95
Exemple pour Cisco TrustSec	96
Prise en charge des VPN sécurisés pour Cisco TrustSec	97
Ajouter une balise SGT aux politiques de groupe du VPN d'accès à distance et aux utilisateurs locaux	97

Surveillance de Cisco TrustSec 98

Historique de Cisco TrustSec 100

CHAPITRE 6

Cisco Umbrella 103

À propos de Cisco Umbrella Connector 103

Politique de sécurité entreprise Cisco Umbrella 103

Enregistrement de Cisco Umbrella 104

Exigences de licence pour Cisco Umbrella Connector 104

Lignes directrices et limites relatives à Cisco Umbrella 105

Configurer le connecteur Cisco Umbrella 107

Installer le certificat d'autorité de certification à partir du serveur d'enregistrement Cisco Umbrella 108

Configurer les paramètres globaux du connecteur Cisco Umbrella 109

Activer Cisco Umbrella dans la liste des politiques d'inspection DNS 111

Vérifier l'enregistrement de Cisco Umbrella 112

Exemples pour le connecteur Cisco Umbrella 113

Exemple : activation de Cisco Umbrella dans la politique d'inspection DNS globale 113

Exemple : activation de Cisco Umbrella sur une interface avec une politique d'inspection personnalisée 114

Exemple : exclusion de certains hôtes ou réseaux de Cisco Umbrella globalement 116

Surveillance du connecteur Cisco Umbrella 117

Surveillance des statistiques de politique de service Cisco Umbrella 117

Surveillance des messages Syslog Cisco Umbrella 118

Historique du connecteur Cisco Umbrella 120

PARTIE II

Services de pare-feu pour environnements virtuels 121

CHAPITRE 7

Contrôle d'accès basé sur les attributs 123

Lignes directrices relatives aux objets réseau basés sur les attributs 123

Configurer le contrôle d'accès basé sur les attributs 124

Configurer les attributs des machines virtuelles vCenter 124

Configurer un agent d'attribut de VM 126

Configurer les objets réseau basés sur les attributs 128

Configurer le contrôle d'accès à l'aide d'objets réseau basés sur les attributs 130

Surveillance des objets réseau basés sur les attributs 131

Historique du contrôle d'accès basé sur les attributs 133

PARTIE III

NAT (Network Address Translation; Translation d'adresses de réseau) 135

CHAPITRE 8

Traduction d'adresses réseau (NAT) 137

Pourquoi utiliser la NAT? 137

Principes de base de la NAT 138

Terminologie NAT 138

Type de NAT 138

NAT objet de réseau et NAT Twice 139

NAT objet de réseau 139

NAT Twice 139

Comparaison de NAT objet de réseau et NAT Twice 140

Ordre des règles NAT 141

Interfaces NAT 143

Lignes directrices pour la NAT 143

Lignes directrices sur le mode pare-feu pour la NAT 143

Lignes directrices pour la NAT pour IPv6 144

Bonnes pratiques pour la NAT IPv6 144

Lignes directrices supplémentaires pour la NAT 145

Lignes directrices relatives à la NAT d'objets réseau pour les objets d'adresses mappées 148

Lignes directrices pour le NAT Twice concernant les objets d'adresses réelles et mappées 149

Lignes directrices de destination de nom de domaine complet (FQDN) 150

Lignes directrices NAT Twice pour les objets de service pour les ports réels et mappés 151

Traduction d'adresses réseau dynamique 151

À propos de la NAT dynamique 152

Avantages et désavantages de la NAT dynamique 153

Configurer la NAT dynamique 153

Configurer la NAT Twice dynamique 156

PAT dynamique 159

À propos de la PAT dynamique 159

Avantages et inconvénients de la PAT dynamique 159

Lignes directrices pour les objets du regroupement PAT 160

Configurer la PAT d'objet réseau dynamique 161

Configurer la PAT Twice dynamique	164
Configurer PAT avec l'attribution de bloc de ports	167
Configurer la PAT par session ou la PAT multi-session	169
NAT statique	171
À propos de la NAT statique	171
NAT statique avec traduction de port	172
NAT statique un vers plusieurs	173
Autres scénarios de mappage (non recommandés)	174
Configurer la NAT d'objet réseau statique ou la NAT statique avec traduction de port	175
Configurer la NAT statique Twice ou la NAT statique avec traduction de port	178
NAT d'identité	181
Configurer la NAT d'objet de réseau d'identité	182
Configurer la NAT d'identité Twice	184
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)	196
Équilibreur de charge interne avec plusieurs adresses mappées (NAT statique, un à plusieurs)	198
Adresse unique pour FTP, HTTP et SMTP (NAT statique avec traduction de port)	199
Exemples pour la NAT Twice	200
Traduction différente selon la destination (PAT manuelle dynamique)	200
Traduction différente selon l'adresse et le port de destination (PAT dynamique)	202
NAT en mode routage et transparent	204
NAT en mode routé	204
NAT en mode transparent ou dans un groupe de pont	204
Routage des paquets NAT	206
Adresses mappées et routage	206
Adresses sur le même réseau que l'interface mappée	206
Adresses sur un réseau unique	206
Même adresse que l'adresse réelle (NAT d'identité)	207

Exigences de routage en mode transparent pour les réseaux distants	208
Détermination de l'interface de sortie	208
NAT pour VPN	209
NAT et VPN d'accès à distance	209
NAT et VPN de site à site	211
Accès à la gestion de la NAT et du VPN	214
Dépannage de la NAT et du VPN	215
Traduction de réseaux IPv6	215
NAT64/46 : traduction d'adresses IPv6 en IPv4	216
Exemple NAT64/46 : réseau IPv6 interne avec Internet IPv4 externe	216
Exemple NAT64/46 : réseau interne IPv6 avec Internet IPv4 externe et traduction DNS	217
NAT66 : Traduction d'adresses IPv6 en adresses différentes IPv6	219
Exemple NAT66, de traduction statique entre réseaux	219
Exemple de NAT66, PAT d'interface IPv6 simple	220
Réécriture des requêtes et réponses DNS à l'aide de la NAT	221
Modification de la réponse DNS, serveur DNS externe	222
Modification de la réponse DNS, serveur DNS, hôte et serveur sur des réseaux séparés	224
Modification de la réponse DNS, serveur DNS sur le réseau hôte	224
Modification de la réponse DNS64	225
Modification PTR, serveur DNS sur le réseau hôte	227

CHAPITRE 10

Mappage de l'adresse et du port (MAP)	229
Mappage de l'adresse et du port (MAP)	229
Mappage de l'adresse et de la traduction du port (MAP-T)	229
Lignes directrices pour le mappage de l'adresse et du port (MAP)	230
Configurer les domaines MAP-T	232
Surveillance MAP	234
Vérification de la configuration du domaine MAP	234
Surveillance des messages Syslog	234
Historique du MAP	235

PARTIE IV

Politiques de service et inspection des applications	237

CHAPITRE 11

Politique de service	239

À propos des politiques de service	239
Les composants d'une politique de service	239
Fonctionnalités configurées avec les politiques de service	241
Sens d'application des fonctionnalités	242
Correspondance des fonctionnalités dans une politique de service	243
Ordre dans lequel plusieurs actions de fonctionnalité sont appliquées	244
Incompatibilité de certaines actions de fonctionnalité	244
Mise en correspondance des fonctionnalités pour plusieurs politiques de service	245
Lignes directrices pour les politiques de service	246
Par défaut pour les politiques de service	247
Configuration de la politique de service par défaut	248
Cartes de trafics par défaut (classes de trafic)	248
Configurer les politiques de service	249
Identifier le trafic (cartes de trafic de couche 3/4)	251
Créer une carte de trafic de couche 3/4 pour le trafic de transit	251
Créer une carte de trafic de couche 3/4 pour le trafic de gestion	253
Définir les actions (liste des politiques de couche 3/4)	254
Appliquer les actions à une interface (politique de service)	256
Surveillance des politiques de service	257
Exemples de politiques de service (cadre de politique modulaire)	257
Application de l'inspection et de la régulation QoS au trafic HTTP	257
Application de l'inspection au trafic HTTP globalement	258
Application des limites d'inspection et de connexion au trafic HTTP vers des serveurs spécifiques	258
Application de l'inspection au trafic HTTP avec NAT	259
Historique des politiques de service	260

CHAPITRE 12
Premiers pas avec l'inspection du protocole de la couche application 261

Inspection des protocoles de la couche applicative	261
Quand utiliser l'inspection du protocole d'application	261
Listes des politiques d'inspection	262
Remplacement d'une liste des politiques d'inspection en cours d'utilisation	262
Comment plusieurs classes de trafic sont gérées	262
Lignes directrices relatives à l'inspection des applications	264
Valeurs par défaut pour l'inspection des applications	265

Inspections par défaut et limites de la NAT	265
Listes des politiques d'inspection par défaut	270
Configurer l'inspection du protocole de couche d'application	270
Choix de la bonne classe de trafic pour l'inspection	275
Configurer les expressions régulières	277
Créer une expression régulière	277
Créer une carte de trafic d'expression régulière	280
Surveillance des politiques d'inspection	280
Historique de l'inspection des applications	282

CHAPITRE 13
Inspection des protocoles Internet de base 283

Inspection DCERPC	283
Présentation de DCERPC	284
Configurer une liste des politiques d'inspection DCERPC	284
Inspection DNS	287
Valeurs par défaut pour l'inspection DNS	287
Configurer la liste des politiques d'inspection DNS	287
Inspection FTP	292
Présentation de l'inspection FTP	292
FTP strict	292
Configurer une liste des politiques d'inspection FTP	293
Inspection HTTP	296
Présentation de l'inspection HTTP	297
Configurer une liste des politiques d'inspection HTTP	297
Inspection ICMP	301
Inspection des erreurs ICMP	301
Inspection ILS	302
Inspection de la messagerie instantanée	303
Inspection des options IP	306
Valeurs par défaut pour l'inspection des options IP	306
Configurer une liste des politiques d'inspection des options IP	307
Inspection IPsec Pass Through	308
Aperçu de l'inspection de transmission directe IPsec	308
Configurer une liste des politiques d'inspection de transmission directe IPsec	309

Inspection IPv6	310
Valeurs par défaut pour l'inspection IPv6	310
Configurer une liste des politiques d'inspection IPv6	310
Inspection NetBIOS	312
Inspection PPTP	313
Inspection RSH	314
Inspection SMTP et SMTP étendue	314
Aperçu de l'inspection SMTP et ESMTP	314
Valeurs par défaut pour l'inspection ESMTP	315
Configurer une liste des politiques d'inspection ESMTP	316
Inspection SNMP	319
Inspection SQL*Net	320
Inspection Sun RPC	320
Aperçu de l'inspection Sun RPC	320
Gérer les services Sun RPC	321
Inspection TFTP	322
Inspection XDMCP	322
Inspection VXLAN	323
Historique de l'inspection du protocole Internet de base	323

CHAPITRE 14

Inspection des protocoles vocaux et vidéo	327
Inspection CTIQBE	327
Limites de l'inspection CTIQBE	327
Inspection H.323	328
Aperçu de l'inspection H.323	328
Fonctionnement de H.323	328
Prise en charge H.239 dans les messages H.245	329
Limites de l'inspection H.323	330
Configurer la liste des politiques d'inspection H.323	330
Inspection MGCP	333
Aperçu de l'inspection MGCP	333
Configurer une liste des politiques d'inspection MGCP	335
Inspection RTSP	336
Survol de l'inspection RTSP	336

Exigences de configuration de RealPlayer	337
Limites de l'inspection RSTP	337
Configurer une liste des politiques d'inspection RTSP	337
Inspection SIP	340
Présentation de l'inspection SIP	340
Limites pour l'inspection SIP	341
Inspection SIP par défaut	342
Configurer une liste des politiques d'inspection SIP	342
Inspection Skinny (SCCP)	346
Aperçu de l'inspection SCCP	346
Prise en charge des téléphones IP Cisco	347
Limites de l'inspection SCCP	347
Inspection SCCP par défaut	347
Configurer une liste des politiques d'inspection Skinny (SCCP)	348
Inspection STUN	349
Historique de l'inspection des protocoles vocaux et vidéo	350

CHAPITRE 15
Inspection des réseaux mobiles 353

Aperçu de l'inspection du réseau mobile	353
Aperçu de l'inspection GTP	353
Suivi des changements d'emplacement pour les stations mobiles	354
Limites d'inspection GTP	354
Inspection et contrôle d'accès SCTP (Stream Control Transmission Protocol)	355
Inspection dynamique SCTP	355
Contrôle d'accès SCTP	356
NAT SCTP	356
Inspection de la couche application SCTP	356
Limites de SCTP	357
Inspection Diameter	357
Inspection M3UA	358
Conformité au protocole M3UA	359
Limites d'inspection M3UA	359
Aperçu de l'inspection de comptabilité RADIUS	360
Licences pour l'inspection des protocoles de réseau mobile	360

Valeurs par défaut pour l'inspection GTP	361
Configurer l'inspection du réseau mobile	361
Configurer une liste des politiques d'inspection GTP	362
Configurer une liste des politiques d'inspection SCTP	367
Configurer une liste des politiques d'inspection Diameter	368
Créer une paire attribut-valeur (AVP) de Diameter personnalisée	373
Inspection des sessions Diameter chiffrées	374
Configurer la relation d'approbation de serveur avec les clients Diameter	375
Configurer le proxy TLS complet avec un certificat client statique pour l'inspection Diameter	377
Configurer le proxy TLS complet avec des certificats dynamiques locaux pour l'inspection Diameter	380
Configurer le serveur proxy TLS avec déchargement TLS pour l'inspection Diameter	383
Configurer une liste des politiques d'inspection M3UA	385
Configurer la politique de service d'inspection de réseau mobile	389
Configurer l'inspection de comptabilité RADIUS	391
Configurer une liste des politiques d'inspection de comptabilité RADIUS	391
Configurer la politique de service d'inspection de comptabilité RADIUS	392
Surveillance de l'inspection du réseau mobile	394
Surveillance de l'inspection GTP	394
Surveillance SCTP	395
Surveillance de Diameter	396
Surveillance M3UA	397
Historique de l'inspection du réseau mobile	398

PARTIE V
Gestion des connexions et détection des menaces 403

CHAPITRE 16
Paramètres de connexion 405

Que sont les paramètres de connexion?	405
Configurer les paramètres de connexion	406
Configurer les délais d'expiration globaux	407
Protéger les serveurs contre une attaque DoS par inondation SYN (interception de TCP)	410
Personnaliser le traitement anormal des paquets TCP (listes TCP, normaliseur TCP)	413
Contourner les vérifications de l'état de TCP pour le routage symétrique (TCP State Bypass)	417
Le problème du routage asymétrique	417

Lignes directrices et limites du contournement d'état TCP	418
Configurer le contournement d'état TCP	419
Désactiver la gestion aléatoire de la séquence TCP	420
Délester les flux volumineux	422
Limites de déchargement de flux	423
Configurer le déchargement de flux	424
Décharge de flux IPsec	426
Configurer le déchargement de flux IPsec	427
Configurer les paramètres de connexion pour des cartes de classes de trafic spécifiques (tous les services)	427
Configurer les options TCP	432
Supervision des connexions	433
Historique des paramètres de connexion	434

CHAPITRE 17
Qualité de service 439

À propos de QoS	439
Fonctionnalités QoS prises en charge	439
Qu'est-ce qu'un compartiment de jetons?	440
Police	440
File d'attente prioritaire	440
Comment les fonctionnalités QoS interagissent	441
Préservation DSCP (DiffServ)	441
Lignes directrices relatives à la QoS	441
Configurer QoS	442
Déterminer les limites de la file d'attente et de l'anneau TX pour une file d'attente prioritaire	442
Feuille de travail sur la limite de la file d'attente	442
Feuille de calcul des limites de l'anneau TX	443
Configurer la file d'attente prioritaire pour une interface	444
Configurer une règle de service pour la mise en file d'attente prioritaire et la régulation	445
Surveiller la QoS	448
Statistiques de régulation QoS	448
Statistiques de priorité QoS	448
Statistiques de file d'attente prioritaire QoS	448
Exemples de configuration pour la mise en file d'attente prioritaire et la régulation	449

Exemples de cartes de trafic pour le trafic VPN	449
Exemple de priorité et de régulation	450
Historique QoS	451

CHAPITRE 18

Détection des menaces 453

Détection des menaces	453
Statistiques de détection des menaces de base	454
Statistiques de détection avancée des menaces	454
Détection des menaces par analyse	455
Lignes directrices pour la détection des menaces	456
Paramètres par défaut pour la détection des menaces	456
Configurer la détection des menaces	457
Configurer les statistiques de base sur la détection des menaces	457
Configurer les statistiques de détection avancée des menaces	458
Configurer l'analyse de détection des menaces	460
Surveillance de la détection des menaces	461
Surveillance des statistiques de base de la détection des menaces	461
Surveillance des statistiques de détection avancée des menaces	462
Évaluation des statistiques de détection des menaces de l'hôte	464
Surveillance de la détection des menaces, des hôtes contournés, des agresseurs et des cibles	466
Exemples pour la détection des menaces	467
Historique de la détection des menaces	468



À propos de ce guide

Les rubriques suivantes expliquent comment utiliser ce guide.

- [Objectifs du document, à la page xix](#)
- [Documentation associée, à la page xix](#)
- [Conventions de document, à la page xix](#)
- [Communications, services et renseignements supplémentaires, à la page xxi](#)

Objectifs du document

L'objectif de ce guide est de vous aider à configurer les fonctionnalités de pare-feu pour la série Secure Firewall ASA à l'aide de l'interface de ligne de commande. Ce guide ne couvre pas toutes les fonctionnalités, mais décrit uniquement les scénarios de configuration les plus courants.

Vous pouvez également configurer et superviser l'ASA à l'aide de l'Adaptive Security Device Manager (ASDM), une application d'interface graphique utilisateur basée sur le Web. ASDM comprend des assistants de configuration pour vous guider dans certains scénarios de configuration courants et une assistance en ligne pour les scénarios moins 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.

Documentation associée

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

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.
<i>italic</i>	Les variables, pour lesquelles vous fournissez des valeurs, sont présentées dans une police de caractères en <i>italique</i> . 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, tel 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 l'impact commercial que vous recherchez avec les technologies qui comptent, visitez [services de 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

L'[outil de recherche de bogues de Cisco](#) est un outil Web qui donne accès au système de suivi des bogues de Cisco, qui conserve une liste complète des défaillances et des vulnérabilités des produits et des 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 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 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 supprimer, lors de l'entrée, des types de trafic spécifiques ou le trafic provenant d'hôtes ou de réseaux spécifiques. 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 53](#) et [Listes de contrôle d'accès, à la page 27](#).

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 71](#).

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 proxy 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 103](#).

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, aléatorisation 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 405](#).

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 453](#).

Services de pare-feu pour 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 123](#).

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 137](#)
- [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 239
- Premiers pas avec l'inspection du protocole de la couche application, à la page 261
- Inspection des protocoles Internet de base, à la page 283
- Inspection des protocoles vocaux et vidéo, à la page 327
- Inspection des réseaux mobiles, à la page 353.

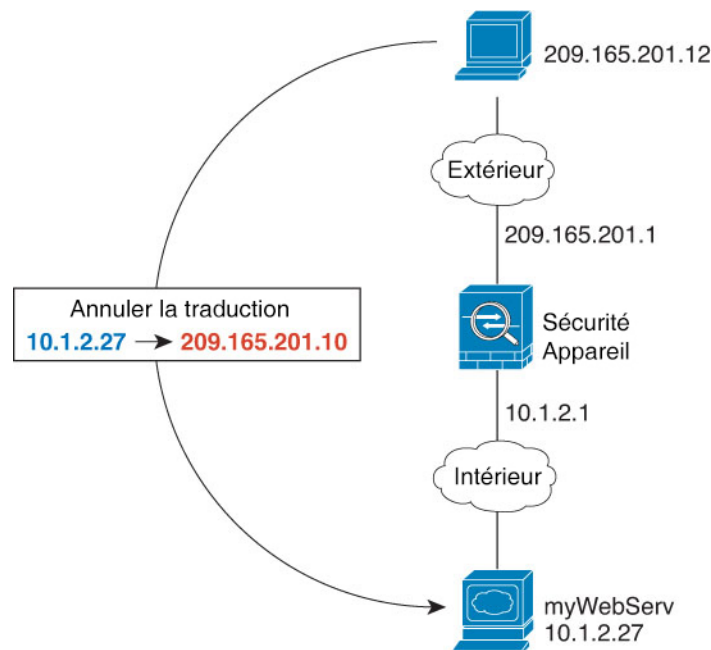
Scénario d'utilisation : exposer un serveur au public

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



Procédure

Étape 1 Créez un objet réseau pour le serveur Web interne.

```
hostname(config)# object network myWebServ  
hostname(config-network-object)# host 10.1.2.27
```

Étape 2 Configurez la NAT statique pour l'objet :

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

Étape 3 Ajoutez une règle d'accès au groupe d'accès associé à l'interface externe pour autoriser l'accès Web au serveur.

```
hostname(config)# access-list outside_access_in line 1 extended  
permit tcp any4 object myWebServ eq http
```

Étape 4 Si vous n'avez pas encore de groupe d'accès sur l'interface externe, appliquez-le à l'aide de la commande access-group :

```
hostname(config)# access-group outside_access_in in interface outside
```



PARTIE I

Contrôle d'accès

- [Objets pour le contrôle d'accès, à la page 9](#)
- [Listes de contrôle d'accès, à la page 27](#)
- [Règles d'accès, à la page 53](#)
- [ASA et Cisco TrustSec, à la page 71](#)
- [Cisco Umbrella, à la page 103](#)



CHAPITRE 2

Objets pour le contrôle d'accès

Les objets sont des composants réutilisables pour 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 9](#)
- [Configurer les objets., à la page 10](#)
- [Surveillance des objets, à la page 24](#)
- [Historique pour les objets, à la page 25](#)

Lignes directrices relatives aux objets

Lignes directrices pour 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.

Lignes directrices 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.
- 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 137.

Procédure

Étape 1 Créez ou modifiez un objet réseau en utilisant le nom de l'objet : **object network** *object_name*

Exemple :

```
hostname(config)# object network email-server
```

Étape 2 Ajoutez une adresse à l'objet à l'aide de l'une des commandes suivantes. Utilisez la forme **no** de la commande pour retirer l'objet.

- **host** {IPv4_address | IPv6_address} : adresse IPv4 ou IPv6 d'un seul hôte. Par exemple, 10.1.1.1 ou 2001:DB8::0DB8:800:200C:417A.
- **subnet** {IPv4_address IPv4_mask | IPv6_address/IPv6_prefix} : l'adresse d'un réseau. Pour les sous-réseaux IPv4, incluez le masque après un espace, par exemple, 10.0.0.0 255.0.0.0. Pour IPv6, incluez l'adresse et le préfixe comme une seule unité (sans espace), comme par exemple 2001:DB8:0:CD30::/60.
- **range** start_address end_address : plage d'adresses. Vous pouvez définir des plages IPv4 ou IPv6. N'incluez pas de masque ni de préfixe.
- **fqdn** [v4 | v6] fully_qualified_domain_name : un nom de domaine complet, c'est-à-dire le nom d'un hôte, tel que www.example.com. Précisez **v4** pour limiter l'adresse à IPv4 et **v6** pour IPv6. Si vous ne spécifiez pas de type d'adresse, IPv4 est présumé.

Exemple :

```
hostname(config-network-object)# host 10.2.2.2
```

Étape 3 (Facultatif) Ajoutez une description : **description** *string*

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 Créez ou modifiez un groupe d'objets réseau en utilisant le nom de l'objet : **object-group network group_name**

Exemple :

```
hostname(config)# object-group network admin
```

Étape 2 Ajoutez des objets et des adresses au groupe d'objets réseau à l'aide d'une ou de plusieurs des commandes suivantes. Utilisez la forme **no** de la commande pour supprimer un objet.

- **network-object host {IPv4_address | IPv6_address}** : adresse IPv4 ou IPv6 d'un seul hôte. Par exemple, 10.1.1.1 ou 2001:DB8::0DB8:800:200C:417A.
- **network-object {IPv4_address IPv4_mask | IPv6_address/IPv6_prefix}** : l'adresse d'un réseau ou d'un hôte. Pour les sous-réseaux IPv4, incluez le masque après un espace, par exemple, 10.0.0.0 255.0.0.0. Pour IPv6, incluez l'adresse et le préfixe comme une seule unité (sans espace), comme par exemple 2001:DB8:0:CD30::/60.
- **network-object object object_name** : nom d'un objet réseau existant.
- **group-object object_group_name** : nom d'un groupe d'objets réseau existant.

Exemple :

```
hostname(config-network-object-group)# network-object 10.1.1.0 255.255.255.0
hostname(config-network-object-group)# network-object 2001:db8:0:cd30::/60
hostname(config-network-object-group)# network-object host 10.1.1.1
hostname(config-network-object-group)# network-object host 2001:DB8::0DB8:800:200C:417A
hostname(config-network-object-group)# network-object object existing-object-1
hostname(config-network-object-group)# group-object existing-network-object-group
```

Étape 3 (Facultatif) Ajoutez une description : **description string**

Exemples

Pour créer un groupe de réseau qui comprend les adresses IP de trois administrateurs, entrez les commandes suivantes :

```
hostname (config)# object-group network admins
hostname (config-protocol)# description Administrator Addresses
hostname (config-protocol)# network-object host 10.2.2.4
hostname (config-protocol)# network-object host 10.2.2.78
```

```
hostname (config-protocol)# network-object host 10.2.2.34
```

Créez des groupes d'objets réseau pour les utilisateurs privilégiés de différents services en entrant les commandes suivantes :

```
hostname (config)# object-group network eng
hostname (config-network)# network-object host 10.1.1.5
hostname (config-network)# network-object host 10.1.1.9
hostname (config-network)# network-object host 10.1.1.89
```

```
hostname (config)# object-group network hr
hostname (config-network)# network-object host 10.1.2.8
hostname (config-network)# network-object host 10.1.2.12
```

```
hostname (config)# object-group network finance
hostname (config-network)# network-object host 10.1.4.89
hostname (config-network)# network-object host 10.1.4.100
```

Vous imbriquez ensuite les trois groupes comme suit :

```
hostname (config)# object-group network admin
hostname (config-network)# group-object eng
hostname (config-network)# group-object hr
hostname (config-network)# group-object finance
```

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 Créez ou modifiez un objet de service en utilisant le nom de l'objet : **object service** *object_name*

Exemple :

```
hostname(config)# object service web
```

Étape 2 Ajoutez un service à l'objet à l'aide de l'une des commandes suivantes. Utilisez la forme **no** de la commande pour supprimer un objet.

- **service** *protocol* : nom ou numéro (0 à 255) d'un protocole IP. Précisez **ip** pour appliquer à tous les protocoles.
- **service** {**icmp** | **icmp6**} [*icmp-type* [*icmp_code*]] : pour les messages 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 (1 à 255). Si vous ne spécifiez pas de code, tous les codes sont utilisés.

- **service {tcp | udp | sctp} [source operator port] [destination operator port]** : pour TCP, UDP ou SCTP. Vous pouvez éventuellement préciser des ports pour la source, la destination ou les deux. Vous pouvez préciser le port par son nom ou son numéro. L'opérateur peut être l'une des options suivantes :
 - **lt** : inférieur à.
 - **gt** : supérieur à.
 - **eq** : égal à.
 - **neq** : différent de.
 - **range** : une plage inclusive de valeurs. Lorsque vous utilisez cet opérateur, spécifiez deux numéros de port, par exemple, **range 100 200**.

Exemple :

```
hostname(config-service-object)# service tcp destination eq http
```

Étape 3 (Facultatif) Ajoutez une description : **description string**

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 Créez ou modifiez un groupe d'objets de service en utilisant le nom de l'objet : **object-group service object_name**

Exemple :

```
hostname(config)# object-group service general-services
```

Étape 2

Ajoutez des objets et des services au groupe d'objets de service à l'aide d'une ou de plusieurs des commandes suivantes. Utilisez la forme **no** de la commande pour supprimer un objet.

- **service-object protocol** : nom ou numéro (0 à 255) d'un protocole IP. Précisez **ip** à appliquer à tous les protocoles.
- **service-object {icmp | icmp6} [icmp-type [icmp_code]]** : pour les messages 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 (1 à 255). Si vous ne spécifiez pas de code, tous les codes sont utilisés.
- **service-object {tcp | udp | tcp-udp | sctp} [source operator port] [destination operator port]** : pour TCP, UDP ou les deux, ou pour SCTP. Vous pouvez éventuellement préciser des ports pour la source, la destination ou les deux. Vous pouvez préciser le port par son nom ou son numéro. L'opérateur peut être l'une des options suivantes :
 - **lt** : inférieur à.
 - **gt** : supérieur à.
 - **eq** : égal à.
 - **neq** : différent de.
 - **range** : une plage inclusive de valeurs. Lorsque vous utilisez cet opérateur, spécifiez deux numéros de port, par exemple, **range 100 à 200**.
- **service-object object object_name**—nom d'un objet de service existant.
- **group-object object_group_name**—nom d'un groupe d'objets de service existant.

Exemple :

```
hostname(config-service-object-group)# service-object ipsec
hostname(config-service-object-group)# service-object tcp destination eq domain
hostname(config-service-object-group)# service-object icmp echo
hostname(config-service-object-group)# service-object object my-service
hostname(config-service-object-group)# group-object Engineering_groups
```

Étape 3

(Facultatif) Ajoutez une description : **description string**

Exemples

L'exemple suivant montre comment ajouter des services TCP et UDP à un groupe d'objets de service :

```
hostname(config)# object-group service CommonApps
hostname(config-service-object-group)# service-object tcp destination eq ftp
hostname(config-service-object-group)# service-object tcp-udp destination eq www
hostname(config-service-object-group)# service-object tcp destination eq h323
hostname(config-service-object-group)# service-object tcp destination eq https
hostname(config-service-object-group)# service-object udp destination eq ntp
```

L'exemple suivant montre comment ajouter plusieurs objets de service à un groupe d'objets de service :


```
hostname(config)# object service SSH
hostname(config-service-object)# service tcp destination eq ssh
hostname(config)# object service EIGRP
hostname(config-service-object)# service eigrp
hostname(config)# object service HTTPS
hostname(config-service-object)# service tcp source range 1 1024 destination eq https
hostname(config)# object-group service Group1
hostname(config-service-object-group)# service-object object SSH
hostname(config-service-object-group)# service-object object EIGRP
hostname(config-service-object-group)# service-object object HTTPS
```

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 `example.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 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 `dns crypt` 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 4294967295. 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

Utilisez la commande **show dns trusted-source detail** pour déterminer les serveurs de confiance actuels qui ont été téléchargés dans le chemin de données pour une utilisation avec la résolution de domaine d'objet de service réseau.

La valeur par défaut est de faire confiance à tout serveur DNS que vous configurez dans un groupe DNS ou qui est configuré par l'intermédiaire d'un client/serveur DHCP ou d'un relais. Cette commande vous affiche les paramètres actuels et les serveurs auxquels vous faites confiance.

Exemple :

```
ciscoasa# show dns trusted-source detail
DNS Trusted Source enabled for DHCP Server Configured
DNS Trusted Source enabled for DHCP Client Learned
DNS Trusted Source enabled for DHCP Relay Learned
DNS Trusted Source enabled for DNS Server Configured
DNS Trusted Source not enabled for Trust-any
DNS Trusted Source: Type: IPs : Interface : Idle/Timeout (sec)
```

```

DNS Server Configured: 10.163.47.11: management : N/A
DNS Server Configured: 10.37.137.85: management : N/A
DNS Server Configured: 10.37.142.73: management : N/A
Data-Path DNS Trusted Source (count 3): <ip>/<refcnt>; Trust-any disabled
10.37.142.73/1
10.37.137.85/1
10.163.47.11/1

```

Étape 2 (Facultatif) Ajoutez ou supprimez des serveurs DNS de confiance configurés de manière explicite :

dns trusted-source liste_ip

La *liste_ip* est une liste séparée par des espaces des adresses IP des serveurs DNS auxquels il faut faire confiance. Vous pouvez répertorier jusqu'à 12 adresses IPv4 et IPv6. Précisez **any** pour couvrir tous les serveurs DNS. Utilisez la forme **no** de la commande pour retirer un serveur.

Étape 3 (Facultatif) Indiquez si les serveurs configurés dans les groupes de serveurs DNS doivent être considérés comme fiables.

dns trusted-source configured-servers

Un serveur configuré est un serveur spécifié dans les groupes DNS ou les commandes de serveur de noms. Par défaut, cette option est activée. Utilisez la forme **no** de la commande pour la désactiver.

Étape 4 (Facultatif) Indiquez 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.

dns trusted-source dhcp-pools

Il s'agit des serveurs qui sont configurés sur la commande **dhcpd dns** et sont donc uniquement IPv4. Par défaut, cette option est activée. Utilisez la forme **no** de la commande pour la désactiver.

Étape 5 (Facultatif) Indiquez 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.

dns trusted-source dhcp-relay

Par défaut, cette option est activée. Utilisez la forme **no** de la commande pour la désactiver.

Étape 6 (Facultatif) Indiquez 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.

dns trusted-source dhcp-client

Cette option s'applique lorsque vous configurez la commande **dhcpd auto_config** pour configurer les serveurs DHCP sur les interfaces internes en utilisant les informations obtenues à partir des interfaces de l'appareil qui utilisent le client DHCP pour obtenir une adresse IP. Par défaut, cette option est activée. Utilisez la forme **no** de la commande pour la désactiver.

Configurer les objets de service de 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 Créez ou modifiez un objet de service réseau en utilisant le nom d'objet :

object network-service *object_name*

Le nom peut comporter jusqu'à 128 caractères. Si vous incluez des espaces, vous devez mettre le nom entre guillemets doubles.

Exemple :

```
ciscoasa(config)# object network-service webex
```

Étape 2 Ajoutez un ou plusieurs emplacements d'application et services facultatifs à l'objet à l'aide de l'une des commandes suivantes. Utilisez la forme **no** de la commande pour supprimer l'emplacement. Vous pouvez entrer ces commandes plusieurs fois.

- **domain** *domain_name* [*service*] : le nom 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** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} [*service*] : l'adresse d'un réseau. Pour les sous-réseaux IPv4, incluez le masque après un espace, par exemple, `10.0.0.0 255.0.0.0`. Pour IPv6, incluez l'adresse et le préfixe comme une seule unité (sans espace), comme par exemple `2001:DB8:0:CD30::/60`.

La spécification de service pour ces commandes est la même. Précisez le service uniquement si vous souhaitez limiter la portée des connexions correspondantes. Par défaut, toute connexion aux adresses IP résolues correspond à l'objet.

protocol [*operator port*]

où :

- *protocol* est le protocole utilisé dans la connexion, tel que `tcp`, `udp`, `ip`, etc. Utilisez ? pour voir la liste des protocoles.
- (TCP/UDP uniquement) *operator* est l'un des suivants :
 - **eq** est égal au numéro de port spécifié.
 - **lt** désigne tout port inférieur au numéro de port spécifié.
 - **gt** désigne tout port supérieur au numéro de port spécifié.
 - **range** désigne tout port entre les deux ports spécifiés.
- (TCP/UDP uniquement.) *port* est le numéro de port, de 1 à 65 535 ou un mnémonique, tel que `www`. Utilisez ? pour voir les mnémoniques. Pour les plages, vous devez spécifier deux ports, le premier port étant un nombre inférieur au deuxième.

Étape 3 (Facultatif) Ajoutez une description (jusqu'à 200 caractères) : **description string**

Exemples

```
object network-service outlook365
  description This defines Microsoft office365 'outlook' application.
  domain outlook.office.com tcp eq 443
object network-service webex
  domain webex.com tcp eq 443
object network-service partner
  subnet 10.34.56.0 255.255.255.0 ip
```

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 Créez ou modifiez un groupe d'objets de service réseau en utilisant le nom de groupe :

object-group network-service *group_name*

Le nom peut comporter jusqu'à 128 caractères et peut inclure des espaces. Si vous incluez des espaces, vous devez mettre le nom entre guillemets doubles.

Exemple :

```
ciscoasa(config)# object-group network-service SaaS_Applications
```

Étape 2 Ajoutez un ou plusieurs emplacements d'application et services facultatifs à l'objet à l'aide de l'une des commandes suivantes. Utilisez la forme **no** de la commande pour supprimer l'emplacement. Vous pouvez entrer ces commandes plusieurs fois.

- **network-service-member *object_name*** : le nom d'un objet de service réseau à inclure dans le groupe. S'il y a des espaces dans le nom, mettez le nom entre guillemets doubles.
- **domain *domain_name* [*service*]** : le nom 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** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} [*service*] : l'adresse d'un réseau. Pour les sous-réseaux IPv4, incluez le masque après un espace, par exemple, 10.0.0.0 255.0.0.0. Pour IPv6, incluez l'adresse et le préfixe comme une seule unité (sans espace), comme par exemple 2001:DB8:0:CD30::/60.

La spécification de service pour ces commandes est la même. Précisez le service uniquement si vous souhaitez limiter la portée des connexions correspondantes. Par défaut, toute connexion aux adresses IP résolues correspond à l'objet.

protocol [*operator port*]

où :

- *protocol* est le protocole utilisé dans la connexion, tel que tcp, udp, ip, etc. Utilisez ? pour voir la liste des protocoles.
- (TCP/UDP uniquement) *operator* est l'un des suivants :
 - **eq** est égal au numéro de port spécifié.
 - **lt** désigne tout port inférieur au numéro de port spécifié.
 - **gt** désigne tout port supérieur au numéro de port spécifié.
 - **range** désigne tout port entre les deux ports spécifiés.
- (TCP/UDP uniquement.) *port* est le numéro de port, de 1 à 65 535 ou un mnémonique, tel que www. Utilisez ? pour voir les mnémoniques. Pour les plages, vous devez spécifier deux ports, le premier port étant un nombre inférieur au deuxième.

Étape 3

(Facultatif) Ajoutez une description (jusqu'à 200 caractères) : **description string**

Exemples

Configurez un ensemble d'applications SaaS à l'aide d'objets de service réseau définis précédemment.

```
object-group network-service SaaS_Applications
  description This group includes relevant 'Software as a Service' applications
  network-service-member "outlook 365"
  network-service-member webex
  network-service-member box
```

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 Créez ou modifiez un groupe d'objets utilisateur en utilisant le nom de l'objet : **object-group user group_name**

Exemple :

```
hostname(config)# object-group user admins
```

Étape 2 Ajoutez des utilisateurs et des groupes au groupe d'objets utilisateur à l'aide d'une ou de plusieurs des commandes suivantes. Utilisez la forme **no** de la commande pour supprimer un objet.

- **user** [domain_NETBIOS_name\]username : un nom d'utilisateur. S'il y a un espace dans le nom de domaine ou le nom d'utilisateur, vous devez placer le nom de domaine et le nom d'utilisateur entre guillemets. Le nom de domaine peut être LOCAL (pour les utilisateurs définis dans la base de données locale) ou un nom de domaine Active Directory (AD), comme spécifié dans la commande **user-identity domain domain_NetBIOS_name aaa-server aaa_server_group_tag**. Lors de l'ajout d'utilisateurs définis dans un domaine AD, *user_name* doit être le sAMAccountName d'Active Directory, qui est unique, plutôt que le nom commun (cn), qui peut ne pas être unique. Si vous ne spécifiez pas de nom de domaine, le nom par défaut est utilisé, qui est LOCAL ou celui défini dans la commande **user-identity default-domain**.
- **user-group** [domain_NETBIOS_name\]username : un groupe d'utilisateurs. S'il y a un espace dans le nom de domaine ou le nom du groupe, vous devez placer le nom de domaine et le nom du groupe entre guillemets. Notez le double \ qui sépare les noms de domaine et de groupe.
- **group-object** object_group_name : nom d'un groupe d'objets utilisateur existant.

Exemple :

```
hostname(config-user-object-group)# user EXAMPLE\admin
hostname(config-user-object-group)# user-group EXAMPLE\managers
hostname(config-user-object-group)# group-object local-admins
```

Étape 3 (Facultatif) Ajoutez une description : **description string**

Configurer les groupes d'objets 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 Créez ou modifiez un groupe d'objets de groupe de sécurité en utilisant le nom d'objet : **object-group security** *group_name*

Exemple :

```
hostname(config)# object-group security mktg-sg
```

Étape 2 Ajoutez des objets au groupe d'objets du groupe de services à l'aide d'une ou de plusieurs des commandes suivantes. Utilisez la forme **no** de la commande pour supprimer un objet.

- **security-group** {tag *sgt_number* | **name** *sg_name*} : balise de groupe de sécurité (SGT) ou nom. 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.
- **group-object** *object_group_name* : nom d'un groupe d'objets de groupe de sécurité existant.

Exemple :


```
hostname(config-security-object-group)# security-group tag 1
hostname(config-security-object-group)# security-group name mgkt
hostname(config-security-object-group)# group-object local-sg
```

Étape 3 (Facultatif) Ajoutez une description : **description** *string*

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 Créez la plage de temps: **time-range** *name*

Étape 2 (Facultatif) Ajoutez une heure de début ou de fin (ou les deux) à la plage temporelle.

absolute [**start** *time date*] [**end** *time date*]

Si vous ne spécifiez pas d'heure de début, l'heure de début par défaut est maintenant.

L'*heure* est au format 24 heures *hh:mm*. Par exemple, 8:00 correspond à 8 h et 20:00 à 20 h.

La *date* est au format *jour mois année*; par exemple, **1 janvier 2014**.

Étape 3 (Facultatif) Ajouter des périodes récurrentes.

periodic *days-of-the-week time to [days-of-the-week] time*

Vous pouvez spécifier les valeurs suivantes pour *days-of-the-week*. Notez que vous pouvez spécifier un deuxième jour de la semaine uniquement si vous spécifiez un seul jour pour le premier argument.

- **Monday, Tuesday, Wednesday, Thursday, Friday, Saturday**, ou **Sunday**. Vous pouvez en spécifier plusieurs, séparés par des espaces, pour le premier argument *days-of-the-week*.
- **tous les jours**
- **jours de la semaine**
- **fin de semaine**

L'heure est au format 24 heures *hh:mm*. Par exemple, 8:00 correspond à 8 h et 20:00 à 20 h.

Vous pouvez répéter cette commande pour configurer plusieurs périodes récurrentes.

Exemples

Voici un exemple de plage de temps absolue commençant à 8 h le 1/01/2006. Comme aucune heure et date de fin ne sont spécifiées, la plage temporelle est en vigueur indéfiniment.

```
hostname(config)# time-range for2006
hostname(config-time-range)# absolute start 8:00 1 january 2006
```

Voici un exemple de plage temporelle hebdomadaire de 8 h à 18 h en semaine :

```
hostname(config)# time-range workinghours
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
```

L'exemple suivant établit une date de fin pour la plage temporelle et définit une période en semaine de 8 h à 17 h, avec des heures différentes après 17 h pour lundi, mercredi, vendredi par rapport à mardi, jeudi.

```
asa4(config)# time-range contract-A-access
asa4(config-time-range)# absolute end 12:00 1 September 2025
asa4(config-time-range)# periodic weekdays 08:00 to 17:00
asa4(config-time-range)# periodic Monday Wednesday Friday 18:00 to 20:00
asa4(config-time-range)# periodic Tuesday Thursday 17:30 to 18:30
```

Surveillance des objets

Pour surveiller des objets et des groupes, entrez les commandes suivantes :

- **show access-list**

Affiche les entrées de la liste d'accès. Les entrées qui comprennent des objets sont également développées en entrées individuelles en fonction du contenu de l'objet.

- **show running-config object [id object_id]**

Affiche tous les objets actuels. Utilisez le mot-clé **id** pour afficher un seul objet par nom.

- **show running-config object object_type**

Affiche les objets actuels par type, **network** ou **service**.

- **show running-config object-group [id group_id]**

Affiche tous les groupes d'objets actuels. Utilisez le mot-clé **id** pour afficher un seul groupe d'objets par nom.

- **show running-config object-group grp_type**

Affiche les groupes d'objets actuels par type de groupe.

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. Nous avons introduit ou modifié les commandes suivantes : object-group protocol , object-group network , object-group service , object-group icmp_type .
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 .
Objets	8.3(1)	La prise en charge des objets a été introduite. Nous avons introduit ou modifié les commandes suivantes : object-network , object-service , object-group network , object-group service , network object , access-list extended , access-list webtype , access-list remark .
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. Nous avons introduit les commandes suivantes : object-network user , user .
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. Nous avons introduit les commandes suivantes : object-network security , security .
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. Nous avons modifié les commandes suivantes : object-group network .
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 commandes suivantes : access-list , extended , service-object , service .

Nom de la caractéristique	Observations Versions	Description
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 commandes suivantes : service-object, service.
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 commandes suivantes : access-list extended, app-id, clear configure object network-service, clear configure object-group network-service, clear dns ip-cache, clear object, clear object-group, debug network-service, description, dns trusted-source, domain, network-service-member, network-service reload, object-group network-service, object network-service, policy-route cost, set adaptive-interface cost, show asp table classify, show asp table network-service, show dns trusted-source, show dns ip-cache, show object, show object-group, show running-config, subnet.
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 3

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 53](#).

- [À propos des ACL, à la page 27](#)
- [Licences pour les ACL, à la page 32](#)
- [Lignes directrices pour les ACL, à la page 32](#)
- [Configurer les ACL, à la page 33](#)
- [Modifier les ACL dans une session de configuration isolée, à la page 48](#)
- [Surveiller les ACL, à la page 49](#)
- [Historique des ACL, à la page 50](#)

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. Consultez [Configurer les ACL étendues, à la page 34](#).
- **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 ACL EtherType, à la page 46](#).

- 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 42](#).
- 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 42](#).

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

Tableau 1 : 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.

Noms des 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 ACL 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.

Dans une ACL étendue, utilisez le paramètre **line** (ligne) *number* avec la commande **access-list** (liste d'accès) pour insérer les règles au bon endroit. Utilisez la commande **show access-list name** pour afficher les entrées d'ACL et leurs numéros de ligne afin de déterminer le bon numéro à utiliser. Pour les autres types d'ACL, vous devez recréer l'ACL (ou mieux, utiliser ASDM) pour modifier l'ordre des ACE.

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 la 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.

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 ACL 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).

```
hostname(config)# object network server1
hostname(config-network-object)# host 10.1.1.5
hostname(config-network-object)# nat (inside,outside) static 209.165.201.5

hostname(config)# access-list OUTSIDE extended permit tcp any host 10.1.1.5 eq www
hostname(config)# access-group OUTSIDE in interface outside
```

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 ACL

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.

Lignes directrices 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).

- (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. Lisez la section sur les bases d'ACL pour obtenir une vue d'ensemble, puis les sections sur des types spécifiques d'ACL pour les détails.

Options de base de configuration et de gestion de l'ACL

Une ACL est composée d'une ou de plusieurs entrées de contrôle d'accès (ACE) ayant le même ID ou le même nom d'ACL. Pour créer une nouvelle ACL, vous créez simplement une ACE avec un nouveau nom d'ACL, et elle devient la première règle de la nouvelle ACL.

En utilisant une liste de contrôle d'accès, vous pouvez effectuer les opérations suivantes :

Examiner le contenu de la liste de contrôle d'accès et déterminer les numéros de ligne et le nombre de correspondances

Utilisez la commande **show access-list name** pour afficher le contenu de la liste de contrôle d'accès. Chaque ligne est une entrée ACE et comprend le numéro de ligne, que vous aurez besoin de connaître si vous souhaitez insérer de nouvelles entrées dans une liste de contrôle d'accès étendue. Les informations comprennent également un nombre de correspondances pour chaque ACE, qui correspond au nombre de fois que la règle a été mise en correspondance avec le trafic. Par exemple :

```
hostname# show access-list outside_access_in
access-list outside_access_in; 3 elements; name hash: 0x6892a938
access-list outside_access_in line 1 extended permit ip 10.2.2.0 255.255.255.0 any
(hitcnt=0) 0xcc48b55c
access-list outside_access_in line 2 extended permit ip host
2001:DB8::0DB8:800:200C:417A any (hitcnt=0) 0x79797f94
access-list outside_access_in line 3 extended permit ip user-group
LOCAL\\usergroup any any (hitcnt=0) 0xb0f5b1e1
```

Ajouter une ACE

La commande pour ajouter une ACE est **access-list name [line line-num] type parameters**. L'argument du numéro de ligne ne fonctionne que pour les listes de contrôle d'accès étendues. Si vous incluez le numéro de ligne, l'ACE est insérée à cet emplacement dans la liste de contrôle d'accès, et l'ACE qui se trouve à cet emplacement est déplacée vers le bas, ainsi que le reste des ACE (c'est-à-dire que l'insertion d'une ACE à un numéro de ligne ne remplace pas l'ancienne ACE à cette ligne). Si vous n'incluez pas de numéro de ligne, l'ACE est ajoutée à la fin de l'ACL. Les paramètres disponibles varient selon le type d'ACL; consultez les rubriques spécifiques sur chaque type d'ACL pour en savoir plus.

Ajouter des commentaires à une liste de contrôle d'accès (tous les types, sauf webtype)

Utilisez la commande **access-list name [line line-num] remark text** pour ajouter des remarques dans une liste de contrôle d'accès afin de faciliter l'explication de l'objectif d'une ACE. Les bonnes pratiques sont d'insérer la remarque avant l'ACE; si vous affichez la configuration dans ASDM, les remarques seront associées à l'ACE qui suit les remarques. Vous pouvez saisir plusieurs remarques avant une ACE pour inclure un commentaire détaillé. Chaque remarque est limitée à 100 caractères. Vous pouvez inclure des espaces de début pour faciliter la mise en valeur des remarques. Si vous n'incluez pas de numéro de ligne, la remarque est ajoutée à la fin de la liste de contrôle d'accès. Par exemple, vous pourriez ajouter des remarques avant d'ajouter chaque ACE :

```
hostname(config)# access-list OUT remark - this is the inside admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT remark - this is the hr admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any
```

Modifier ou déplacer une ACE ou une remarque

Vous ne pouvez pas modifier ou déplacer une ACE ou une remarque. Au lieu de cela, vous devez créer une nouvelle ACE ou une remarque avec les valeurs souhaitées au bon emplacement (en utilisant le numéro de ligne), puis supprimer l'ancienne ACE ou l'ancienne remarque. Comme vous ne pouvez insérer des ACE que dans les listes de contrôle d'accès étendues, vous devez recréer les listes de contrôle d'accès standard, webtype ou EtherType si vous devez modifier ou déplacer des ACE. Il est beaucoup plus facile de réorganiser une liste de contrôle d'accès longue à l'aide d'ASDM.

Supprimer une ACE ou une remarque

Utilisez la commande **no access-list parameters** pour supprimer une ACE ou une remarque. Utilisez la commande **show access-list** pour afficher la chaîne de paramètres que vous devez saisir : la chaîne doit correspondre exactement à une ACE ou à une remarque pour la supprimer, à l'exception de l'argument **line line-num**, qui est facultatif dans la commande **no access-list**.

Supprimer une liste de contrôle d'accès complète, y compris les remarques

Utilisez la commande **clear configure access-list name**. ATTENTION La commande ne vous demande pas de confirmation. Si vous n'incluez pas de nom, toutes les listes d'accès de l'ASA sont supprimées.

Renommer une liste de contrôle d'accès

Utilisez la commande **access-list name rename new_name**.

Appliquer l'ACL à une politique

La création d'une liste de contrôle d'accès ne modifie pas à elle seule le trafic. Vous devez appliquer la liste de contrôle d'accès à une politique. Par exemple, vous pouvez utiliser la commande **access-group** pour appliquer une liste de contrôle d'accès étendue à une interface, refusant ou autorisant ainsi le trafic qui passe par l'interface.

Configurer les ACL étendues

Une ACL étendue est composée de toutes les ACE ayant le même ID ou le même nom d'ACL. Les Ajouter étendues sont le type d'ACL le plus complexe et le plus complet, et vous pouvez les utiliser pour de nombreuses fonctionnalités. L'utilisation la plus importante des ACL étendues est en tant que groupes d'accès appliqués globalement ou aux interfaces, qui déterminent le trafic qui sera refusé ou autorisé à passer par la boîte. Mais les ACL étendues sont également utilisées pour déterminer le trafic auquel d'autres services seront fournis.

Les ACL étendues étant complexes, les sections suivantes se concentrent sur la création d'ACE pour fournir des types spécifiques de correspondance de trafic. Les premières sections, sur les ACE basées sur les adresses de base et sur les ACE TCP/UDP, bâtissent les fondations pour les sections restantes.

Ajouter une ACE étendue pour la correspondance basée sur les adresses IP ou les noms de domaine complets

L'ACE étendue de base fait correspondre le trafic en fonction des adresses source et de destination, y compris les adresses IPv4 et IPv6 et les noms de domaine complets (FQDN), tels que `www.example.com`. En fait, chaque type d'ACE étendue doit inclure des spécifications pour l'adresse source et de destination. Cette rubrique explique donc l'ACE étendue minimale.



Astuces

Conseil : Si vous souhaitez mettre en correspondance le trafic en fonction d'un FQDN, vous devez créer un objet réseau pour chaque FQDN.

Pour ajouter une ACE pour la mise en correspondance des adresses IP ou des FQDN, utilisez la commande suivante :

```
access-list access_list_name [line line_number] extended {deny | permit} protocol_argument
source_address_argument dest_address_argument [log [[level]]] [interval secs] | disable |
default]] [time-range time_range_name] [inactive]
```

Exemple :

```
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-list ACL_IN extended permit object service-obj-http any any
```

Les options sont les suivantes :

- *access_list_name* : nom de la nouvelle ACL ou de l'ACL existante.
- Numéro de ligne : l'option **line***line_number* spécifie le numéro de ligne à laquelle insérer l'ACE; sinon, l'ACE est ajouté à la fin de l'ACL.
- Autoriser ou refuser : le mot-clé **deny** refuse ou exempte un paquet si les conditions sont remplies. Le mot-clé **permit** autorise ou inclut un paquet si les conditions correspondent.
- Protocole : *protocol_argument* spécifie le protocole IP. Si vous utilisez des groupes d'objets de service réseau qui précisent le protocole et les ports, vous devez préciser **ip** dans cet argument.
 - *name* or *number*(nom ou numéro) : spécifie le nom ou le numéro du protocole. Précisez **ip** pour appliquer à tous les protocoles.
 - **object-group** *protocol_grp_id* : spécifie un groupe d'objets de protocole créé à l'aide de la commande **object-group protocol**.
 - **object** *service_obj_id* : spécifie un objet de service créé à l'aide de la commande **object service**. L'objet peut inclure des spécifications de port ou de type ICMP et de code, si nécessaire.
 - **object-group** *service_grp_id* : spécifie un groupe d'objets de service créé à l'aide de la commande **object-group service**.

- Adresse source, adresse de destination : *source_address_argument* spécifie l'adresse IP ou le FQDN à partir duquel le paquet est envoyé, et *dest_address_argument* spécifie l'adresse IP ou le FQDN auquel le paquet est envoyé :
 - **host** *ip_address* : spécifie une adresse d'hôte IPv4.
 - *ip_address mask* : spécifie une adresse réseau et un filtre d'adresse locale IPv4, tels que 10.100.10.0 255.255.255.0.
 - *ipv6-address/prefix-length* : spécifie un hôte IPv6 ou une adresse réseau et un préfixe.
 - **any**, **any4**, et **any6** - **any** spécifie le trafic IPv4 et IPv6 ; **any4** spécifie uniquement le trafic IPv4 ; et **any6** spécifie uniquement le trafic IPv6.
 - **interface** *interface_name* : spécifie le nom d'une interface ASA. Utilisez le nom de l'interface plutôt que l'adresse IP pour faire correspondre le trafic en fonction de l'interface qui est la source ou la destination du trafic.
 - **object** *nw_obj_id* : spécifie un objet réseau créé à l'aide de la commande **object network**.
 - **object-group** *nw_grp_id* : spécifie un groupe d'objets réseau créé à l'aide de la commande **object-group network**.
 - **object-group-network-service** *name* : spécifie le nom d'un groupe d'objets de service réseau.
- Logging (Journalisation) : les arguments **log** définissent les options de journalisation lorsqu'une ACE correspond à une connexion pour l'accès réseau (une liste de contrôle d'accès appliquée avec la commande **access-group**). Si vous saisissez l'option **log** sans arguments, vous activez le message syslog 106100 au niveau par défaut (6) et pour l'intervalle par défaut (300 secondes). Les options de journalisation sont les suivantes :
 - **level** : un niveau de gravité entre 0 et 7. La valeur par défaut est 6 (informational). Si vous modifiez ce niveau pour une ACE active, le nouveau niveau s'applique aux nouvelles connexions; les connexions existantes continuent d'être journalisées au niveau précédent.
 - **interval** *secs* : intervalle de temps en secondes entre les messages syslog, de 1 à 600. La valeur par défaut est de 300 secondes. Cette valeur est également utilisée comme valeur de délai d'expiration pour supprimer un flux inactif de la mémoire cache qui recueille les statistiques d'abandon.
 - **disable** : désactive toute la journalisation ACE.
 - **default** : active la journalisation dans le message 106023 pour les paquets refusés. Ce paramètre est identique à l'option **log** non incluse.
- Time Range (Plage temporelle) : **time-range** l'option *time_range_name* spécifie un objet de plage temporelle, qui détermine les heures du jour et les jours de la semaine pendant lesquels l'ACE est active. Si vous ne spécifiez pas de plage temporelle, l'ACE est toujours actif.
- Activation : utilisez l'option **inactive** pour désactiver l'ACE sans le supprimer. Pour la réactiver, saisissez l'ACE complète sans le mot-clé **inactive**.

Ajoutez une ACE étendue pour la correspondance basée sur le port

Si vous spécifiez des objets de service dans une ACE, les objets de service peuvent inclure des protocoles avec des spécifications de port, comme TCP/80. Sinon, vous pouvez spécifier les ports directement dans

l'ACE. Grâce à la correspondance basée sur le port, vous pouvez cibler certains types de trafic pour les protocoles basés sur le port plutôt que tout le trafic pour le protocole.



Remarque Si vous utilisez des groupes d'objets de service réseau qui précisent le protocole et les ports, vous ne devez pas préciser les ports comme décrit dans cette rubrique. Précisez **ip** comme protocole afin que le protocole ou le port défini dans l'objet puisse correspondre.

L'ACE étendue basée sur le port est simplement l'ACE de base correspondant à l'adresse dont le protocole est **tcp**, **udp**, ou **sctp**. Pour ajouter des spécifications de port, utilisez la commande suivante :

```
access-list access_list_name [line line_number] extended {deny | permit} {tcp | udp | sctp}
source_address_argument [port_argument] dest_address_argument [port_argument] [log [[level]]] [interval
secs] | disable | default] [time-range time-range-name] [inactive]
```

Exemple :

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
```

L'option *port_argument* spécifie le port source ou de destination. Si vous ne spécifiez pas de port, tous les ports sont mis en correspondance. Les arguments disponibles sont les suivants :

- *operator port* : le *port* peut être l'entier ou le nom d'un port. L'*operator* peut être l'une des options suivantes :
 - **lt** : inférieur à
 - **gt** : supérieur à
 - **eq** : égal à
 - **neq** : différent de
 - **plage** : une plage inclusive de valeurs. Lorsque vous utilisez cet opérateur, spécifiez deux numéros de port, par exemple, **range 100 200**.



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.

- **object-group** *service_grp_id* : spécifie un groupe d'objets de service créé à l'aide de la commande **object-group service** {**tcp** | **udp** | **tcp-udp**}. Notez que ces types d'objets ne sont plus conseillés.

Vous ne pouvez pas spécifier les objets de service génériques recommandés, où le protocole et le port sont définis dans l'objet, comme arguments de port. Vous spécifiez ces objets dans le cadre de l'argument du protocole, comme expliqué dans [Ajouter une ACE étendue pour la correspondance basée sur les adresses IP ou les noms de domaine complets](#), à la page 35.

Pour obtenir une explication des autres mots-clés et comment utiliser les objets de service pour préciser les protocoles et les ports, consultez [Ajouter une ACE étendue pour la correspondance basée sur les adresses IP ou les noms de domaine complets](#), à la page 35.

Ajouter une ACE étendue pour la correspondance basée sur ICMP

Pour faire correspondre le trafic ICMP, utilisez l'un des mots-clés de protocole ICMP : **icmp** ou **icmp6**. Le protocole **icmp** correspond uniquement aux adresses IPv4, tandis que le protocole **icmp6** correspond uniquement aux adresses IPv6. Assurez-vous que vos adresses réseau correspondent au protocole que vous sélectionnez, sinon l'ACE ne correspondra à aucune connexion.

Si vous spécifiez des objets de service dans une ACE, les objets de service peuvent inclure des spécifications de type et de code ICMP des protocoles ICMP/ICMP6. Sinon, vous pouvez spécifier le type et le code ICMP directement dans l'ACE. Par exemple, vous pouvez cibler le trafic de demande d'écho ICMP (pings).

L'ACE étendue ICMP est simplement l'ACE de mise en correspondance d'adresses de base dont le protocole est **icmp** ou **icmp6**. Étant donné que ces protocoles ont des valeurs de type et de code, vous pouvez ajouter des spécifications de type et de code à l'ACE.

Pour ajouter une ACE pour la correspondance d'adresse IP ou de FQDN, où le protocole est ICMP ou ICMP6, utilisez la commande suivante :

```
access-list access_list_name [line line_number] extended {deny | permit} {icmp | icmp6}
source_address_argument dest_address_argument [icmp_argument] [log [[level]] [interval secs] | disable |
default]] [time-range time_range_name] [inactive]
```

Exemple :

```
hostname(config)# access-list abc extended permit icmp any any object-group obj_icmp_1
hostname(config)# access-list abc extended permit icmp any any echo
```

L'option *icmp_argument* spécifie le type et le code ICMP.

- **icmp_type** [*icmp_code*] : spécifie le type ICMP par nom ou par numéro, ainsi que le code ICMP facultatif pour ce type. Si vous ne spécifiez pas de code, tous les codes sont utilisés.
- **object-group** *icmp_grp_id* : spécifie un groupe d'objets pour ICMP/ICMP6 créé à l'aide de la commande (obsolète) **object-group icmp-type**.

Vous ne pouvez pas spécifier les objets de service génériques recommandés, où le protocole et le type sont définis dans l'objet, comme l'argument ICMP. Vous spécifiez ces objets dans le cadre de l'argument du protocole, comme expliqué dans [Ajouter une ACE étendue pour la correspondance basée sur les adresses IP ou les noms de domaine complets](#), à la page 35.

Pour obtenir une explication des autres mots-clés, consultez [Ajouter une ACE étendue pour la correspondance basée sur les adresses IP ou les noms de domaine complets](#), à la page 35.

Ajouter une ACE étendue pour la correspondance basée sur l'utilisateur (pare-feu d'identité)

L'ACE étendue basée sur l'utilisateur est simplement l'ACE de base pour la mise en correspondance d'adresses, dans laquelle vous incluez un nom d'utilisateur ou un groupe d'utilisateurs dans les critères de correspondance de la source. En créant des règles en fonction de l'identité de l'utilisateur, vous pouvez éviter d'associer des règles à des adresses d'hôte ou de réseau statiques. Par exemple, si vous définissez une règle pour user1 et que la fonctionnalité de pare-feu d'identité associe cet utilisateur à un hôte affecté à 10.100.10.3 un jour, mais à 192.168.1.5 le jour suivant, la règle basée sur l'utilisateur s'applique toujours.

Comme vous devez toujours fournir des adresses de source et de destination, élargissez l'adresse source pour inclure les adresses probablement attribuées à l'utilisateur (généralement par DHCP). Par exemple, l'utilisateur « LOCAL\user1 any » correspondra à l'utilisateur LOCAL\user1, quelle que soit l'adresse attribuée, alors

que « LOCAL\user1 10.100.1.0 255.255.255.0 » correspond à l'utilisateur uniquement si l'adresse se trouve sur le réseau 10.100.1.0/24.

En utilisant les noms de groupe, vous pouvez définir des règles pour des catégories entières d'utilisateurs, tels que les étudiants, les enseignants, les gestionnaires, les ingénieurs, etc.

Pour ajouter une ACE pour la mise en correspondance d'utilisateurs ou de groupes, utilisez la commande suivante :

```
access-list access_list_name [line line_number] extended {deny | permit} protocol_argument [user_argument]
source_address_argument [port_argument] dest_address_argument [port_argument] [log [[level]]] [interval
secs] | disable | default]] [time-range time_range_name] [inactive]
```

Exemple :

```
hostname(config) # access-list v1 extended permit ip user LOCAL\idfw
any 10.0.0.0 255.255.255.0
```

L'option *user_argument* spécifie l'utilisateur ou le groupe pour lequel mettre en correspondance le trafic en plus de l'adresse source. Les arguments disponibles sont les suivants :

- **object-group-user** *user_obj_grp_id* : spécifie un groupe d'objets utilisateur créé à l'aide de la commande **object-group user**.
- **user** {[*domain_nickname*]*name* | **any** | **none**} : spécifie un nom d'utilisateur. Précisez **any** pour correspondre à tous les utilisateurs avec des informations d'authentification d'utilisateur, ou **none** pour faire correspondre les adresses qui ne sont pas mappées aux noms d'utilisateurs. Ces options sont particulièrement utiles pour combiner les politiques de **correspondance access-group** et **aaa authentication**.
- **user-group** [*domain_nickname*]*user_group_name* : spécifie le nom d'un groupe d'utilisateurs. Notez la double barre oblique inverse (\) qui sépare le domaine et le nom de groupe.

Pour obtenir une explication des autres mots-clés, consultez [Ajouter une ACE étendue pour la correspondance basée sur les adresses IP ou les noms de domaine complets](#), à la page 35.



Astuces

Vous pouvez inclure à la fois des utilisateurs et des groupes de sécurité Cisco Trustsec dans une ACE donnée.

Ajouter une ACE étendue pour la correspondance basée sur un groupe de sécurité (Cisco TrustSec)

L'ACE étendue de groupe de sécurité (Cisco TrustSec) est simplement l'ACE de mise en correspondance d'adresses de base où vous incluez des groupes de sécurité ou des balises aux critères de correspondance de source ou de destination. En créant des règles en fonction de groupes de sécurité, vous pouvez éviter d'associer des règles à des adresses d'hôte ou de réseau statiques. Comme vous devez toujours fournir des adresses source et de destination, élargissez les adresses pour inclure les adresses qui seront probablement attribuées aux utilisateurs (généralement par DHCP).



Astuces

Avant d'ajouter ce type d'ACE, configurez Cisco TrustSec.

Pour ajouter une ACE pour la correspondance de groupe de sécurité, utilisez la commande suivante :

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument* [*security_group_argument*] *source_address_argument* [*port_argument*] [*security_group_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*]]] [**interval** *secs*] | **disable** | **default**] [**inactive** | **time-range** *time_range_name*]

Exemple :

```
hostname(config)# access-list INSIDE_IN extended permit ip
security-group name my-group any any
```

L'option *security_group_argument* spécifie le groupe de sécurité pour lequel mettre en correspondance le trafic en plus de l'adresse source ou de destination. Les arguments disponibles sont les suivants :

- **object-group-security** *security_obj_grp_id* : spécifie un groupe d'objets de sécurité créé à l'aide de la commande **object-group security**.
- **security-group** {**name** *security_grp_id* | **tag** *security_grp_tag*} : spécifie un nom ou une balise de groupe de sécurité.

Pour obtenir une explication des autres mots-clés, consultez [Ajouter une ACE étendue pour la correspondance basée sur les adresses IP ou les noms de domaine complets, à la page 35](#).



Astuces

Vous pouvez inclure à la fois des utilisateurs et des groupes de sécurité Cisco Trustsec dans une ACE donnée.

Exemples d'ACL étendues

La liste de contrôle d'accès suivante permet à tous les hôtes (sur l'interface à laquelle vous appliquez la liste de contrôle d'accès) de passer par l'ASA :

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

La liste de contrôle d'accès suivante empêche les hôtes de l'adresse 192.168.1.0/24 d'accéder au réseau 209.165.201.0/27 pour le trafic basé sur TCP. Toutes les autres adresses sont autorisées.

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

Si vous souhaitez restreindre l'accès aux hôtes sélectionnés uniquement, saisissez une autorisation ACE limitée. Par défaut, tout autre trafic est refusé, sauf autorisation explicite.

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

La liste de contrôle d'accès suivante restreint tous les hôtes (sur l'interface à laquelle vous appliquez la liste de contrôle d'accès) d'accéder à un site Web à l'adresse 209.165.201.29. Tout autre trafic est autorisé.

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

La liste de contrôle d'accès suivante, qui utilise des groupes d'objets, empêche plusieurs hôtes du réseau interne d'accéder à plusieurs serveurs Web. Tout autre trafic est autorisé.

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

L'exemple suivant désactive temporairement une liste de contrôle d'accès qui autorise le trafic d'un groupe d'objets réseau (A) vers un autre groupe d'objets réseau (B) :

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

Pour mettre en œuvre une ACE basée sur le temps, utilisez la commande **time-range** pour définir des heures spécifiques du jour et de la semaine. Utilisez ensuite la commande **access-list extended** pour lier la plage temporelle à une ACE. L'exemple suivant associe une ACE dans la liste de contrôle d'accès « Sales » à une plage temporelle nommée « New_York_Minute ».

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
```

L'exemple suivant montre une liste de contrôle d'accès mixte IPv4/IPv6 :

```
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 10.2.2.0
255.255.255.0
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 2001:DB8:2::/64
hostname(config)# access-list demoacl extended permit ip host 10.3.3.3 host 10.4.4.4
```

Exemple de conversion d'adresses en objets pour les ACL étendues

La liste de contrôle d'accès normale suivante qui n'utilise pas de groupes d'objets empêche plusieurs hôtes du réseau interne d'accéder à plusieurs serveurs Web. Tout autre trafic est autorisé.

```
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

Si vous créez deux groupes d'objets réseau, un pour les hôtes internes et un pour les serveurs Web, la configuration peut être simplifiée et peut être facilement modifiée pour ajouter d'autres hôtes :

```
hostname(config)# object-group network denied
hostname(config-network)# network-object host 10.1.1.4
hostname(config-network)# network-object host 10.1.1.78
hostname(config-network)# network-object host 10.1.1.89

hostname(config-network)# object-group network web
hostname(config-network)# network-object host 209.165.201.29
hostname(config-network)# network-object host 209.165.201.16
hostname(config-network)# network-object host 209.165.201.78

hostname(config)# access-list ACL_IN extended deny tcp object-group denied object-group
web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

Configurer les ACL standard

Une liste de contrôle d'accès standard est composée de toutes les ACE ayant le même ID ou le même nom d'ACL. Les listes de contrôle d'accès standard sont utilisées pour un nombre limité de fonctionnalités, telles que les listes de routage ou les filtres VPN. Une liste de contrôle d'accès standard utilise uniquement des adresses IPv4 et définit uniquement les adresses de destination.

Pour ajouter une entrée de liste d'accès standard, utilisez la commande suivante :

access-list *access_list_name* **standard** {**deny** | **permit**} {**any4** | **host** *ip_address* | *ip_address mask*}

Exemple :

```
hostname(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

Les options sont les suivantes :

- Nom : l'argument *access_list_name* spécifie le nom ou le numéro d'une ACL. Les numéros traditionnels pour les listes de contrôle d'accès standard sont de 1 à 99 ou de 1 300 à 1 999, mais vous pouvez utiliser n'importe quel nom ou numéro. Vous créez une nouvelle liste de contrôle d'accès si elle n'existe pas déjà, sinon, vous ajoutez l'entrée à la fin de l'ACL.
- Autoriser ou refuser : le mot-clé **deny** refuse ou exempte un paquet si les conditions sont remplies. Le mot-clé **permit** autorise ou inclut un paquet si les conditions correspondent.
- Adresse de destination : le mot-clé **any4** correspond à toutes les adresses IPv4. L'argument **host** *ip_address* correspond à une adresse IPv4 d'hôte. L'argument *ip_address ip_mask* correspond à un sous-réseau IPv4, par exemple, 10.1.1.0 255.255.255.0.

Configurer les ACL de type Web

Les ACL 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 ACL de type Web est composée de toutes les ACE ayant le même ID ou le même nom d'ACL.

Les ACL de type Web vous permettent de faire correspondre le trafic en fonction des URL ou des adresses de destination. Une seule ACE ne peut pas combiner ces spécifications. Les sections suivantes expliquent chaque type d'ACE.

Ajouter une ACE de type Web pour la correspondance d'URL

Pour faire correspondre le trafic en fonction de l'URL à laquelle l'utilisateur tente d'accéder, utilisez la commande suivante :

```
access-list access_list_name webtype {deny | permit} url {url_string | any} [log [[level] [interval secs] | disable | default]] [time_range time_range_name] [inactive]
```

Exemple :

```
hostname(config)# access-list acl_company webtype deny url http://*.example.com
```

Les options sont les suivantes :

- **access_list_name** : nom de la liste de contrôle d'accès nouvelle ou existante. Si l'ACL existe déjà, vous ajoutez l'ACE à la fin de l'ACL.
- Autoriser ou refuser : le mot-clé **deny** refuse ou exempte un paquet si les conditions sont remplies. Le mot-clé **permit** autorise ou inclut un paquet si les conditions correspondent.
- URL : le mot-clé **url** spécifie l'URL à mettre en correspondance. Utilisez **url any** pour faire correspondre tout le trafic basé sur des URL. Sinon, saisissez une chaîne d'URL, qui peut inclure des caractères génériques. Voici quelques conseils et limites sur la spécification des URL :
 - Précisez **any** pour qu'il corresponde à 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 « permit url any », 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]/**.

- **Journalisation** : les arguments **log** définissent les options de journalisation lorsqu'une ACE correspond à un paquet. Si vous saisissez l'option **log** sans arguments, vous activez le message syslog 106102 au niveau par défaut (6) et pour l'intervalle par défaut (300 secondes). Les options de journalisation sont les suivantes :
 - **level** : un niveau de gravité entre 0 et 7. La valeur par défaut est 6.
 - **interval secs** : intervalle de temps en secondes entre les messages syslog, de 1 à 600. La valeur par défaut est de 300 secondes.
 - **disable** : désactive toute la journalisation des ACL.
 - **default** : active la journalisation vers le message 106103. Ce paramètre est identique à ne pas inclure l'option **log**.
- **Option de plage de temps** – l'option **time-range time_range_name** spécifie un objet de plage temporelle, qui détermine les heures du jour et les jours de la semaine pendant lesquels l'ACE est actif. Si vous ne spécifiez pas de plage temporelle, l'ACE est toujours actif.
- **Activation** – utilisez l'option **inactive** pour désactiver l'ACE sans le supprimer. Pour la réactiver, saisissez l'ACE complète sans le mot-clé **inactive**.

Ajouter une ACE de type Web pour la correspondance d'adresses IP

Vous pouvez mettre en correspondance le trafic en fonction de l'adresse de destination à laquelle l'utilisateur tente d'accéder. L'ACL de type Web peut inclure une combinaison d'adresses IPv4 et IPv6 en plus des spécifications d'URL.

Pour ajouter une ACE de type Web pour la mise en correspondance des adresses IP, utilisez la commande suivante :

```
access-list access_list_name webtype {deny | permit} tcp dest_address_argument [operator port] [log  
[[level] [interval secs] | disable | default]] [time_range time_range_name]] [inactive]]
```

Exemple :

```
hostname(config)# access-list acl_company webtype permit tcp any
```

Pour obtenir une explication des mots-clés non expliqués ici, consultez [Ajouter une ACE de type Web pour la correspondance d'URL, à la page 43](#). Les mots-clés et les arguments spécifiques à ce type d'ACE sont les suivants :

- **tcp** : le protocole TCP. Les listes de contrôle d'accès de type Web correspondent uniquement au trafic TCP.
- **Adresse de destination** : le *dest_address_argument* précise l'adresse IP à laquelle le paquet est envoyé :
 - **host ip_address** : spécifie une adresse d'hôte IPv4.
 - **dest_ip_address masque** : spécifie une adresse réseau IPv4 et un masque de sous-réseau, tel que 10.100.10.0 255.255.255.0.
 - **ipv6-address/prefix-length** : spécifie un hôte IPv6 ou une adresse réseau et un préfixe.
 - **any, any4, et any6** : **any** spécifie le trafic IPv4 et IPv6 ; **any4** spécifie uniquement le trafic IPv4 ; et **any6** spécifie uniquement le trafic IPv6.

- *operator port* : le port de destination. Si vous ne spécifiez pas de ports, tous les ports sont mis en correspondance. Le *port* peut être l'entier ou le nom d'un port TCP. L'*opérateur* peut être l'une des options suivantes :
 - **lt** : inférieur à
 - **gt** : supérieur à
 - **eq** : égal à
 - **neq** : différent de
 - **range** : une plage inclusive de valeurs. Lorsque vous utilisez cet opérateur, spécifiez deux numéros de port, par exemple, **range 100 à 200**.

Exemples d'ACL de type Web

L'exemple suivant montre comment refuser l'accès à une URL d'entreprise spécifique :

```
hostname(config)# access-list acl_company webtype deny url http://*.example.com
```

L'exemple suivant montre comment refuser l'accès à une page Web spécifique :

```
hostname(config)# access-list acl_file webtype deny url https://www.example.com/dir/file.html
```

L'exemple suivant montre comment refuser l'accès HTTP à toute URL sur un serveur spécifique via le port 8080 :

```
hostname(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

Les exemples suivants montrent comment utiliser les caractères génériques dans les listes de contrôle d'accès de type Web.

- L'exemple suivant correspond à des URL telles que `http://www.example.com/layouts/1033`:

```
access-list VPN-Group webtype permit url http://www.example.com/*
```

- L'exemple suivant correspond à des URL telles que `http://www.example.com/` et `http://www.example.net/`:

```
access-list test webtype permit url http://www.example.*
```

- L'exemple suivant correspond à des URL telles que `http://www.example.com` et `ftp://wwwz.example.com`:

```
access-list test webtype permit url *://ww?.e*co*/
```

- L'exemple suivant correspond à des URL telles que `http://www.cisco.com:80` et `https://www.cisco.com:81`:

```
access-list test webtype permit url *://ww?.c*co*:8[01]/
```

L'opérateur de plage « [] » dans l'exemple précédent spécifie que les caractères **0** ou **1** peuvent se produire à cet emplacement.

- L'exemple suivant correspond à des URL telles que `http://www.example.com` et `http://www.example.net`:

```
access-list test webtype permit url http://www.[a-z]xample?*/
```

L'opérateur de plage « [] » dans l'exemple précédent spécifie que tout caractère dans la plage de **a** à **z** peut se produire.

- L'exemple suivant correspond aux URL `http` ou `https` qui comprennent « `cgi` » quelque part dans le nom ou le chemin d'accès du fichier.

```
access-list test webtype permit url htt*:///*/*cgi?*
```



Remarque Pour faire correspondre une URL `http`, vous devez saisir **`http:///*/*`** au lieu de `http://*`.

L'exemple suivant montre comment appliquer une liste de contrôle d'accès de type Web pour désactiver l'accès à des partages CIFS spécifiques.

Dans ce scénario, nous avons un dossier racine nommé « `shares` » qui contient deux sous-dossiers nommés « `Marketing_Reports` » et « `Sales_Reports` ». Nous souhaitons refuser spécifiquement l'accès au dossier « `shares/Marketing_Reports` ».

```
access-list CIFS_Avoid webtype deny url cifs://172.16.10.40/shares/Marketing_Reports.
```

Cependant, en raison du « refuser tout » implicite à la fin de la liste de contrôle d'accès, l'ACL ci-dessus rend tous les sous-dossiers inaccessibles (« `shares/Sales_Reports` » et « `shares/Marketing_Reports` »), y compris le dossier racine (« `shares` »).

Pour résoudre le problème, ajoutez une nouvelle liste de contrôle d'accès pour autoriser l'accès au dossier racine et aux sous-dossiers restants :

```
access-list CIFS_Allow webtype permit url cifs://172.16.10.40/shares*
```

Configurer les ACL EtherType

Les ACL EtherType s'appliquent au trafic de couche 2 non IP sur les interfaces membres de groupes 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 ACL EtherType vous permettent de contrôler le flux du trafic non IP dans le groupe de ponts. Notez que les trames au format 802.3 ne sont pas gérées par la liste de contrôle d'accès, car elles utilisent un champ de longueur par opposition à un champ de type.

Pour ajouter une EtherType ACE, utilisez la commande suivante :

```
access-list access_list_name ethertype {deny | permit} {any | bpdud | dsap {hex_address | bpdud | ipx | isis | raw-ipx} | eii-ipx | ipx | isis | mpls-multicast | mpls-unicast | hex_number}
```

Exemple :


```
hostname(config)# access-list ETHER ethertype deny mpls-multicast
```

Les options sont les suivantes :

- *access_list_name*—Le nom de la nouvelle ou existante ACL. Si l'ACL existe déjà, vous ajoutez l'ACE à la fin de l'ACL.
- Autoriser ou refuser : le mot-clé **deny** refuse un paquet si les conditions correspondent. Le mot-clé **permit** autorise un paquet si les conditions correspondent.
- Critères de correspondance du trafic : vous pouvez mettre en correspondance le trafic en utilisant les options suivantes :
 - **any** : correspond à tout le trafic de couche 2.
 - **bpdu** : unités de données de protocole de pont (dsap 0x42), qui sont autorisées par défaut. Ce mot-clé est converti en **dsap bpdu**.
 - **dsap {hex_address | bpdu | ipx | isis | raw-ipx}** : l'adresse du point d'accès au service de destination du paquet de contrôle de liaison logique IEEE 802.2. Incluez l'adresse que vous souhaitez autoriser ou refuser en format hexadécimal, de 0x01 à 0xff. Vous pouvez également utiliser les mots-clés suivants pour créer des règles pour les valeurs communes :
 - **bpdu** pour 0x42, unités de données de protocole de pont.
 - **ipx** pour 0xe0, Internet Packet Exchange (IPX) 802.2 LLC.
 - **isis** pour 0xfe, Intermediate System to Intermediate System (IS-IS).
 - **raw-ipx** pour 0xff, format brut IPX 802.3.
 - **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**.
 - **isis** : Intermediate System to Intermediate System (IS-IS). Ce mot-clé est converti en **dsap isis**.
 - **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.

Exemples d'ACL EtherType

Les exemples suivants montrent comment configurer les listes de contrôle d'accès EtherType, y compris comment les appliquer à une interface.

Par exemple, l'exemple d'ACL suivant permet les EtherTypes courants provenant de l'interface interne :

```
hostname(config)# access-list ETHER ethertype permit ipx
INFO: ethertype ipx is saved to config as ethertype eii-ipx
INFO: ethertype ipx is saved to config as ethertype dsap ipx
```

```
INFO: ethertype ipx is saved to config as ethertype dsap raw-ipx
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

L'exemple suivant autorise certains EtherTypes par l'ASA, mais il refuse tous les autres :

```
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

L'exemple suivant refuse le trafic avec EtherType 0x1256, mais autorise tous les autres sur les deux interfaces :

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group nonIP in interface inside
hostname(config)# access-group nonIP in interface outside
```

Modifier les ACL dans une session de configuration isolée

Lorsque vous modifiez une liste de contrôle d'accès utilisée pour les règles d'accès ou à toute autre fin, la modification est immédiatement mise en œuvre et a une incidence sur le trafic. Avec les règles d'accès, vous pouvez activer le modèle de validation transactionnelle pour vous assurer que les nouvelles règles ne deviennent actives qu'une fois la compilation des règles terminée, mais la compilation se produit après chaque ACE que vous modifiez.

Si vous souhaitez isoler davantage l'impact de la modification des listes de contrôle d'accès, vous pouvez apporter vos modifications dans une « session de configuration », qui est un mode isolé qui vous permet de modifier plusieurs ACE et objets avant de valider explicitement vos modifications. Ainsi, vous pouvez vous assurer que toutes les modifications prévues sont terminées avant de modifier le comportement du périphérique.

Avant de commencer

- Vous pouvez modifier les listes de contrôle d'accès référencées par une commande access-group, mais vous ne pouvez pas modifier les listes de contrôle d'accès référencées par une autre commande. Vous pouvez également modifier les listes de contrôle d'accès non référencées ou en créer de nouvelles.
- Vous pouvez créer ou modifier des objets et des groupes d'objets, mais si vous en créez un dans une session, vous ne pouvez pas le modifier dans la même session. Si l'objet n'est pas défini comme vous le souhaitez, vous devez valider vos modifications, puis modifier l'objet, ou ignorer la session complète et recommencer.
- Lorsque vous modifiez une liste de contrôle d'accès référencée par une commande access-group (règles d'accès), le modèle de validation transactionnelle est utilisé lorsque vous validez la session. Ainsi, l'ACL est complètement compilée avant que la nouvelle ACL ne remplace l'ancienne version.

Procédure

Étape 1 Démarrer une session.

```
hostname#configure session session_name  
hostname(config-s)#
```

Si *session_name* existe déjà, vous ouvrez cette session. Sinon, vous créez une nouvelle session.

Utilisez la commande **show configuration session** pour afficher les sessions existantes. Vous pouvez avoir au maximum 3 sessions actives à la fois. Si vous devez supprimer une ancienne session inutilisée, utilisez la commande **clear configuration session session_name**.

Si vous ne pouvez pas ouvrir une session existante parce que quelqu'un d'autre la modifie, vous pouvez effacer l'indicateur qui indique que la session est en cours de modification. Effectuez cette opération uniquement si vous êtes certain que la session n'est pas modifiée. Utilisez la commande **clear session session_name access** pour réinitialiser l'indicateur.

Étape 2 (Sessions non validées uniquement.) Apportez vos modifications. Vous pouvez utiliser les commandes de base suivantes avec n'importe quel paramètre :

- **Accès-Liste**
- **objet**
- **object-group**

Étape 3 Décidez que faire de la session. Les commandes disponibles dépendent de la validation précédente de la session. Les commandes possibles sont :

- **exit** : pour quitter simplement la session sans valider ni ignorer les modifications, afin de pouvoir revenir ultérieurement.
- **commit [noconfirm [revert-save | config-save]]** : (sessions non validées uniquement.) Validez vos modifications. Il vous est demandé si vous souhaitez enregistrer la session. Vous pouvez enregistrer la session de rétablissement (**revert-save**), ce qui vous permet d'annuler vos modifications à l'aide de la commande **revert**, ou de la session de configuration (**config-save**), qui comprend toutes les modifications apportées dans la session (vous permettant de valider les mêmes modifications à nouveau si vous le souhaitez). Si vous enregistrez la session de restauration ou de configuration, les modifications sont validées, mais la session reste active. Vous pouvez ouvrir la session et revenir ou valider les modifications. Vous pouvez éviter l'invite en incluant l'option **noconfirm** et, éventuellement, l'option d'enregistrement souhaitée.
- **abort** : (sessions non validées uniquement.) Pour abandonner vos modifications et supprimer la session. Si vous souhaitez conserver la session, quittez la session et utilisez la commande **clear session session_name configuration**, qui vide la session sans la supprimer.
- **revert** : (sessions validées uniquement.) Pour annuler vos modifications, rétablissez la configuration à ce qu'elle était avant de valider la session, puis supprimez la session.
- **show configuration session [session_name]** : pour afficher les modifications apportées dans la session.

Surveiller les ACL

Pour superviser les ACLs, saisissez l'une des commandes suivantes :

- **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 ACL sont utilisées pour contrôler l'accès au réseau ou pour spécifier le trafic pour de nombreuses fonctionnalités à utiliser. 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 ACL de type Web sont utilisées dans le filtrage VPN SSL sans client. Les ACL EtherType contrôlent le trafic de couche 2 non IP. Nous avons lancé les commandes suivantes : access-list extended, access-list standard, access-list webtype, access-list ethertype.
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. Nous avons modifié les commandes suivantes : access-list extended.
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 contrôler le trafic IS-IS à l'aide d'une liste de contrôle d'accès EtherType. Nous avons modifié la commande suivante : access-list ethertype {permit deny} isis.
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. Nous avons modifié les commandes suivantes : access-list extended.

Nom de la caractéristique	Versions	Description
ACL unifiées étendues et de type Web pour IPv4 et IPv6	9.0(1)	Les ACL 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 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 commandes suivantes : access-list extended, access-list webtype. Nous avons supprimé les commandes suivantes : ipv6 access-list, ipv6 access-list webtype, ipv6-vpn-filter.
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 commandes suivantes : access-list extended, service-object, service.
Session de configuration pour modifier les listes de contrôle d'accès et les objets. Référencement ultérieur des objets et des ACL 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. Nous avons introduit les commandes clear configuration session, clear session, configure session, forward-reference et show configuration session.
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 la commande suivante : access-list extended.
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. Rewrite bpdu rules for dsap 0x42. Nous avons modifié les commandes suivantes : access-list 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 commandes suivantes : access-group, access-list ethertype.

Nom de la caractéristique	Versions	Description
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 commandes suivantes : access-list ethertype a ajouté les nouveaux mots clés eii-ipx et dsap {bpd ipx isis raw-ipx}; capture ethernet-type ne prend plus en charge le mot clé ipx.
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 la commande suivante : access-list extended.
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 <i>nouveaux</i> 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 4

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 53](#)
- [Licences pour les règles d'accès, à la page 59](#)
- [Lignes directrices relatives au contrôle d'accès, à la page 59](#)
- [Configurer le contrôle d'accès, à la page 61](#)
- [Surveillance des règles d'accès, à la page 64](#)
- [Exemples de configuration pour autoriser ou refuser l'accès au réseau, à la page 66](#)
- [Historique des règles d'accès, à la page 67](#)

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 :

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

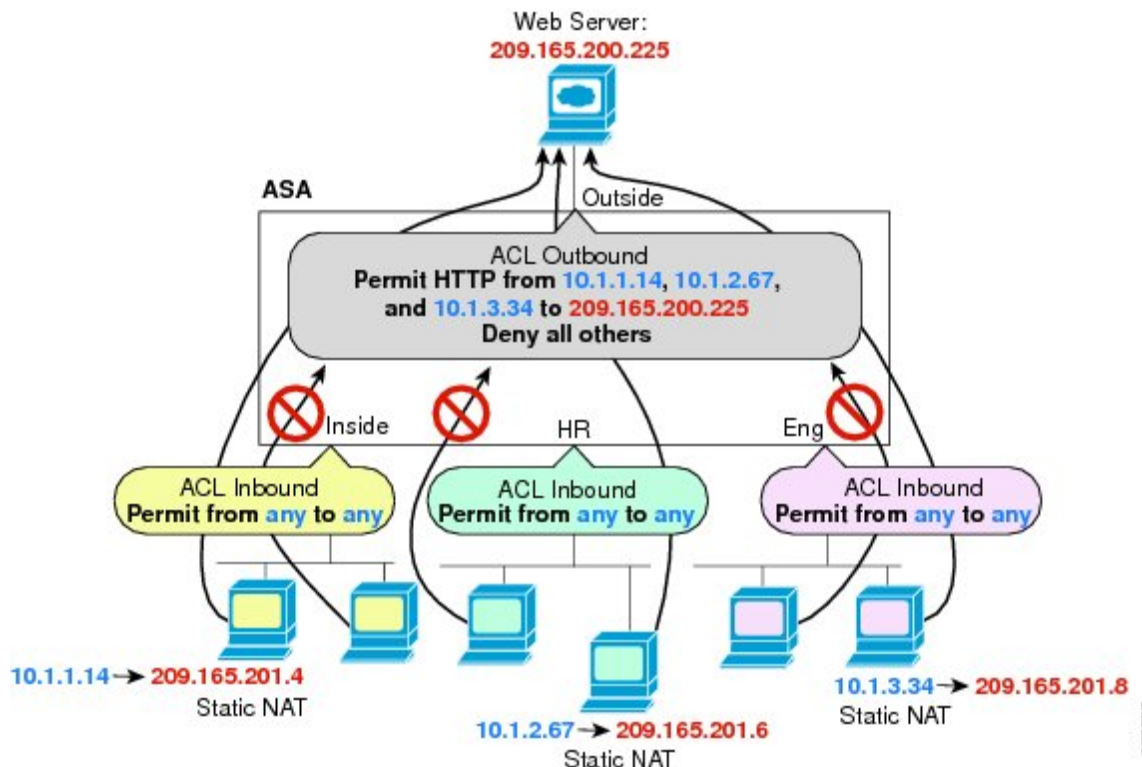


Remarque

« 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



Consultez les commandes suivantes pour cet exemple :

```
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.1.14 host 209.165.200.225
eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.2.67 host 209.165.200.225
eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.3.34 host 209.165.200.225
eq www
hostname(config)# access-group OUTSIDE out interface outside
```

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 permit 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 de contrôle 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 2 : 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 (défini par des commandes telles que **http**, **ssh**, ou **telnet**) ont une priorité plus élevée qu'une règle d'accès de gestion appliquée avec l'option **control-plane**. 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

Lignes directrices pour IPv6

Prend en charge IPv6. Les adresses de source et de destination peuvent inclure n'importe quelle combinaison d'adresses IPv4 et IPv6.

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.

Lignes directrices 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 à l'aide de la commande **object-group-search access-control**.

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. Elle 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. Utilisez la commande **asp rule-engine transactional-commit access-group**.
- 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.

- 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 un groupe d'accès

Avant de pouvoir créer un groupe d'accès, créez la liste de contrôle d'accès.

Pour lier une liste de contrôle d'accès à une interface ou pour l'appliquer globalement, utilisez la commande suivante :

access-group *access_list* { {in | out} **interface** *interface_name* [**per-user-override** | **control-plane**] | **global** }

Pour un groupe d'accès spécifique à l'interface :

- Précisez le nom de l'ACL étendue ou EtherType. Vous pouvez configurer une commande **access-group** par type d'ACL, interface et direction, ainsi qu'une ACL de plan de contrôle. L'ACL de plan de contrôle doit être une ACL étendue. Les ACL EtherType sont autorisées sur les interfaces de membres de groupe de ponts uniquement. Pour les groupes de ponts en mode routé, vous pouvez spécifier des listes de

contrôle d'accès étendues pour chaque direction sur l'interface virtuelle de pont (BVI) et chaque interface de membre de groupe de ponts.

- Le mot-clé **in** applique l'ACL au trafic entrant. Le mot-clé **out** applique l'ACL au trafic sortant.
- Précisez le nom **de l'interface**.
- Le mot-clé **per-user-override** (pour les ACL étendues entrantes uniquement) permet aux ACL d'utilisateur dynamiques qui sont téléchargées pour l'autorisation de l'utilisateur de remplacer l'ACL attribuée à l'interface. Par exemple, si l'ACL de l'interface refuse tout le trafic de 10.0.0.0, mais que l'ACL dynamique autorise tout le trafic de 10.0.0.0, l'ACL dynamique remplace l'ACL de l'interface pour cet utilisateur.

Par défaut, le trafic d'accès à distance du VPN ne correspond pas aux listes de contrôle d'accès d'interface. Toutefois, si vous utilisez la commande **no sysopt connection permit-vpn** pour désactiver ce contournement, le comportement dépend de l'application d'un **vpn-filter** dans la stratégie de groupe et de la définition de l'option **per-user-override** :

- Aucun **per-user-override**, aucun **vpn-filter** : le trafic est comparé à l'ACL de l'interface.
 - Aucun **per-user-override**, **vpn-filter** : le trafic est d'abord comparé à l'ACL de l'interface, puis au filtre VPN.
 - **per-user-override**, **vpn-filter** : le trafic est comparé au filtre VPN uniquement.
 - Le mot-clé **control-plane** spécifie si l'ACL étendue est destinée au trafic 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 (plan de contrôle) 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 un groupe d'accès global, spécifiez le mot-clé **global** pour appliquer l'ACL étendue à la direction entrante de toutes les interfaces.

Exemple

L'exemple suivant montre comment utiliser la commande **access-group** :

```
hostname(config)# access-list outside_access permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group outside_access in interface outside
```

La commande **access-list** permet à tout hôte d'accéder à l'adresse de l'hôte en utilisant le port 80. La commande **access-group** précise que la commande **access-list** s'applique au trafic entrant dans l'interface externe.

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

Créez des règles pour le trafic ICMP.

icmp {permit | deny} {host ip_address | ip_address mask | any} [icmp_type] interface_name

Si vous ne spécifiez pas de *icmp_type*, la règle s'applique à tous les types. Vous pouvez saisir le numéro ou le nom. Pour contrôler ping, spécifiez echo-reply (0) (ASA-to-host) ou echo (8) (host-to-ASA).

Pour l'adresse, vous pouvez appliquer la règle à **any** adresse, à un **hôte** unique ou à un réseau (*ip_address mask*).

Étape 2

Créez des règles pour le trafic ICMPv6 (IPv6).

ipv6 icmp {permit | deny} {host ipv6_address | ipv6-network/prefix-length | any} [icmp_type] interface_name

Si vous ne spécifiez pas de *icmp_type*, la règle s'applique à tous les types.

Pour l'adresse, vous pouvez appliquer la règle à **any** adresse, à un **hôte** unique ou à un réseau (*ipv6-network/prefix-length*).

Étape 3

(Facultatif) Définissez des limites de débit sur les messages ICMP inaccessibles afin que l'ASA apparaisse sur la sortie de la route de trace.

icmp unreachable rate-limit rate burst-size size

La limite de débit peut aller de 1 à 100, 1 étant la valeur par défaut. La taille de rafale peut être comprise entre 1 et 10. Le nombre de réponses de la taille de rafale est envoyé, mais les réponses suivantes ne sont pas envoyées tant que la limite de débit n'est pas atteinte.

Exemple :

Augmenter la limite de débit, ainsi qu'activer la commande **set connection decrement-ttl** dans une politique de service, est nécessaire pour permettre un traceroute à travers l'ASA qui montre l'ASA comme l'un des sauts. Par exemple, la politique suivante augmente la limite de débit et décrémente la valeur de durée de vie (TTL) pour tout le trafic via l'ASA.

```
icmp unreachable rate-limit 50 burst-size 10
class-map global-class
  match any
policy-map global_policy
  class global-class
```

```
set connection decrement-ttl
```

Exemples

L'exemple suivant montre comment autoriser tous les hôtes, à l'exception de celui à 10.1.1.15, à utiliser ICMP pour l'interface interne :

```
hostname(config)# icmp deny host 10.1.1.15 inside
hostname(config)# icmp permit any inside
```

L'exemple suivant montre comment autoriser l'hôte à 10.1.1.15 à utiliser uniquement le message ping vers l'interface interne :

```
hostname(config)# icmp permit host 10.1.1.15 inside
```

L'exemple suivant montre comment refuser toutes les demandes ping et autoriser tous les messages packet-too-big (pour prendre en charge la découverte de MTU du chemin) sur l'interface externe :

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

L'exemple suivant montre comment autoriser l'hôte 2000:0:0:4::2 ou les hôtes du préfixe 2001::/64 à envoyer un message ping à l'interface externe :

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

Surveillance des règles d'accès

Pour surveiller l'accès au réseau, entrez les commandes suivantes :

- **clear access-list *id* counters**

Efface le nombre d'accès de la liste d'accès.

- **show access-list [*name*]**

Affiche les listes d'accès, y compris le numéro de ligne de chaque ACE et le nombre d'accès. Incluez un nom d'ACL ou vous verrez toutes les listes d'accès.

- **show running-config access-group**

Affiche l'ACL actuelle liée aux interfaces.

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 à l'aide de la commande **access-list alert-interval secs** et le nombre maximal de flux de refus mis en cache à l'aide de la commande **access-list deny-flow-max number**.

Exemples de configuration pour autoriser ou refuser l'accès au réseau

Voici quelques exemples de configuration typiques pour autoriser ou refuser l'accès au réseau.

Exemples d'ACL étendues

L'exemple suivant ajoute un objet réseau pour le serveur interne 1, effectue une NAT statique pour le serveur et permet l'accès de l'extérieur pour le serveur interne 1.

```
hostname(config)# object network inside-server1
hostname(config)# host 10.1.1.1
hostname(config)# nat (inside,outside) static 209.165.201.12

hostname(config)# access-list outside_access extended permit tcp any object inside-server1
eq www
hostname(config)# access-group outside_access in interface outside
```

L'exemple suivant permet à tous les hôtes de communiquer entre les réseaux interne et RH, mais uniquement des hôtes spécifiques d'accéder au réseau externe :

```
hostname(config)# access-list ANY extended permit ip any any
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any

hostname(config)# access-group ANY in interface inside
hostname(config)# access-group ANY in interface hr
hostname(config)# access-group OUT out interface outside
```

L'exemple suivant utilise des groupes d'objets pour autoriser un trafic spécifique sur l'interface interne :

```
!
hostname (config)# object-group service myaclog
hostname (config-service)# service-object tcp source range 2000 3000
hostname (config-service)# service-object tcp source range 3000 3010 destination$
hostname (config-service)# service-object ipsec
hostname (config-service)# service-object udp destination range 1002 1006
hostname (config-service)# service-object icmp echo

hostname(config)# access-list outsideacl extended permit object-group myaclog interface
inside any
```

Exemples EtherType

Par exemple, l'exemple d'ACL suivant permet les EtherTypes courants provenant de l'interface interne :

```
hostname(config)# access-list ETHER ethertype permit ipx
INFO: ethertype ipx is saved to config as ethertype eii-ipx
INFO: ethertype ipx is saved to config as ethertype dsap ipx
INFO: ethertype ipx is saved to config as ethertype dsap raw-ipx
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

L'exemple suivant autorise certains EtherTypes par l'ASA, mais il refuse tous les autres :

```
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

L'exemple suivant refuse le trafic avec EtherType 0x1256, mais autorise tous les autres sur les deux interfaces :

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group nonIP in interface inside
hostname(config)# access-group nonIP in interface outside
```

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 la commande suivante : access-group .
Critères d'accès globaux	8.3(1)	Des règles d'accès globales ont été introduites. Nous avons modifié la commande suivante : access-group .
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. Nous avons modifié les commandes suivantes : access-list extended .
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 la commande suivante : access-list ethertype {permit deny} isis .
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. Nous avons modifié les commandes suivantes : access-list extended .

Nom de la caractéristique	Versions de plateforme	Description
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 commandes suivantes : access-list extended, access-list webtype. Nous avons supprimé les commandes suivantes : ipv6 access-list, ipv6 access-list webtype, ipv6-vpn-filter
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 commandes suivantes : access-list extended, service-object, service.
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 les commandes suivantes : asp rule-engine transactional-commit, show running-config asp rule-engine transactional-commit, clear configure asp rule-engine transactional-commit.
Session de configuration pour modifier les ACL et les objets. Référencement ultérieur des objets et des ACL 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. Nous avons introduit les commandes clear config-session, clear session, configure session, forward-reference, et show config-session.
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 la commande suivante : access-list extended.
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. Rewrite bpdu rules for dsap 0x42. Nous avons modifié les commandes suivantes : access-list ethertype

Nom de la caractéristique	Versions de plateforme	Description
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 commandes suivantes : access-group, access-list 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 commandes suivantes : access-list ethertype a ajouté les nouveaux mots clés eii-ipx et dsap {bpdu ipx isis raw-ipx}; capture ethernet-type ne prend plus en charge le mot clé ipx.
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 ajouté la commande suivante : object-group-search threshold.
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 <i>nouveaux</i> 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 71](#)
- [Lignes directrices relatives à Cisco TrustSec, à la page 79](#)
- [Configurer l'ASA pour s'intégrer à Cisco TrustSec, à la page 82](#)
- [Exemple pour Cisco TrustSec, à la page 96](#)
- [Prise en charge des VPN sécurisés\) pour Cisco TrustSec, à la page 97](#)
- [Surveillance de Cisco TrustSec, à la page 98](#)
- [Historique de Cisco TrustSec, à la page 100](#)

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 par Cisco TrustSec pour propager la base de données de mappage IP-SGT entre les 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 commande, transmet le mappage IP-SGT des points d'authentification (comme les commutateurs de couche d'accès existants) aux périphériques en amont dans le 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

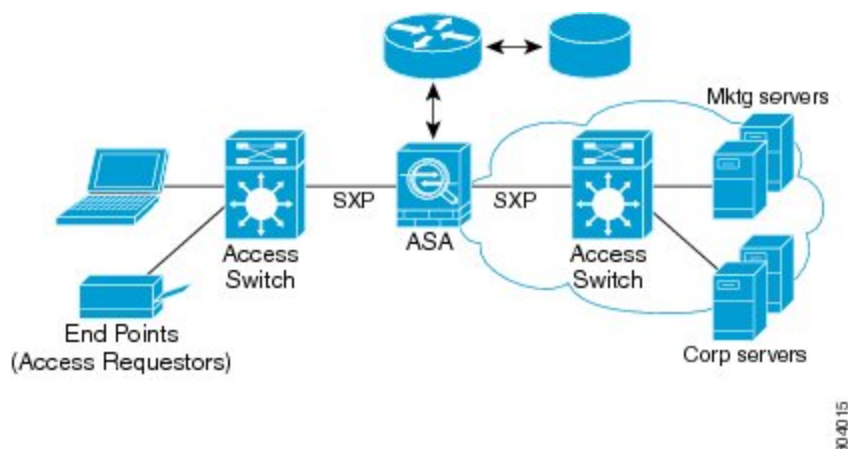
L'application de la politique de sécurité est basée sur le nom du groupe de sécurité. Un périphérique terminal tente d'accéder à une ressource dans le centre de données. Par rapport aux politiques traditionnelles basées sur IP configurées sur les pare-feu, les politiques basées sur l'identité sont configurées 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.

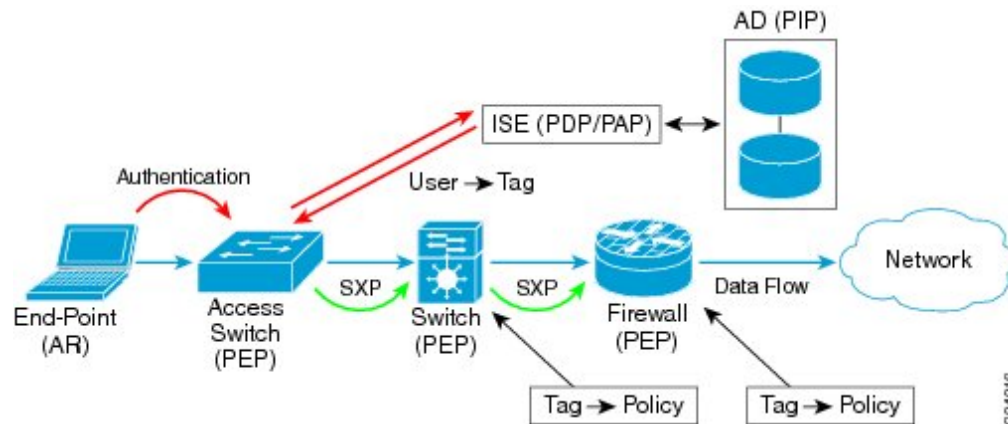
Pour configurer l'ASA pour qu'il fonctionne avec Cisco TrustSec, vous devez importer un fichier d'identifiant d'accès protégé (PAC) à partir de l'ISE.

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 du temporisateur 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 devenir 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 sécurité 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 de la balise de groupe de sécurité 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.

Lignes directrices supplémentaires

- L'ASA prend en charge SXP version 3. L'ASA négocie les versions de SXP avec différents périphériques réseau compatibles avec SXP.
- Vous pouvez configurer l'ASA pour actualiser la table de groupes de sécurité à l'expiration du temporisateur de resynchronisation SXP et télécharger la table de groupes 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 78](#)
- [Créer un groupe de sécurité sur l'ISE, à la page 78](#)
- [Générer le fichier PAC, à la page 79](#)

Procédure

-
Étape 1	Configurer le serveur AAA pour l'intégration de Cisco TrustSec, à la page 83
Étape 2	Importer un fichier PAC, à la page 85

- Étape 3** [Configurer le protocole d'échange de sécurité, à la page 86](#)
Cette tâche active et définit les valeurs par défaut pour SXP.
- Étape 4** [Ajouter un homologue de connexion SXP, à la page 88](#)
- Étape 5** [Actualiser les données d'environnement, à la page 90](#)
Effectuez cette opération selon les besoins.
- Étape 6** [Configurer la politique de sécurité, à la page 90](#)
- Étape 7** [Configurer l'imposition du balisage de groupe de sécurité de couche 2, à la page 92](#)
-

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 d'ISE. Communiquez avec votre administrateur ISE pour obtenir ces informations.

Procédure

- Étape 1** Créez le groupe de serveurs AAA et configurez les paramètres de serveur AAA pour que l'ASA communique avec le serveur ISE.
- aaa-server** *server_tag* **protocol** **radius**
- Exemple :**
- ```
ciscoasa(config)# aaa-server ISEserver protocol radius
```
- L'argument *server-tag* spécifie le nom du groupe de serveurs.
- Étape 2**      Quittez le mode de configuration de groupe de serveurs aaa.
- exit**
- Exemple :**
- ```
ciscoasa(config-aaa-server-group)# exit
```
- Étape 3** Configurez un serveur AAA dans le cadre d'un groupe de serveurs AAA et définissez des données de connexion spécifiques à l'hôte.

```
ciscoasa(config)# aaa-server server-tag(interface-name) host server-ip
```

Exemple :

```
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
```

L'argument *interface-name* spécifie l'interface réseau dans laquelle se trouve le serveur ISE. Les parenthèses sont requises dans ce paramètre. L'argument *server-tag* est le nom du groupe de serveurs AAA. L'argument *server-ip* spécifie l'adresse IP du serveur ISE.

Étape 4 Spécifiez la valeur de clé secrète de serveur utilisée pour authentifier l'ASA auprès du serveur ISE.

```
key key
```

Exemple :

```
ciscoasa(config-aaa-server-host)# key myexclusivekey
```

L'argument *de clé* est un mot-clé alphanumérique de 127 caractères maximum.

Si ISE est également utilisé pour l'authentification des utilisateurs, saisissez le secret partagé qui a été saisi sur ISE lorsque vous avez enregistré l'ASA auprès d'ISE.

Étape 5 Quittez le mode de configuration de l'hôte du serveur AAA.

```
exit
```

Exemple :

```
ciscoasa(config-aaa-server-host)# exit
```

Étape 6 Déterminez le groupe de serveurs AAA utilisé par Cisco TrustSec pour la récupération des données d'environnement.

```
cts server-group AAA-server-group-name
```

Exemple :

```
ciscoasa(config)# cts server-group ISEserver
```

L'argument *AAA-server-group-name* est le nom du groupe de serveurs AAA que vous avez spécifié à l'étape 1 dans l'argument *server-tag*.

Remarque

Vous ne pouvez configurer qu'une seule instance du groupe de serveurs sur l'ASA pour Cisco TrustSec.

L'exemple suivant montre comment configurer l'ASA pour qu'il communique avec le serveur ISE pour l'intégration de Cisco TrustSec :

```
ciscoasa(config)#aaa-server ISEserver protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
```

```
ciscoasa(config-aaa-server-host)# exit  
ciscoasa(config)# cts server-group ISEserver
```

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

Importer un fichier PAC Cisco TrustSec.

cts import-pac *filepath* **password** *value*

Exemple :

```
ciscoasa(config)# cts import-pac disk0:/xyz.pac password IDFW-pac99
```

L'argument *value* spécifie 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. L'argument *filepath* est saisi comme l'une des options suivantes :

Mode unique

- **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

Multi-mode

- **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

L'exemple suivant montre comment importer un fichier PAC dans l'ASA :

```
ciscoasa(config)# cts import pac disk0:/pac123.pac password hideme
PAC file successfully imported
```

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 Activez SXP sur l'ASA. Par défaut, SXP est désactivé.

cts sxp enable

Exemple :

```
ciscoasa(config)# cts sxp enable
```

Étape 2 (Facultatif ; non recommandé.) Configurez l'adresse IP source par défaut pour les connexions SXP.

cts sxp default source-ip ipaddress

Exemple :

```
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
```

L'argument *ipaddress* peut être une adresse IPv4 ou IPv6.

Lorsque vous configurez une adresse IP source par défaut pour les connexions SXP, vous devez spécifier la même adresse que l'interface sortante ASA. Si l'adresse IP source ne correspond pas à l'adresse de l'interface sortante, les connexions SXP échouent.

Lorsqu'une adresse IP source pour une connexion SXP n'est pas configurée, l'ASA effectue une recherche de routage/ARP pour déterminer l'interface sortante pour la connexion SXP. 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 3

(Facultatif) Configurez 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.

```
cts sxp default password [0 | 8] password
```

Exemple :

```
ciscoasa(config)# cts sxp default password 8 IDFW-TrustSec-99
```

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.

La longueur du mot de passe dépend du niveau de déchiffrement, qui prend la valeur 0 par défaut si vous ne le spécifiez pas :

- **0** : texte en clair non chiffré. Le mot de passe peut comporter jusqu'à 80 caractères.
- **8** : texte chiffré. Le mot de passe peut comporter jusqu'à 162 caractères.

Étape 4

(Facultatif) Précisez l'intervalle de temps entre les tentatives de l'ASA pour configurer de nouvelles connexions SXP entre les homologues SXP.

```
cts sxp retry period timervalue
```

Exemple :

```
ciscoasa(config)# cts sxp retry period 60
```

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 le temporisateur de nouvelle tentative à une valeur différente de celle des périphériques homologues SXP.

Étape 5

(Facultatif) Précisez la valeur du temporisateur de resynchronisation.

```
cts sxp reconciliation period timervalue
```

Exemple :

```
ciscoasa(config)# cts sxp reconciliation period 60
```

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

À l'expiration du temporisateur de resynchronisation, 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 du temporisateur de resynchronisation, 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 6

(Facultatif) Configurez le temporisateur de maintien de suppression pour les mappages IP-SGT appris d'un homologue après qu'un homologue SXP ait mis fin à sa connexion SXP.

cts sxp delete-hold-down period *timervalue*

La valeur du temporisateur spécifie le nombre de secondes, de 120 à 64 000, pendant lesquelles les mappages IP-SGT appris d'une connexion SXP interrompue sont conservés avant d'être supprimés.

Exemple :

```
ciscoasa(config)# cts sxp delete-hold-down period 240
```

Chaque connexion SXP est associée à un temporisateur de maintien de suppression. Ce temporisateur est déclenché lorsqu'une connexion SXP du côté de l'écouteur est interrompue. Les mappages IP-SGT appris de cette connexion SXP ne sont pas supprimés immédiatement. Au lieu de cela, ils sont conservés jusqu'à l'expiration du temporisateur de maintien de suppression. Les mappages sont supprimés à l'expiration de ce temporisateur.

Étape 7

(Facultatif) Configurez la profondeur d'expansion du sous-réseau IPv4 lorsque l'ASA agit en tant que speaker pour des homologues utilisant SXPv2 ou une version antérieure.

cts sxp mapping network-map *maximum_hosts*

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.

Ajouter un homologue de connexion SXP

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

Procédure

Établissez une connexion SXP avec un homologue SXP.

cts sxp connection peer *peer_ip_address* [**source** *source_ip_address*] **password** {**default** | **none**} [**mode** {**local** | **peer**}] {**speaker** | **listener**}

Exemple :

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker
```

Les connexions SXP sont définies par adresse IP; une seule paire de périphériques peut assurer plusieurs connexions SXP.

L'argument *peer_ip_address* est 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.

L'argument *source_ip_address* est l'adresse locale IPv4 ou IPv6 de la connexion SXP. L'adresse IP source doit être la même que celle de l'interface sortante de l'ASA, sinon la connexion échoue.

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.

Indiquez s'il faut utiliser ou non la clé d'authentification pour la connexion SXP :

- **default** : utilisez le mot de passe par défaut configuré pour les connexions SXP.
- **none** : n'utilisez pas de mot de passe pour la connexion SXP.

Indiquez le mode de la connexion SXP :

- **local** : utilisez le périphérique SXP local.
- **peer** : utilisez le périphérique SXP homologue.

Indiquez si l'ASA fonctionne comme speaker ou comme listener pour la connexion SXP.

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

L'exemple suivant montre comment configurer les homologues SXP sur l'ASA :

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default  
mode peer speaker  
ciscoasa(config)# cts sxp connection peer 192.168.1.101 password default  
mode peer speaker
```

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

Actualisez les données d'environnement depuis l'ISE et réinitialisez le temporisateur de resynchronisation à la valeur par défaut configurée.

```
cts refresh environment-data
```

Exemple :

```
ciscoasa(config)# cts refresh environment-data
```

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 une liste de contrôle d'accès étendue, consultez [Ajouter une ACE étendue pour la correspondance basée sur un groupe de sécurité \(Cisco TrustSec\)](#), à la page 39.

- Pour configurer les groupes d'objets de groupe de sécurité qui peuvent être utilisés dans l'ACL, consultez [Configurer les groupes d'objets de sécurité, à la page 22](#).

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.

L'exemple suivant montre comment créer une liste de contrôle d'accès qui utilise un groupe d'objets de sécurité défini localement :

```
object-group security objgrp-it-admin
  security-group name it-admin-sg-name
  security-group tag 1
object-group security objgrp-hr-admin
  security-group name hr-admin-sg-name // single sg_name
  group-object it-admin // locally defined object-group as nested object
object-group security objgrp-hr-servers
  security-group name hr-servers-sg-name
object-group security objgrp-hr-network
  security-group tag 2
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
```

La liste de contrôle d'accès configurée dans l'exemple précédent peut être activée en configurant un groupe d'accès ou le cadre de politique modulaire.

Exemples supplémentaires :

```
!match src hr-admin-sg-name from any network to dst host 172.23.59.53
access-list idw-acl permit ip security-group name hr-admin-sg-name any host 172.23.59.53

!match src hr-admin-sg-name from host 10.1.1.1 to dst any
access-list idfw-acl permit ip security-group name hr-admin-sg-name host 10.1.1.1 any

!match src tag 22 from any network to dst hr-servers-sg-name any network
access-list idfw-acl permit ip security-group tag 22 any security-group
name hr-servers-sg-name any

!match src user mary from any host to dst hr-servers-sg-name any network
access-list idfw-acl permit ip user CSC0\mary any security-group
name hr-servers-sg-name any

!match src objgrp-hr-admin from any network to dst objgrp-hr-servers any network
access-list idfw-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers any

!match src user Jack from objgrp-hr-network and ip subnet 10.1.1.0/24
! to dst objgrp-hr-servers any network
access-list idfw-acl permit ip user CSC0\Jack object-group-security
objgrp-hr-network 10.1.1.0 255.255.255.0 object-group-security objgrp-hr-servers any

!match src user Tom from security-group mktg any google.com
```

```

object network net-google
fqdn google.com
access-list sgacl permit ip sec name mktg any object net-google

! If user Tom or object_group security objgrp-hr-admin needs to be matched,
! multiple ACEs can be defined as follows:
access-list idfw-acl2 permit ip user CSCO\Tom 10.1.1.0 255.255.255.0
    object-group-security objgrp-hr-servers any
access-list idfw-acl2 permit ip object-group-security objgrp-hr-admin
    10.1.1.0 255.255.255.0 object-group-security objgrp-hr-servers any

```

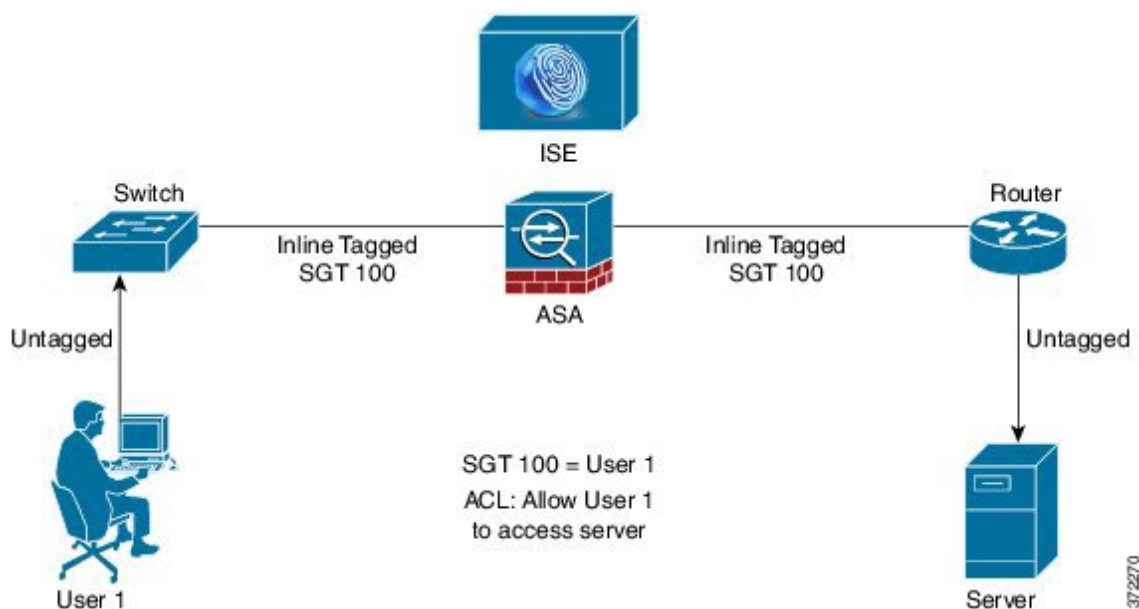
Configurer l'imposition du balisage de groupe de sécurité de couche 2

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 propagation de SGT.

Configuration de l'interface	Paquet étiqueté ou non étiqueté reçu
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'a de la politique. Le numéro SGT provient du gestionnaire
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 provie 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** Configurez une interface et passez en mode de configuration d'interface :
- interface** *ID*
- Exemple :**
- ```
ciscoasa(config)# interface gigabitethernet 0/0
```
- Étape 2** Activez l'imposition SGT de couche 2 et passez en mode de configuration d'interface cts manual.
- cts manual**
- Exemple :**
- ```
ciscoasa(config-if)# cts manual
```
- Étape 3** Activez la propagation d'une balise de groupe de sécurité sur une interface. La propagation est activée par défaut.
- propagate sgt**
- Exemple :**
- ```
ciscoasa(config-if-cts-manual)# propagate sgt
```
- Étape 4** Appliquez une politique à une liaison CTS configurée manuellement.
- policy static sgt** *sgt\_number* [**trusted**]
- Exemple :**



```
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

Le mot-clé **static** spécifie une politique SGT pour le trafic entrant sur la liaison.

La paire mot-clé-argument **sgt sgt\_number** spécifie le numéro SGT à appliquer au trafic entrant de l'homologue. Les valeurs valides sont comprises entre 2 et 65 519.

Le mot-clé **trusted** indique que le trafic d'entrée sur l'interface avec la SGT spécifiée dans la commande ne devrait pas voir sa SGT remplacée. Untrusted est la valeur par défaut.

L'exemple suivant active une interface pour l'application de la balise SGT de couche 2 et définit si l'interface est fiable ou non :

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)# propagate sgt
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

## Configurer manuellement les liaisons IP-SGT

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

### Procédure

Configurez les liaisons IP-SGT manuellement.

**cts role-based sgt-map** {IPv4\_addr[/mask] | IPv6\_addr[/prefix]} **sgt sgt\_value**

**Exemple :**

```
ciscoasa(config)# cts role-based sgt-map 10.2.1.2 sgt 50
```

Vous pouvez utiliser une adresse IPv4 ou IPv6. Vous pouvez également spécifier des adresses réseau en incluant un masque de sous-réseau ou une valeur de préfixe (pour IPv6), comme 10.100.10.0/24. La *valeur sgt\_value* est le numéro SGT, de 2 à 65 519.

## Astuces de dépannage

Utilisez la commande **packet-tracer** pour déterminer pourquoi une session particulière a été autorisée ou refusée, quelle valeur SGT est utilisée (de SGT dans le paquet, du gestionnaire IP-SGT ou de la commande **policy static sgt** configurée sur l'interface), et quelles politiques de sécurité basées sur des groupes de sécurité ont été appliquées.

L'exemple suivant affiche la sortie de la commande **packet-tracer** pour afficher le mappage de la balise de groupe de sécurité vers une adresse IP :

```
ciscoasa# packet-tracer input inside tcp inline-tag 100
```

```
security-group name alpha 30 security-group tag 31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.
```

```
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.1.0 255.255.255.0 outside....
-----More-----
```

Utilisez la commande **capture capture-name type inline-tag tag** pour capturer uniquement les paquets Cisco CMD (EtherType 0x8909) avec ou sans une valeur SGT spécifique.

L'exemple suivant affiche la sortie de la commande **show capture** pour une valeur SGT spécifiée :

```
ciscoasa# show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
4: 11:34:43.933164 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
```

## Exemple pour Cisco TrustSec

L'exemple suivant montre comment configurer l'ASA pour utiliser Cisco TrustSec :

```
// Import an encrypted CTS PAC file
cts import-pac asa.pac password Cisco
// Configure ISE for environment data download
aaa-server cts-server-list protocol radius
aaa-server cts-server-list host 10.1.1.100 cisco123
cts server-group cts-server-list
// Configure SXP peers
cts sxp enable
cts sxp connection peer 192.168.1.100 password default mode peer speaker
//Configure security-group based policies
object-group security objgrp-it-admin
 security-group name it-admin-sg-name
 security-group tag 1
object-group security objgrp-hr-admin
 security-group name hr-admin-sg-name
group-object it-admin
object-group security objgrp-hr-servers
 security-group name hr-servers-sg-name
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
//Configure security group tagging plus Ethernet tagging
interface gi0/1
 cts manual
 propagate sgt
 policy static sgt 100 trusted
 cts role-based sgt-map 10.1.1.100 sgt 50
```

# Prise en charge des VPN sécurisés) pour Cisco TrustSec

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) Entrez dans le mode de configuration des attributs group-policy.

**group-policy name**

**Exemple :**

```
ciscoasa(config)# group policy Grpolicy1
```

- b) Configurez la balise SGT pour la politique de groupe.

**security-group-tag {none | value sgt}**

Si vous définissez une balise à l'aide de **value**, la balise peut être comprise entre 2 et 65 519. Précisez **none** pour ne définir aucune SGT.

**Exemple :**

```
ciscoasa(config-group-policy# security-group-tag value 101
```

**Étape 2**

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

- a) Si nécessaire, créez l'utilisateur.

**username name {nopassword | password password [encrypted]} [privilege priv\_level]}**

**Exemple :**

```
ciscoasa(config)# username newuser password changeme encrypted privilege 15
```

- b) Entrez dans le mode de configuration du nom d'utilisateur.

**username name attributes**

**Exemple :**

```
asa3(config)# username newuser attributes
asa3(config-username)#
```

- c) Configurez la SGT pour l'utilisateur.

**security-group-tag {none | value sgt}**

Si vous définissez une balise à l'aide de **value**, la balise peut être comprise entre 2 et 65 519. Précisez **none** pour ne définir aucune SGT.

**Exemple :**

```
ciscoasa(config-username)# security-group-tag value 101
```

## Surveillance de Cisco TrustSec

Consultez les commandes suivants pour superviser Cisco TrustSec :

- **show running-config cts**
- **show running-config [all] cts role-based [sgt-map]**

Cette commande affiche les entrées du tableau de liaison IP-SGT définies par l'utilisateur.

- **show cts sxp connections**

Cette commande affiche les connexions SXP sur l'ASA pour un contexte d'utilisateur particulier lorsque le mode contexte multiple est utilisé.

- **show conn security-group**

Affiche les données de toutes les connexions SXP.

- **show cts environment-data**

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

- **show cts sgt-map**

Affiche les entrées du gestionnaire de tableau de groupe de sécurité d'adresse IP dans le chemin de contrôle.

- **show asp table cts sgt-map**

Cette commande affiche les entrées de mappage de la table du groupe de sécurité IP de la base de données de mappage de la table du groupe de sécurité IP gérée dans le chemin de données.

- **show cts 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)                 | <p>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.</p> <p>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.</p> <p>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.</p> <p>Nous avons introduit ou modifié les commandes suivantes : <b>access-list extended</b>, <b>cts sxp enable</b>, <b>cts server-group</b>, <b>cts sxp default</b>, <b>cts sxp retry period</b>, <b>cts sxp reconciliation period</b>, <b>cts sxp connection peer</b>, <b>cts import-pac</b>, <b>cts refresh environment-data</b>, <b>object-group security</b>, <b>security-group</b>, <b>show running-config cts</b>, <b>show running-config object-group</b>, <b>clear configure cts</b>, <b>clear configure object-group</b>, <b>show cts pac</b>, <b>show cts environment-data</b>, <b>show cts environment-data sg-table</b>, <b>show cts sxp connections</b>, <b>show object-group</b>, <b>show configure security-group</b>, <b>clear cts environment-data</b>, <b>debug cts</b>, et <b>packet-tracer</b>.</p> |
| Imposition de balises de groupe de sécurité de couche 2 | 9.3(1)                 | <p>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.</p> <p>Nous avons introduit ou modifié les commandes suivantes : <b>cts manual</b>, <b>policy static sgt</b>, <b>propagate sgt</b>, <b>cts role-based sgt-map</b>, <b>show cts sgt-map</b>, <b>packet-tracer</b>, <b>capture</b>, <b>show capture</b>, <b>show asp drop</b>, <b>show asp table classify</b>, <b>show running-config all</b>, <b>clear configure all</b> et <b>write memory</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Nom de la caractéristique                                                                   | Versions de plateforme | Description                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.<br><br>Nous avons introduit ou modifié les commandes suivantes : <b>cts sxp mapping network-map</b> , <b>cts role-based sgt-map</b> , <b>show cts sgt-map</b> , <b>show cts sxp sgt-map</b> , <b>show asp table cts sgt-map</b> . |
| Temporisateur de retenue de suppression configurable de la connexion Trustsec SXP           | 9.8(3)                 | Le temporisateur de retenue de la connexion SXP par défaut est de 120 secondes. Vous pouvez maintenant configurer ce temporisateur, entre 120 et 64 000 secondes.<br><br>Commandes nouvelles/modifiées : <b>cts sxp delete-hold-down period</b> , <b>show cts sxp connection brief</b> , <b>show cts sxp connections</b>                                              |







## 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 103](#)
- [Exigences de licence pour Cisco Umbrella Connector, à la page 104](#)
- [Lignes directrices et limites relatives à Cisco Umbrella, à la page 105](#)
- [Configurer le connecteur Cisco Umbrella, à la page 107](#)
- [Exemples pour le connecteur Cisco Umbrella, à la page 113](#)
- [Surveillance du connecteur Cisco Umbrella, à la page 117](#)
- [Historique du connecteur Cisco Umbrella, à la page 120](#)

## 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. Il s'agit du comportement normal de recherche DNS.
- **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.

## Lignes directrices 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, veuillez 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 le connecteur Cisco Umbrella

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 108.](#)
- 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.
- 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
- Exemple :**
- ```
ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220
```
- Étape 4** [Configurer les paramètres globaux du connecteur Cisco Umbrella, à la page 109.](#)
- Étape 5** [Activer Cisco Umbrella dans la liste des politiques d'inspection DNS, à la page 111.](#)
- Étape 6** [Vérifier l'enregistrement de Cisco Umbrella, à la page 112.](#)
-

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 Créez un point de confiance pour le serveur d'enregistrement Cisco Umbrella.

crypto ca trustpoint name

Vous pouvez utiliser le nom que vous souhaitez pour le point de confiance (jusqu'à 128 caractères), tel que ctx1 ou umbrella_server.

Exemple :

```
ciscoasa(config)# crypto ca trustpoint ctx1
ciscoasa(config-ca-trustpoint)#
```

Étape 2 Indiquez que vous souhaitez vous inscrire manuellement en collant le certificat.

enrollment terminal

Exemple :

```
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)#
```

Étape 3 Importez le certificat.

crypto ca authenticate name

Saisissez le nom du point de confiance que vous avez créé pour ce certificat. Suivez les invites et collez le certificat codé en base 64. Ne pas inclure les lignes BEGIN CERTIFICATE et END CERTIFICATE.

```
ciscoasa(config-ca-trustpoint)# crypto ca authenticate ctx1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

Configurer les paramètres globaux du connecteur Cisco Umbrella

Les paramètres globaux de Cisco 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 Umbrella dans votre carte de politique d'inspection DNS, comme décrit dans [Activer Cisco Umbrella dans la liste des politiques d'inspection DNS, à la page 111](#).

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

Entrez en mode de configuration Cisco Umbrella.

umbrella-global

Exemple :

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)#
```

Étape 2

Configurez le jeton API nécessaire pour s'enregistrer auprès de Cisco Umbrella.

token *api_token*

Exemple :

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
```

Étape 3

(Facultatif) Si vous avez l'intention d'activer DNSCrypt dans la carte de politiques d'inspection DNS, vous pouvez éventuellement configurer la 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.

public-key *hex_key*

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, saisissez **no public-key**. Vous pouvez soit omettre la clé que vous avez configurée, soit l'inclure dans la version **no** de la commande.

Exemple :

```
ciscoasa(config-umbrella)# public-key
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
```

- Étape 4** (Facultatif) Configurez 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.

timeout edns *hh:mm:ss*

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).

Exemple :

```
ciscoasa(config-umbrella)# timeout edns 00:01:00
```

- Étape 5** (Facultatif) Configurez les noms de domaine locaux pour lesquels Cisco Umbrella doit être contourné.

Spécifiez le nom des 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 saisir directement votre nom de domaine local. En option, vous pouvez créer les expressions régulières qui définissent le nom, puis créer une carte de classe d'expression régulière et la spécifier dans la commande suivante :

local-domain-bypass {*regular_expression* | **regex class** *regex_classmap*}

Exemple :

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# local-domain-bypass example.com
```

- Étape 6** (Facultatif) Configurez les adresses des serveurs DNS Cisco Umbrella non par défaut, qui résolvent les demandes DNS, que vous souhaitez utiliser.

resolver {ipv4 | ipv6} *ip_address*

Vous pouvez entrer la commande séparément pour définir les adresses IPv4 et IPv6 des résolveurs Cisco Umbrella autres que les valeurs par défaut.

Exemple :

```
ciscoasa(config-umbrella)# resolver ipv4 208.67.222.222
ciscoasa(config-umbrella)# resolver ipv6 2620:119:35::35
```


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 classe 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 287.

Procédure

Étape 1 Modifiez la liste des politiques d'inspection `preset_dns_map` et passez en mode de configuration des paramètres.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)#
```

Étape 2 Activez Cisco Umbrella et précisez éventuellement le nom de la politique de Cisco Umbrella à appliquer au périphérique.

umbrella [**tag umbrella_policy**] [**fail-open**]

La balise est le nom d'une politique telle qu'elle est définie dans Cisco Umbrella. Lors de l'enregistrement, Cisco Umbrella attribuera la politique au périphérique (si le nom de la politique existe). Si vous ne spécifiez pas de politique, la politique par défaut est appliquée.

Incluez le mot-clé **fail-open** si vous souhaitez que la résolution DNS fonctionne si le serveur DNS Cisco Umbrella n'est pas disponible. 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 n'incluez pas cette option, les requêtes DNS continuent d'être acheminées au résolveur Cisco Umbrella inaccessible, de sorte qu'elles ne recevront pas de réponse.

Exemple :

```
ciscoasa(config-pmap-p)# umbrella fail-open
```

Étape 3 (Facultatif) Activez DNSCrypt pour chiffrer les connexions entre le périphérique et Cisco Umbrella.

dnscrypt

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.

Exemple :

```
ciscoasa(config-pmap-p) # dnscrypt
```

Exemple

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella fail-open
ciscoasa(config-pmap-p)# dnscrypt
```

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.

Tout d'abord, vérifiez les statistiques de la politique de service et recherchez la ligne d'enregistrement Cisco Umbrella. Elle 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:
010a13b8fbd9c9aa
      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.

```
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
```

Exemples pour le connecteur Cisco Umbrella

Les rubriques suivantes fournissent des exemples de configuration du connecteur Cisco Umbrella.

Exemple : activation de Cisco Umbrella dans la politique d'inspection DNS globale

L'exemple suivant montre comment activer Cisco Umbrella globalement. La configuration active DNSCrypt à l'aide de la clé publique par défaut. Elle attribue la politique par défaut de sécurité entreprise Cisco Umbrella.



Remarque

Cet exemple utilise le certificat DigiCert Global Root G2. Assurez-vous de télécharger le dernier certificat racine utilisé par le site Cisco Umbrella, car le certificat correct change avec le temps. Le certificat affiché ici n'est qu'un exemple.

```
ciscoasa(config)# crypto ca trustpoint ctx1
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate ctx1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

```
MIIDjjCCAnagAwIBAgIQAzrx5qcRqAC7KGSxHQN65TANBgkqhkiG9w0BAQsFADBi
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRG1naUNlcnQgSW5jMRkwFwYDVQQLEwB3
d3cuZGlnaWNlcnQyY29tMSAwHgYDVQQDEwxEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xMDE4MDE4MDE4MDE4MDE4MDE4MDE4MDE4MDE4MDE4MDE4MDE4MDE4MDE4
MRUwEwYDVQQKEwxEaWdpQ2VydCBHbG9iYWwgYXV0eG9iYWwgYXV0eG9iYWwgYXV0
b20xIDAeBgNVBAMTF0R5b29tMSAwHgYDVQDEwxEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAAuzfNNN7a8myaJCTsnX/RrohCgin9RlUyfuI
2/Ou8jqJkTx65qsGGmvPrC3oXgkkRLpin7Wo6h+4FR1IAWsULecYxpsMNzaHmx
1x7e/dfgy5SDN67sH0NO3Xss0r0upS/kqbitOtSZpLY16ZtrAGCSYP9PIUky92eQ
q2EGnI/yuum06ZIya7XzV+hdG82MHauVBjVJ8zUtlunJbd134/tJS7SsVQepj5Wz
tCO7TGLF8PapsUwtP1MVYwnSlcUfIKdzXOS0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vIO1CsRnKPZzFBQ9RnbDhxSJITRNrw9FDKZJobq7nMWxM4MphQIDAQABo0IwQDAP
```

```

BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUtiJUIBiV
5uNu5g/6+rKS7QYXjzkWdQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Y19PMWLSn/pvtsrF9+wX3N3KjITOYFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrvHRAiGfzZ0JFrabA0UWTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NG
Fdtom/DzMNU+MeKNhJ7jitrAlj41E6Vf8PlwUHBHQRFXGU7Aj64GxJUTFy8bJZ91
8rGomaFvE7FBcf6IKshPECBV1/MURexgRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfj1lDiIGknibVb63dDcY3fe0Dkhvld1927jyNxFlWW6LZzm6zNTf1
MrY=
quit
...

Do you accept this certificate? [yes/no]: yes

...

% Certificate successfully imported
ciscoasa(config)#

ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220

ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license

ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella
ciscoasa(config-pmap-p)# dnsencrypt

```

Exemple : activation de Cisco Umbrella sur une interface avec une politique d'inspection personnalisée

L'exemple suivant montre comment activer Cisco Umbrella pour une classe de trafic spécifique. Cisco Umbrella est activé sur l'interface interne uniquement pour le trafic DNS/UDP. Comme nous activons DNSCrypt, UDP/443 doit être inclus dans la classe de trafic. Une politique de sécurité d'entreprise nommée mypolicy (définie dans Cisco Umbrella) est appliquée.



Remarque

Cet exemple utilise le certificat DigiCert Global Root G2. Assurez-vous de télécharger le dernier certificat racine utilisé par le site Cisco Umbrella, car le certificat correct change avec le temps. Le certificat affiché ici n'est qu'un exemple.

```

ciscoasa(config)# crypto ca trustpoint ctx1
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate ctx1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

MIIDjjCCAnagAwIBAgIQAzrx5qcRqaC7KGSxHQN65TANBgkqhkiG9w0BAQsFADBh

```

```

MQswCQYDVQZQEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWN1cnQuY29tMSAwHgYDVQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xMzA4MDExMjAwMDBaFw0zODAxMTUxMjAwMDBaMGExCzAJBgNVBAYTA1VT
MRUwEwYDVQZKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTFORpZ21DZXJ0IEdsb2JhbCBSb290IEcyMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEaUzfNnN7a8myaJCTsnX/RrohCgiN9RlUyfuI
2/Ou8jqJkTx65qsGGmvPrC3oXgkRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHmx
1x7e/dfgy5SDN67sH0NO3Xss0r0ups/kqbitOtSszpLY16ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuum06ZIya7XzV+hdG82MHauVBjVJ8zUtlunJbd134/tJS7SsVQepj5Wz
tCO7TG1F8PapsPwUwP1MVYwnSlcUfIKdzXOS0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vIO1CsRnKPZzFBQ9RnbDhxSJITRnrw9FDKZJobq7nmWxm4MphQIDAQABo0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUtiJUIBiV
5uNu5g/6+rkS7QYXjzkwdQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Y19PMWLSn/pvtsrF9+wX3N3KjITOYFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrVHRAiGfzZ0JFrabA0UWTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NG
Fdmom/DzMNU+MeKNhJ7jitrAlj41E6Vf8PlwUHBHQRFxGU7Aj64GxJUTfy8bJZ91
8rGomaFvE7FBcf6IKshPECBV1/MURexgRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfjllDiIGknibVb63dDcy3fe0Dkhvld1927jyNxF1WW6LZZm6zNTf1
MrY=
quit

...

Do you accept this certificate? [yes/no]: yes
...

% Certificate successfully imported
ciscoasa(config)#

ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220

ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE

ciscoasa(config)# policy-map type inspect dns umbrella-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella tag mypolicy
ciscoasa(config-pmap-p)# dnsencrypt

ciscoasa(config)# object-group service umbrella-service-object
ciscoasa(config-service-object-group)# service-object udp destination eq domain
ciscoasa(config-service-object-group)# service-object udp destination eq 443

ciscoasa(config)# access-list umbrella-acl extended permit
object-group umbrella-service-object any any

ciscoasa(config)# class-map dns-umbrella
ciscoasa(config-cmap)# match access-list umbrella-acl

ciscoasa(config)# policy-map inside-policy
ciscoasa(config-pmap)# class dns-umbrella
ciscoasa(config-pmap-c)# inspect dns umbrella-policy

ciscoasa(config)# service-policy inside-policy interface inside

```

Exemple : exclusion de certains hôtes ou réseaux de Cisco Umbrella globalement

Si vous devez exclure certains hôtes ou réseaux de l'utilisation de Cisco Umbrella et que le choix est global plutôt que basé sur l'interface, vous pouvez supprimer l'inspection DNS globale et créer des cartes distinctes pour exclure ou inclure l'inspection Cisco Umbrella.

L'exemple suivant modifie la politique d'inspection globale pour exclure le réseau 192.168.1.0/24 de Cisco Umbrella.

Avant de commencer

Cet exemple suppose que vous avez déjà activé le DNS et configuré les paramètres globaux de Cisco Umbrella.

Procédure

Étape 1 Supprimez l'inspection DNS globale par défaut.

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# no inspect dns
```

Étape 2 Créez une liste des politiques DNS qui active Cisco Umbrella.

Dans cet exemple, la liste des politiques est nommée umbrella-policy.

```
ciscoasa(config)# policy-map type inspect dns umbrella-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella tag mypolicy
```

Étape 3 Créez une carte de trafic pour le trafic exclu.

L'exemple suivant utilise une liste de contrôle d'accès pour identifier le trafic UDP/53 à partir du réseau 192.168.1.0/24.

```
ciscoasa(config)# access-list Umb_Exclude permit udp 192.168.1.0 255.255.255.0 any eq 53
ciscoasa(config)# class-map Umbrella_Exclude
ciscoasa(config-cmap)# match access-list Umb_Exclude
```

Étape 4 Créez une carte de trafic pour les hôtes qui doivent utiliser Cisco Umbrella.

L'exemple suivant fait correspondre le trafic UDP/53 de n'importe quelle source.

```
ciscoasa(config)# class-map Umbrella_Include
ciscoasa(config-cmap)# match port udp eq 53
```

Étape 5 Mettre à jour la politique d'inspection globale pour activer l'inspection DNS pour les cartes de trafic à l'aide de la liste des politiques DNS appropriée.

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class Umbrella_Exclude
ciscoasa(config-pmap-c)# inspect dns
```

```
ciscoasa(config-pmap)# class Umbrella_Include
ciscoasa(config-pmap-c)# inspect dns umbrella-policy
```

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.

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 est **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:
010a13b8fdbfc9aa
      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: dnsencrypt30000
      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 rcv 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 pour *number* 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 *number* 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. Nous avons ajouté ou modifié les commandes suivantes : umbrella, umbrella-global, token, public-key, timeout edns, dnscrypt, show service-policy inspect dns detail.
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 ajouté ou modifié les commandes suivantes : local-domain-bypass, resolver, umbrella fail-open.



PARTIE II

Services de pare-feu pour environnements virtuels

- [Contrôle d'accès basé sur les attributs, à la page 123](#)



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. Les attributs vous permettent de définir des listes de contrôle d'accès (ACL) pour attribuer des politiques au trafic provenant de groupes de machines virtuelles 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 virtuel 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 123](#)
- [Configurer le contrôle d'accès basé sur les attributs, à la page 124](#)
- [Surveillance des objets réseau basés sur les attributs, à la page 131](#)
- [Historique du contrôle d'accès basé sur les attributs, à la page 133](#)

Lignes directrices relatives aux objets réseau basés sur les attributs

Lignes directrices pour 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.

Lignes directrices 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

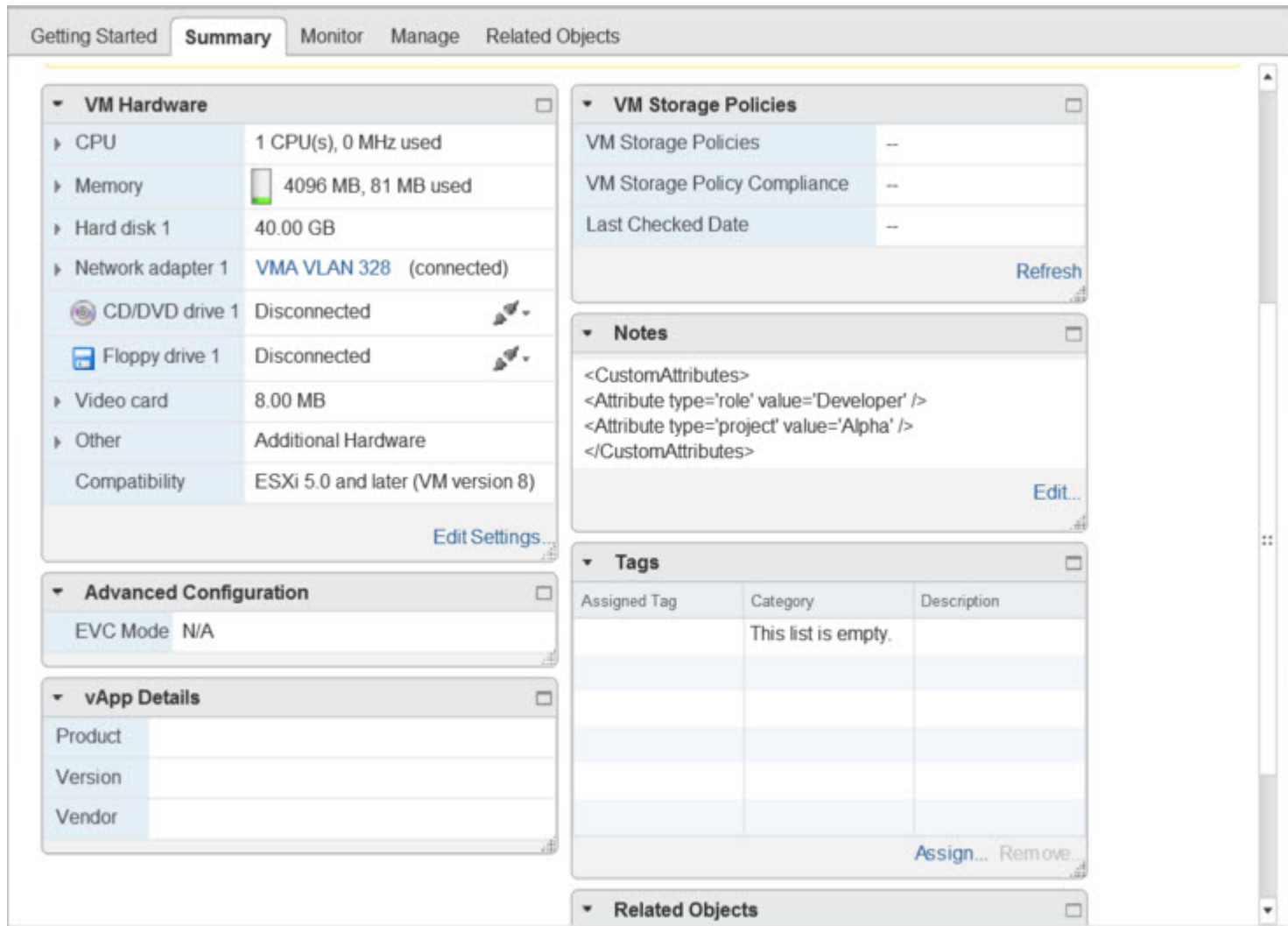
-
Étape 1	Attribuez des types d'attributs et des valeurs personnalisés à vos machines virtuelles gérées. Consultez Configurer les attributs des machines virtuelles vCenter, à la page 124 .
Étape 2	Configurez un agent d'attributs pour une connexion à votre serveur vCenter ou à votre hôte ESXi. Consultez Configurer un agent d'attribut de VM, à la page 126 .
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 128 .
Étape 4	Configurez les listes de contrôle d'accès et les règles. Voir Configurer le contrôle d'accès à l'aide d'objets réseau basés sur les attributs, à la page 130 .
-

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**.

Exemple

L'exemple suivant montre un fichier texte XML correctement formaté qui définit les attributs personnalisés du « Rôle » et du « Projet » que vous pouvez appliquer aux machines virtuelles :

```
<CustomAttributes>
<Attribute type='role' value='Developer' />
<Attribute type='project' value='Alpha' />
</CustomAttributes>
```

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 Créez l'agent d'attribut de VM pour communiquer avec vCenter : **attribute source-group** *agent-name* **type** *agent-type*

Exemple :

```
hostname(config)# attribute source-group VMagent type esxi
```

L'argument *agent-name* spécifie le nom de l'agent de l'attribut VM. L'argument *de type* est le type d'agent d'attribut.

Remarque

Actuellement, ESXi est le seul type d'agent pris en charge.

Étape 2 Configurez les informations d'authentification de votre hôte vCenter : **host ip-address username** *ESXi-username* **password** *ESXi-password*

Exemple :

```
hostname(config-attr)# host 10.122.202.217 user admin password Cisco123
```

Étape 3 Configurez les paramètres Keepalive pour la communication avec vCenter : **keepalive retry-interval** *interval* **retry-count** *count*

Exemple :

```
hostname(config-attr)# keepalive retry-timer 10 retry-count 3
```

Les valeurs par défaut du temporisateur Keepalive sont de 3 tentatives à des intervalles de 30 secondes.

Étape 4 Examinez la configuration de l'agent de l'attribut VM : **show attribute source-group** *agent-name*

Exemple :

```
hostname(config-attr)# sh attribute source-group VMagent
```

```
Attribute agent VMagent
Agent type: ESXi
Agent state: Inactive
Connection state: Connected
Host Address: 10.122.202.217
Retry interval: 30 seconds
Retry count: 3
```

Agent State (État de l'agent) reste inactif jusqu'à ce que vous configuriez un objet réseau et spécifiez les attributs à associer à l'objet.

Étape 5 Quitter le mode de configuration des attributs : **exit**

Exemple :

```
hostname(config-attr)# exit
```

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 Activer la recherche de groupe d'objets : **object-group-search access-control**

Exemple :

```
hostname(config)# object-group-search access-control
```

Vous devez activer `object-group-search` pour configurer les objets réseau basés sur les attributs.

Étape 2 Créez ou modifiez un objet réseau basé sur les attributs en utilisant le nom de l'objet : **object network object-id**

Exemple :

```
hostname(config)# object network dev
```

Étape 3 Spécifiez un agent, le type d'attribut et la valeur d'attribut à associer à l'objet : **attribute agent-name attribute-type attribute-value**

Exemple :

```
hostname(config-network-object)# attribute VMAgent custom.role Developer
```

L'argument *agent-name* spécifie l'agent d'attribut de VM ; voir [<XREF>](#). 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 à l'aide de la sous-commande **host**.

Ensemble, la paire *attribute-type* et *attribute-value* définit un attribut unique. L'argument *attribute-type* est une chaîne arbitraire et doit inclure le préfixe **custom.** préfixe Si vous définissez le même type d'attribut plus d'une fois avec plusieurs valeurs d'attribut, la dernière valeur définie remplace la précédente.

Exemples

L'exemple suivant crée l'objet réseau basé sur les attributs *dev* pour un groupe de développement, avec le rôle de « Developer ». L'agent d'attribut de VM communique avec vCenter et renvoie toutes les liaisons de machine virtuelle qui correspondent à l'attribut *custom.role*.

```
hostname(config)# object network dev
hostname(config-network-object)# attribute VMAgent custom.role Developer
```

L'exemple suivant crée l'objet réseau basé sur les attributs *test* pour un groupe de tests, avec le rôle « Automation ». L'agent d'attribut de VM communique avec vCenter et renvoie toutes les liaisons de machine virtuelle qui correspondent à l'attribut *custom.role*. Notez qu'il s'agit de la même liste de machines virtuelles que dans l'exemple précédent :

```
hostname(config)# object network test
hostname(config-network-object)# attribute VMAgent custom.role Automation
```

L'exemple suivant crée l'objet réseau basé sur les attributs *project* pour un groupe de projets, avec le rôle « Alpha ». L'agent d'attribut de VM communique avec vCenter et renvoie toutes les liaisons de machine virtuelle qui correspondent à l'attribut *custom.project*. Notez que certaines machines chevauchent plus d'un attribut :

```
hostname(config)# object network project
hostname(config-network-object)# attribute VMAgent custom.project Alpha
```

L'exemple suivant montre un agent d'attributs de VM dans un état actif avec des demandes d'attributs en attente :

```
hostname(config-attr)# show attribute source-group VMAgent

Attribute agent VMAgent
Agent type: ESXi
Agent state: Active
Connection state: Connected
Host Address: 10.122.202.217
Retry interval: 30 seconds
Retry count: 3
Attribute requests pending:
  'custom.project'
  'custom.role'
```

Configurer le contrôle d'accès à l'aide d'objets réseau basés sur les attributs

Vous pouvez utiliser des objets réseau basés sur les attributs lorsque vous définissez des ACL (ACL) pour le trafic provenant de groupes de machines virtuelles partageant un ou plusieurs attributs. Les listes d'accès sont composées d'une ou de plusieurs entrées de contrôle d'accès (ACE). Une ACE est une entrée unique dans une liste d'accès qui spécifie une règle d'autorisation ou de refus (pour transférer ou abandonner le paquet). En règle générale, une règle d'autorisation ou de refus est appliquée à un protocole, à une adresse IP source et de destination ou à un réseau et, éventuellement, aux ports source et de destination.

Lorsque vous utilisez des objets réseau basés sur des attributs, vous pouvez remplacer les adresses IP de source et/ou de destination par ces objets. À mesure que les machines virtuelles sont déployées, déplacées ou retirées, les attributs peuvent être mis à jour sur les machines virtuelles tandis que les politiques de contrôle d'accès attribuées peuvent rester en vigueur sans modification de configuration.

Pour des informations complètes sur toutes les options disponibles pour les ACL, consultez [Configurer les ACL](#), à la page 33.

Procédure

Étape 1 Créez et configurez une entrée d'ACL étendue (ACE) à l'aide d'objets réseau basés sur les attributs : **access-list** *access_list_name* **extended** {**deny** | **permit**} *protocol_argument* **object** *source_object_name* **object** *dest_object_name*

Exemple :

```
hostname(config)# access-list lab-access extended permit ip object dev object test
```

Remarque

Répétez l'opération autant de fois que nécessaire pour vos politiques.

Les options sont les suivantes :

- *access_list_name* : nom de la liste de contrôle d'accès nouvelle ou existante.
- Autoriser ou refuser : le mot-clé **deny** refuse ou exempte un paquet si les conditions sont remplies. Le mot-clé **permit** autorise ou inclut un paquet si les conditions correspondent.
- Protocole : *protocol_argument* spécifie le protocole IP.
 - *name* or *number* : spécifie le nom ou le numéro du protocole. Précisez **ip** pour appliquer à tous les protocoles.
 - **object-group** *protocol_grp_id* : spécifie un groupe d'objets de protocole créé à l'aide de la commande **object-group protocol**.
- Objet source : **object** spécifie un objet réseau basé sur les attributs créé à l'aide de la commande **object network**. Le *source_object_name* spécifie l'objet à partir duquel le paquet est envoyé.
- Objet de destination : **object** spécifie un objet réseau basé sur les attributs créé à l'aide de la commande **object network**. Le *dest_object_name* spécifie l'objet vers lequel le paquet est envoyé.

Étape 2 Lier l'ACL à une interface ou l'appliquer globalement : **access-group** *access_list_name* {**in** **interface** *interface_name* | **global**}

Exemple :

```
hostname(config)# access-group lab-access in interface inside
```

Pour un groupe d'accès spécifique à l'interface :

- Précisez le nom de l'ACL étendue. Vous pouvez configurer une commande **access-group** par type d'ACL et par interface.
- Le mot-clé **in** applique l'ACL au trafic entrant.
- Précisez le nom de l'**interface**.

Pour un groupe d'accès global, spécifiez le mot-clé **global** pour appliquer l'ACL étendue à la direction entrante de toutes les interfaces.

Exemple

L'exemple suivant montre comment appliquer globalement une liste de contrôle d'accès étendue basée sur des attributs :

```
hostname(config)# access-list lab-access extended permit ip object dev object test
hostname(config)# access-group lab-access global
hostname(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list lab-access; 1 elements; name hash: 0x62b4790b
access-list lab-access line 1 extended permit ip object dev object test (hitcnt=0) 0x64a1be76

      access-list lab-access line 1 extended permit ip object dev(2) object test(3) (hitcnt=0)
      0x64a1be76
```

Surveillance des objets réseau basés sur les attributs

Pour surveiller les objets réseau basés sur les attributs, entrez les commandes suivantes :

- **show attribute host-map**

Affiche les liaisons d'attribut pour l'agent, le type et la valeur d'un attribut donné.

- **show attribute object-map**

Affiche les liaisons objet-attribut.

- **show attribute source-group**

Affiche les agents d'attribut de VM configurés.

Exemples

L'exemple suivant montre une liste des liaisons hôtes-attributs :

```
hostname# show attribute host-map /all
IP Address-Attribute Bindings Information
```

Source/Attribute	Value
VMAgent.custom.project	'Alpha'
10.15.28.34	
10.15.28.32	
10.15.28.31	
10.15.28.33	
VMAgent.custom.role	'Automation'
10.15.27.133	
10.15.27.135	
10.15.27.134	
VMAgent.custom.role	'Developer'
10.15.28.34	
10.15.28.12	
10.15.28.31	
10.15.28.13	

L'exemple suivant montre un mappage des liaisons hôte-attribut :

```
hostname# show attribute object-map /all
Network Object-Attribute Bindings Information
```

Object	Source/Attribute	Value
dev	VMAgent.custom.role	'Developer'
test	VMAgent.custom.role	'Automation'
project	VMAgent.custom.project	'Alpha'

L'exemple suivant montre la configuration de l'agent d'attributs :

```
hostname# show attribute source-group
Attribute agent VMAgent
Agent type: ESXi
Agent state: Active
Connection state: Connected
Host Address: 10.122.202.217
Retry interval: 30 seconds
Retry count: 3
Attributes being monitored:
'custom.role' (2)
```

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 les commandes suivantes : object network <i>attribute</i> attribute <i>agent-name attribute-type attribute-value</i> attribute source-group <i>agent-name type agent-type</i> host <i>ip-address username ESXi-username password ESXi-password</i> keepalive retry-interval <i>interval</i> retry-count <i>count</i>
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 137](#)
- [Exemples et références de NAT, à la page 195](#)
- [Mappage de l'adresse et du port \(MAP\), à la page 229](#)



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 137](#)
- [Principes de base de la NAT, à la page 138](#)
- [Lignes directrices pour la NAT, à la page 143](#)
- [Traduction d'adresses réseau dynamique, à la page 151](#)
- [PAT dynamique, à la page 159](#)
- [NAT statique, à la page 171](#)
- [NAT d'identité, à la page 181](#)
- [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 routage uniquement) Si vous souhaitez connecter un réseau IPv6 à un réseau IPv4, la NAT vous permet de traduire entre les deux types d'adresses.

**Remarque**

La NAT n'est pas requise. Si vous ne configurez pas la NAT pour un ensemble donné de trafic, ce trafic ne sera pas traduit, mais toutes les politiques de sécurité seront appliquées normalement.

Principes de base de la NAT

Les rubriques suivantes expliquent certains des principes de base de la NAT.

Terminologie NAT

Le présent document utilise les termes suivants :

- Real address/host/network/interface : L'adresse réelle est l'adresse définie sur l'hôte avant qu'elle ne soit traduite. Dans un scénario NAT typique, vous souhaitez traduire le réseau interne lorsqu'il accède à l'extérieur, le réseau interne serait le « vrai » réseau. Notez que vous pouvez traduire n'importe quel réseau connecté au périphérique, pas seulement un réseau interne. Par conséquent, si vous configurez la NAT pour traduire les adresses externes, « réel » peut faire référence au réseau externe lorsqu'il accède au réseau interne.
- Mapped address/host/network/interface (adresse/hôte/réseau/interface mappée) : l'adresse mappée est l'adresse dans laquelle l'adresse réelle est traduite. Dans un scénario NAT typique, où vous souhaitez traduire le réseau interne lorsqu'il accède à l'extérieur, le réseau externe serait le réseau « mappé ».

**Remarque**

Pendant la traduction d'adresses, les adresses IP configurées pour les interfaces de périphérique ne sont pas traduites.

- Lancement bidirectionnel : la NAT statique permet aux connexions d'être lancées de façon *bidirectionnelle*, c'est-à-dire à la fois vers l'hôte et à partir de l'hôte.
- NAT de source et de destination : pour tout paquet donné, les adresses IP de source et de destination sont comparées aux règles de la NAT, et l'une d'elles ou les deux peuvent être traduites ou non traduites, selon le cas. Pour la NAT statique, la règle est bidirectionnelle, il faut donc savoir que les termes « source » et « destination » sont utilisés dans les commandes et les descriptions tout au long de ce guide, même si une connexion donnée peut provenir de l'adresse de « destination ».

Type 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 151](#).
- 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 159](#).
- 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 171](#).
- 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 181](#).

NAT objet de réseau et NAT Twice

Vous pouvez mettre en œuvre la traduction d'adresses de deux manières : *network object NAT* (NAT objet de réseau) et *NAT Twice*.

Nous vous recommandons d'utiliser le *network object NAT* (NAT objet de réseau), sauf si vous avez besoin des fonctionnalités supplémentaires offertes par *NAT Twice*. 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 *NAT Twice* pour ce type de fonctionnalité, où vous pouvez identifier l'adresse de source et de destination dans une seule règle.

NAT Twice

NAT Twice 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 NAT Twice

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.
 - NAT Twice : vous identifiez un objet réseau ou un groupe d'objets réseau pour les adresses réelles et mappées. Dans ce cas, la NAT n'est pas un paramètre de l'objet réseau; l'objet ou le groupe de réseau est un paramètre de la configuration NAT. La possibilité d'utiliser un *groupe* d'objets réseau pour l'adresse réelle signifie que NAT Twice 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.
 - NAT Twice : une règle unique traduit à la fois la source et la destination. Un paquet correspond à une seule règle et les autres règles ne sont pas vérifiées. Même si vous ne configurez pas l'adresse de destination facultative, un paquet correspondant correspond toujours à une seule règle NAT Twice. 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.
 - NAT Twice : 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 NAT Twice 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 règles 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	NAT Twice	Appliqués lors de la première correspondance, dans l'ordre dans lequel elles apparaissent dans la configuration. Étant donné que la première correspondance est appliquée, vous devez vous assurer que les règles spécifiques précèdent les règles plus générales, sans quoi les règles spécifiques pourraient ne pas être appliquées comme vous le souhaitez. Par défaut, les règles NAT Twice 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	NAT Twice	Si aucune correspondance n'est trouvée, les règles de la section 3 sont appliquées selon la première correspondance, dans l'ordre dans lequel elles apparaissent dans la configuration. Cette section devrait contenir vos règles les plus générales. Vous devez également vous assurer que toutes les règles spécifiques de cette section précèdent les règles générales qui s'appliqueraient autrement.

Pour les règles de la section 2, par exemple, les adresses IP suivantes sont définies dans les objets réseau :

- 192.168.1.0/24 (statique)
- 192.168.1.0/24 (dynamique)
- 10.1.1.0/24 (statique)
- 192.168.1.1/32 (statique)
- 172.16.1.0/24 (dynamique) (définition de l'objet)
- 172.16.1.0/24 (dynamique) (objet abc)

L'ordre résultant serait le suivant :

- 192.168.1.1/32 (statique)
- 10.1.1.0/24 (statique)
- 192.168.1.0/24 (statique)
- 172.16.1.0/24 (dynamique) (objet abc)

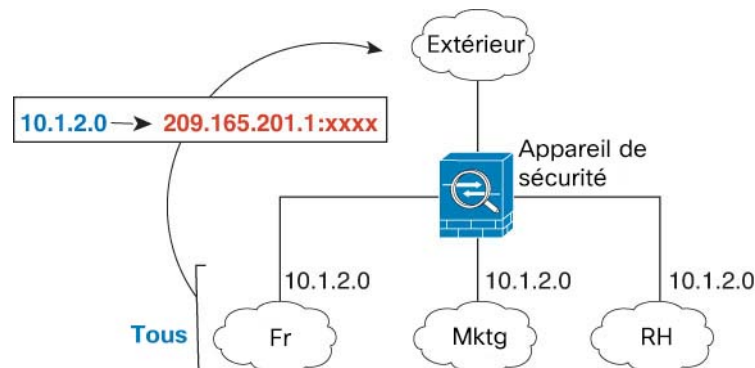
- 172.16.1.0/24 (dynamique) (définition de l'objet)
- 192.168.1.0/24 (dynamique)

Interfaces NAT

À l'exception des interfaces membres des groupes de ponts, vous pouvez configurer une règle NAT à appliquer à n'importe quelle interface (c'est-à-dire à toutes les interfaces) ou vous pouvez identifier des interfaces réelles et mappées spécifiques. Vous pouvez également spécifier n'importe quelle interface pour l'adresse réelle et une interface particulière pour l'adresse mappée, ou inversement.

Par exemple, vous pourriez souhaiter spécifier n'importe quelle interface pour l'adresse réelle et spécifier l'interface externe pour l'adresse mappée si vous utilisez les mêmes adresses privées sur plusieurs interfaces et que vous souhaitez les traduire toutes vers le même ensemble global lors de l'accès à .

Illustration 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.

Lignes directrices 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 dynamique 44/66 et la PAT 44 dynamique sont les seules méthodes autorisées; La PAT 66 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 pour la NAT pour IPv6

La NAT prend en charge IPv6 avec les lignes directrices et restrictions suivantes.

- Pour les interfaces en mode routé standard, vous pouvez également traduire entre IPv4 et IPv6.
- Vous ne pouvez pas traduire entre IPv4 et IPv6 pour des interfaces qui sont membres du même groupe de pont. Vous pouvez uniquement traduire entre deux réseaux IPv6 ou deux réseaux IPv4. Cette restriction ne s'applique pas lorsque les interfaces sont membres de différents groupes de ponts ou entre un membre de groupe de ponts et une interface de routage standard.
- Vous ne pouvez pas utiliser la PAT dynamique pour IPv6 (NAT66) lors de la traduction entre les interfaces du même groupe de ponts. Cette restriction ne s'applique pas lorsque les interfaces sont membres de différents groupes de ponts ou entre un membre de groupe de ponts et une interface de routage standard.
- Pour la NAT statique, vous pouvez spécifier un sous-réseau IPv6 jusqu'à /64. Les sous-réseaux plus importants ne sont pas pris en charge.
- Lors de l'utilisation de FTP avec NAT46, lorsqu'un client FTP pour IPv4 se connecte à un serveur FTP pour IPv6, le client doit utiliser le mode passif étendu (EPSV), ou le mode Port étendu (EPRT); Les commandes PASV et PORT ne sont pas prises en charge avec IPv6.

Bonnes pratiques pour la NAT IPv6

Vous pouvez utiliser la NAT pour traduire entre des réseaux IPv6, mais aussi entre des réseaux IPv4 et IPv6 (mode routage uniquement). Nous recommandons les bonnes pratiques suivantes :

- NAT66 (IPv6-vers-IPv6) : nous vous recommandons d'utiliser une NAT statique. Bien que vous puissiez utiliser la NAT ou la PAT dynamique, les adresses IPv6 sont si nombreuses que vous n'êtes pas obligé d'utiliser la NAT dynamique. Si vous ne souhaitez pas autoriser le trafic de retour, vous pouvez rendre la règle NAT statique unidirectionnelle (NAT Twice uniquement).
- NAT46 (IPv4-vers-IPv6) : nous vous recommandons d'utiliser une NAT statique. Étant donné que l'espace d'adresse IPv6 est beaucoup plus important que l'espace d'adresse IPv4, vous pouvez facilement réaliser une traduction statique. Si vous ne souhaitez pas autoriser le trafic de retour, vous pouvez rendre la règle NAT statique unidirectionnelle (NAT Twice 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 tunnellation 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. Par exemple, **objet network obj-10.10.10.1-01**, **objet network obj-10.10.10.1-02**, etc.
- Si un VPN est défini sur une interface, le trafic ESP entrant sur l'interface n'est pas soumis aux règles de la NAT. Le système autorise le trafic ESP uniquement pour les tunnels VPN établis, abandonnant le trafic non associé à un tunnel existant. Cette restriction s'applique aux ports ESP et UDP 500 et 4500.
- Si vous définissez un VPN de site à site sur un périphérique qui se trouve derrière un périphérique qui applique la PAT dynamique, de sorte que les ports UDP 500 et 4500 ne soient pas ceux réellement utilisés, vous devez établir la connexion à partir du périphérique qui se trouve derrière la PAT. Le répondeur ne peut pas lancer l'association de sécurité (SA), car il ne connaît pas les bons numéros de port.
- Si vous modifiez la configuration NAT et que vous ne souhaitez pas attendre que les traductions existantes expirent avant d'utiliser la nouvelle configuration NAT, vous pouvez effacer le tableau de traduction à l'aide de la commande **clear xlate** dans la CLI du périphérique. Cependant, l'effacement du tableau de traduction déconnecte toutes les connexions actuelles qui utilisent des traductions.

Si vous créez une nouvelle règle NAT qui doit s'appliquer à une connexion existante (comme un tunnel VPN), vous devez utiliser **clear conn** pour mettre fin à la connexion. Ensuite, la 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 ne 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 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.
- (NAT Twice seulement.) Lorsque vous utilisez **any** (n'importe laquelle) comme adresse source dans une règle NAT, la définition du trafic « tout » (IPv4 ou IPv6) dépend de la règle. Avant que 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 265](#).
- Le comportement par défaut de la NAT d'identité a le serveur mandataire ARP activé, correspondant aux autres règles NAT statiques. Vous pouvez désactiver le mandataire ARP si vous le souhaitez. Consultez [Routage des paquets NAT, à la page 206](#) 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. Utilisez la commande **asp rule-engine transactional-commit nat**.
- 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).
- (NAT Twice) 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 relatives à la 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. Utilisez les commandes **object network** et **object-group network** pour créer les objets.

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 145](#) pour en savoir plus sur les adresses IP mappées non autorisées.
- N'utilisez pas de combinaisons de lettres majuscules ou minuscules avant de nommer un objet réseau ou un ensemble TAP.
- 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 pool 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. Utilisez les commandes **object network** et **object-group network** pour créer les objets.

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 145](#) pour en savoir plus sur les adresses IP mappées non autorisées.
- N'utilisez pas de combinaisons de lettres majuscules ou minuscules avant de nommer un objet réseau ou un ensemble TAP.
- 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 pool PAT, une plage. Le groupe (pour un pool 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 NAT Twice, à la page 140](#).
 - 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.example.com`, comme destination traduite (mappée). Pour de plus amples renseignements, consultez la section [Lignes directrices de destination de nom de domaine complet \(FQDN\), à la page 150](#).

Lignes directrices de destination de nom de domaine complet (FQDN)

Vous pouvez spécifier la destination traduite (mappée) dans une règle NAT Twice 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.example.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 pour la source traduite et 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**

Utilisez la commande **objet service** pour créer les objets.

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 (par exemple, TCP pour les deux). 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. L'ensemble mappé comprend généralement moins d'adresses que le groupe réel. Lorsqu'un hôte que vous souhaitez traduire accède au réseau de destination, la NAT attribue à l'hôte une adresse IP de l'ensemble mappé. La traduction est créée uniquement lorsque l'hôte réel lance la connexion. La traduction n'est en place que pour la durée de la connexion et un utilisateur donné ne conserve pas la même adresse IP après l'expiration de la traduction. Par conséquent, les utilisateurs du réseau de destination ne peuvent pas établir de connexion fiable avec un hôte qui utilise la NAT dynamique, même si la connexion est autorisée par une règle d'accès.

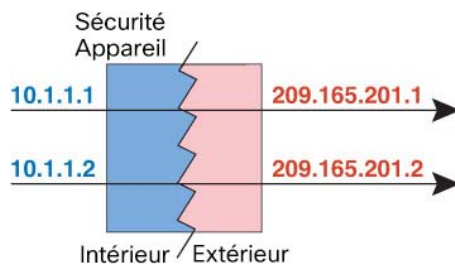


Remarque

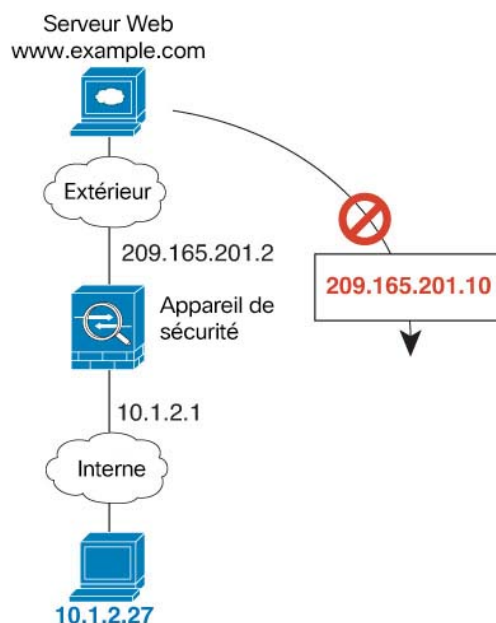
Pour la durée de la traduction, un hôte distant peut établir une connexion avec l'hôte traduit si une règle d'accès le permet. Comme l'adresse est imprévisible, une connexion à l'hôte est peu probable. Cependant, dans ce cas, vous pouvez vous fier à la sécurité de la règle d'accès. Une connexion réussie à partir d'un hôte distant peut réinitialiser le temporisateur 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

Avantages et désavantages de la NAT dynamique

La NAT dynamique présente les désavantages suivants :

- Si l'ensemble mappé comporte moins d'adresses que le groupe réel, vous risquez de manquer d'adresses si le trafic est supérieur aux attentes.

Utilisez PAT ou une méthode de secours PAT si cet événement se produit souvent, car PAT fournit plus de 64 000 traductions utilisant les ports d'une seule adresse.

- Vous devez utiliser un grand nombre d'adresses routables dans l'ensemble mappé, et les adresses routables peuvent ne pas être disponibles en grande quantité.

L'avantage de la NAT dynamique est que certains protocoles ne peuvent pas utiliser la PAT. La PAT ne fonctionne pas avec les éléments suivants :

- Les protocoles IP qui n'ont pas de port à surcharger comme GRE version 0.
- Certaines applications multimédias qui ont un flux de données sur un port et le chemin de contrôle sur un autre port, et qui ne sont pas conformes aux normes ouvertes.

Configurer la NAT dynamique

Cette section décrit comment configurer la NAT d'objet réseau pour la NAT dynamique.

Procédure

Étape 1 Créez un objet réseau d'hôte ou de plage (commande **object network**), ou un groupe d'objets réseau (commande **object-group network**), pour les adresses mappées.

- 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.

Étape 2 Créez ou modifiez l'objet réseau pour lequel vous souhaitez configurer la NAT : **object network obj_name**
Exemple :

```
hostname(config)# object network my-host-obj1
```

Étape 3 (Ignorer lors de la modification d'un objet qui possède la bonne adresse.) Définissez les adresses réelles IPv4 ou IPv6 que vous souhaitez traduire.

- **host** {IPv4_address | IPv6_address} : adresse IPv4 ou IPv6 d'un seul hôte. Par exemple, 10.1.1.1 ou 2001:DB8::0DB8:800:200C:417A.
- **subnet** {IPv4_address IPv4_mask | IPv6_address/IPv6_prefix} : l'adresse d'un réseau. Pour les sous-réseaux IPv4, incluez le masque après un espace, par exemple, 10.0.0.0 255.0.0.0. Pour IPv6, incluez l'adresse et le préfixe comme une seule unité (sans espace), comme par exemple 2001:DB8:0:CD30::/60.
- **range** start_address end_address : plage d'adresses. Vous pouvez définir des plages IPv4 ou IPv6. N'incluez pas de masque ni de préfixe.

Exemple :

```
hostname(config-network-object)# host 10.2.2.2
```

Étape 4 Configurez la **NAT dynamique** pour les adresses IP de l'objet. Vous ne pouvez définir qu'une seule règle de NAT pour un objet donné.

nat [(real_ifc,mapped_ifc)] dynamic mapped_obj [interface [ipv6]] [dns]

Lieu :

- Interfaces : (obligatoire pour les interfaces membres de groupes de ponts.) Précisez les interfaces réelles (*real_ifc*) et mappées (*mapped_ifc*). Assurez-vous d'inclure les parenthèses. En mode routé, si vous ne spécifiez pas les interfaces réelles et mappées, toutes les interfaces sont utilisées. Vous pouvez également spécifier le mot-clé **any** pour l'une des interfaces ou les deux, par exemple (any,outside), mais **any** ne s'applique pas aux interfaces membres de groupes de ponts.
- Adresse IP mappée : spécifiez l'objet réseau ou le groupe d'objets réseau qui comprend les adresses IP mappées.
- Interface PAT fallback (Repli PAT d'interface) : (facultatif) le mot-clé **interface** active le repli PAT d'interface. Une fois les adresses IP mappées utilisées, puis l'adresse IP de l'interface mappée est utilisée.

Si vous spécifiez **ipv6**, l'adresse IPv6 de l'interface est utilisée. Pour cette option, vous devez configurer une interface spécifique pour le *mapped_ifc*. (Vous ne pouvez pas préciser **interface** lorsque l'interface mappée est membre d'un groupe de ponts.)

- DNS : (facultatif) le mot-clé **dns** traduit les réponses DNS. Assurez-vous que l'inspection DNS est activée (elle est activée par défaut). Consultez [Réécriture des requêtes et réponses DNS à l'aide de la NAT](#), à la page 221 pour de plus amples renseignements.

Exemple :

```
hostname(config-network-object)# nat (inside,outside) dynamic MAPPED_IPS interface
```

Exemples

L'exemple suivant configure la NAT dynamique qui cache le réseau 192.168.2.0 derrière une plage d'adresses externes 10.2.2.1 à 10.2.2.10 :

```
hostname(config)# object network my-range-obj
hostname(config-network-object)# range 10.2.2.1 10.2.2.10
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic my-range-obj
```

L'exemple suivant configure la NAT dynamique avec la sauvegarde PAT dynamique. Les hôtes du réseau interne 10.76.11.0 sont d'abord mappés au pool nat-range1 (10.10.10.10-10.10.10.20). Une fois que toutes les adresses du pool nat-range1 ont été attribuées, une PAT dynamique est effectuée à l'aide de l'adresse pat-ip1 (10.10.10.21). Dans le cas peu probable où les traductions PAT sont également épuisées, la PAT dynamique est effectuée en utilisant l'adresse de l'interface externe.

```
hostname(config)# object network nat-range1
hostname(config-network-object)# range 10.10.10.10 10.10.10.20

hostname(config-network-object)# object network pat-ip1
hostname(config-network-object)# host 10.10.10.21

hostname(config-network-object)# object-group network nat-pat-grp
hostname(config-network-object)# network-object object nat-range1
hostname(config-network-object)# network-object object pat-ip1

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 10.76.11.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic nat-pat-grp interface
```

L'exemple suivant configure la NAT dynamique avec sauvegarde PAT dynamique pour traduire les hôtes IPv6 en IPv4. Les hôtes du réseau interne 2001:DB8::/96 sont d'abord mappés au pool IPv4_NAT_RANGE (209.165.201.1 à 209.165.201.30). Une fois que toutes les adresses du pool IPv4_NAT_RANGE sont allouées, une PAT dynamique est effectuée à l'aide de l'adresse IPv4_PAT (209.165.201.31). Si les traductions PAT sont également épuisées, la PAT dynamique est effectuée en utilisant l'adresse de l'interface externe.

```
hostname(config)# object network IPv4_NAT_RANGE
```

```
hostname(config-network-object)# range 209.165.201.1 209.165.201.30

hostname(config-network-object)# object network IPv4_PAT
hostname(config-network-object)# host 209.165.201.31

hostname(config-network-object)# object-group network IPv4_GROUP
hostname(config-network-object)# network-object object IPv4_NAT_RANGE
hostname(config-network-object)# network-object object IPv4_PAT

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic IPv4_GROUP interface
```

Configurer la NAT Twice dynamique

Cette section décrit comment configurer la NAT Twice pour la NAT dynamique.

Procédure

Étape 1 Créez des objets réseau hôtes ou de plage (commande **object network**), ou des groupes d'objets réseau (commande **object-group network**), pour les adresses réelles source, les adresses mappées source, les adresses réelles de destination et les adresses mappées de destination. Vous pouvez également utiliser un objet réseau FQDN pour l'adresse mappée de destination.

- Si vous souhaitez traduire tout le trafic source, vous pouvez ignorer l'ajout d'un objet pour les adresses réelles source et spécifier plutôt le mot-clé **any** dans la commande **nat**.
- Si vous souhaitez configurer la NAT d'interface statique de destination avec traduction de port uniquement, vous pouvez ignorer l'ajout d'un objet pour les adresses mappées de destination et spécifier le mot-clé **interface** dans la commande **nat**.

Si vous créez des objets, tenez compte des consignes suivantes :

- Vous configurez généralement un groupe plus important d'adresses réelles à mapper à un groupe plus restreint.
- 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 contient une seule adresse d'hôte, elle est utilisée pour la PAT.

Étape 2 (Facultatif) Créez des objets de service pour les ports réels de destination et les ports mappés de destination.

Pour la NAT dynamique, vous pouvez uniquement effectuer une traduction de port 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.

Étape 3 Configurer la **NAT dynamique**.

```

nat [(real_ifc,mapped_ifc)] [line | {after-auto [line]}] source dynamic {real_obj | any} {mapped_obj
[interface [ipv6]]} [destination static {mapped_obj | interface [ipv6]} real_obj] [service
mapped_dest_svc_obj real_dest_svc_obj] [dns] [unidirectional] [inactive] [description desc]

```

Lieu :

- Interfaces : (obligatoire pour les interfaces membres de groupes de ponts.) Précisez les interfaces réelles (*real_ifc*) et mappées (*mapped_ifc*). Assurez-vous d'inclure les parenthèses. En mode routé, si vous ne spécifiez pas les interfaces réelles et mappées, toutes les interfaces sont utilisées. Vous pouvez également spécifier le mot-clé **Any** pour l'une des interfaces ou les deux, par exemple (toutes, externes), mais **any** ne s'applique pas aux interfaces des membres du groupe de ponts.
- Section et ligne : (facultatif) Par défaut, la règle NAT est ajoutée à la fin de la section 1 de la table NAT (voir [Ordre des règles NAT, à la page 141](#)). Si vous souhaitez plutôt ajouter la règle dans la section 3 (après les règles NAT de l'objet réseau), utilisez le mot-clé **after-auto**. Vous pouvez insérer une règle n'importe où dans la section applicable en utilisant l'argument *line*.
- Adresses de source
 - Réel : spécifiez un objet réseau, un groupe ou le **mot** -clé.
 - Mappé : spécifiez un autre objet ou groupe de réseau. Vous pouvez éventuellement configurer la méthode de repli suivante :
 - Repli PAT d'interface : (facultatif) Le mot-clé **interface** active l'interface de repli PAT. Une fois les adresses IP mappées utilisées, puis l'adresse IP de l'interface mappée est utilisée. Si vous spécifiez **ipv6**, l'adresse IPv6 de l'interface est utilisée. Pour cette option, vous devez configurer une interface spécifique pour le *mapped_ifc*. (Vous ne pouvez pas préciser **interface** lorsque l'interface mappée est membre d'un groupe de ponts.)
- Adresses de destination (facultatif) :
 - Mappées : spécifiez un objet ou un groupe de réseau, ou pour la NAT d'interface statique avec traduction de port uniquement, spécifiez le mot-clé **interface**. Si vous spécifiez **ipv6**, l'adresse IPv6 de l'interface est utilisée. Si vous spécifiez **interface**, veillez à configurer également le mot-clé **service**. Pour cette option, vous devez configurer une interface spécifique pour le *real_ifc*. Consultez [NAT statique avec traduction de port, à la page 172](#) pour de plus amples renseignements.
 - Réelle : spécifiez un objet ou un groupe de réseau. Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.
- Port de destination : (facultatif.) Précisez le mot-clé **service** ainsi que les objets de service mappés et réels. Pour la traduction de port d'identité, utilisez simplement le même objet de service pour les ports réels et mappés.
- DNS : (facultatif; pour une règle de source uniquement.) Le mot clé **dns** traduit les réponses DNS. Assurez-vous que l'inspection DNS est activée (elle est activée par défaut). Vous ne pouvez pas configurer le mot-clé **DNS** si vous configurez une adresse **de destination**. Consultez [Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 221](#) pour de plus amples renseignements.
- Unidirectionnel : (facultatif) Précisez **unidirectionnel** pour que les adresses de destination ne puissent pas initier le trafic vers les adresses source.
- Inactif : (facultatif.) Pour rendre cette règle inactive sans avoir à supprimer la commande, utilisez le mot-clé **inactive**. Pour la réactiver, entrez de nouveau la commande complète sans le mot-clé **inactive**.

- Description : (facultatif.) Fournir une description de 200 caractères maximum à l'aide du mot-clé **description**.

Exemple :

```
hostname(config)# nat (inside,outside) source dynamic MyInsNet NAT_POOL
destination static Server1_mapped Server1 service MAPPED_SVC REAL_SVC
```

Exemples

L'exemple suivant configure la NAT dynamique pour le réseau interne 10.1.1.0/24 lors de l'accès aux serveurs sur le réseau 209.165.201.1/27 ainsi qu'aux serveurs sur le réseau 203.0.113.0/24 :

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1
destination static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2
destination static SERVERS_2 SERVERS_2
```

L'exemple suivant configure la NAT dynamique pour un réseau interne IPv6 2001:DB8:AAAA::/96 lors de l'accès aux serveurs sur le réseau IPv4 209.165.201.1/27 ainsi qu'aux serveurs sur le réseau 203.0.113.0/24 :

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1
destination static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2
```



```
destination static SERVERS_2 SERVERS_2
```

PAT dynamique

Les rubriques suivantes décrivent la PAT dynamique.

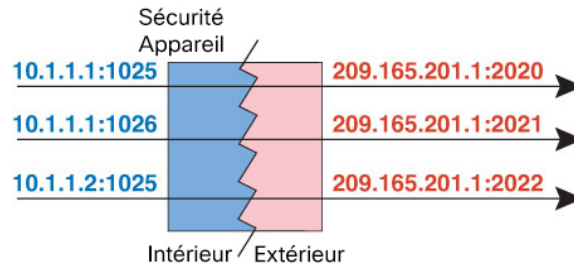
À propos de la PAT dynamique

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.

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 ensemble d'adresses PAT et utiliser une affectation des adresses PAT à tour de rôle pour atténuer cette situation.

Lignes directrices pour les objets du regroupement PAT

Lors de la création d'objets réseau pour un ensemble de PAT, suivez ces lignes directrices.

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), veuillez 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, veuillez 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.
- 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 la version 10.1.1, 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

Cette section décrit comment configurer la NAT d'objet réseau pour la PAT dynamique.

Procédure

Étape 1	(Facultatif) Créez un objet réseau d'hôte ou de plage (commande object network), ou un groupe d'objets réseau (commande object-group network), pour les adresses mappées. • 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 pool PAT) peut inclure des hôtes et des plages.
Étape 2	Créez ou modifiez l'objet réseau pour lequel vous souhaitez configurer la NAT : object network obj_name Exemple : <pre>hostname(config)# object network my-host-obj1</pre>
Étape 3	(Ignorer lors de la modification d'un objet qui possède la bonne adresse.) Définissez les adresses réelles IPv4 ou IPv6 que vous souhaitez traduire. • host {IPv4_address IPv6_address} : l'adresse IPv4 ou IPv6 d'un seul hôte. Par exemple, 10.1.1.1 ou 2001:DB8::0DB8:800:200C:417A.

- **subnet** {IPv4_address IPv4_mask | IPv6_address / IPv6_prefix} : l'adresse d'un réseau. Pour les sous-réseaux IPv4, incluez le masque après un espace, par exemple, 10.0.0.0 255.0.0.0. Pour IPv6, incluez l'adresse et le préfixe comme une seule unité (sans espace), comme par exemple 2001:DB8:0:CD30::/60.
- **range** start_address end_address : une plage d'adresses. Vous pouvez définir des plages IPv4 ou IPv6. N'incluez pas de masque ni de préfixe.

Exemple :

```
hostname(config-network-object)# range 10.1.1.1 10.1.1.90
```

Étape 4

Configurez la **PAT dynamique** pour les adresses IP de l'objet. Vous ne pouvez définir qu'une seule règle de NAT pour un objet donné.

```
nat [(real_ifc,mapped_ifc)] dynamic {mapped_inline_host_ip | mapped_obj | pat-pool mapped-obj  
[round-robin] [extended] [include-reserve] [block-allocation] | interface [ipv6]} [interface [ipv6]]
```

Lieu :

- Interfaces : (obligatoire pour les interfaces membres de groupes de ponts.) Précisez les interfaces réelles (*real_ifc*) et mappées (*mapped_ifc*). Assurez-vous d'inclure les parenthèses. En mode routé, si vous ne spécifiez pas les interfaces réelles et mappées, toutes les interfaces sont utilisées. Vous pouvez également spécifier le mot-clé **any** pour l'une des interfaces ou les deux, par exemple (any,outside), mais **any** ne s'applique pas aux interfaces membres de groupes de ponts.
- Adresse IP mappée : vous pouvez spécifier l'adresse IP mappée comme suit :
 - *mapped_inline_host_ip* : une adresse d'hôte en ligne.
 - *mapped_obj* : un objet réseau qui est défini comme une adresse d'hôte.
 - **pat-pool mapped-obj** : un objet ou un groupe de réseau qui contient plusieurs adresses.
 - **interface [ipv6]** : l'adresse IP de l'interface mappée est utilisée comme adresse mappée. Si vous spécifiez **ipv6**, l'adresse IPv6 de l'interface est utilisée. Pour cette option, vous devez configurer une interface spécifique pour le *mapped_ifc*. (Vous ne pouvez pas préciser **interface** lorsque l'interface mappée est membre d'un groupe de ponts.) Vous devez utiliser ce mot-clé lorsque vous souhaitez utiliser l'adresse IP de l'interface; vous ne pouvez pas le saisir en ligne ou en tant qu'objet.
- Pour un pool PAT, vous pouvez spécifier une ou plusieurs des options suivantes :
 - **round-robin** : active l'allocation d'adresses à tour de rôle pour un pool PAT. 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.
 - **extended** : active 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-reserve** : inclut les ports réservés, 1-1 023, dans la plage de 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.
- **block-allocation** : 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 attribuez 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 bloc de port est compatible avec **round-robin**, mais vous ne pouvez pas utiliser l'option **extended**. Vous ne pouvez pas non plus utiliser l'option de rechange de PAT d'interface.
- **Repli PAT d'interface** : (facultatif) Le mot-clé **interface [ipv6]** active le repli PAT d'interface lorsqu'il est saisi après une adresse PAT principale. Une fois les adresses PAT principales utilisées, l'adresse IP de l'interface mappée est utilisée. Si vous spécifiez **ipv6**, l'adresse IPv6 de l'interface est utilisée. Pour cette option, vous devez configurer une interface spécifique pour le *mapped_ifc*. (Vous ne pouvez pas préciser **interface** lorsque l'interface mappée est membre d'un groupe de ponts.)

Exemple :

```
hostname(config-network-object)# nat (any,outside) dynamic interface
```

Exemples

L'exemple suivant configure la PAT dynamique qui cache le réseau 192.168.2.0 derrière l'adresse 10.2.2.2 :

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 10.2.2.2
```

L'exemple suivant configure la PAT dynamique qui cache le réseau 192.168.2.0 derrière l'adresse de l'interface externe :

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic interface
```

L'exemple suivant configure la PAT dynamique avec un pool PAT pour traduire le réseau IPv6 interne en un réseau IPv4 externe :

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 203.0.113.1 203.0.113.254
hostname(config)# object network IPv6_INSIDE
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

Configurer la PAT Twice dynamique

Cette section décrit comment configurer la NAT Twice pour la PAT dynamique.

Procédure

Étape 1

Créez des objets réseau d'hôte ou de plage (commande **object network**), ou des groupes d'objets réseau (commande **object-group network**), pour les adresses réelles source, les adresses mappées source, les adresses réelles de destination et les adresses mappées de destination. Vous pouvez également utiliser un objet réseau FQDN pour l'adresse mappée de destination.

- Si vous souhaitez traduire tout le trafic source, vous pouvez ignorer l'ajout d'un objet pour les adresses réelles source et spécifier plutôt le mot-clé **any** dans la commande **nat**.
- Si vous souhaitez utiliser l'adresse de l'interface comme adresse mappée, vous pouvez ignorer l'ajout d'un objet pour les adresses mappées source et spécifier plutôt le mot-clé **interface** dans la commande **nat**.
- Si vous souhaitez configurer la NAT de l'interface statique de destination avec traduction de port uniquement, vous pouvez ignorer l'ajout d'un objet pour les adresses mappées de destination et spécifier le mot-clé **interface** dans la commande **nat**.

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 pool PAT) peut inclure des hôtes et des plages.

Étape 2

(Facultatif) Créez des objets de service pour les ports réels de destination et les ports mappés de destination.

Pour la NAT dynamique, vous pouvez uniquement effectuer une traduction de port 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.

Étape 3

Configurer la **PAT dynamique**.

```
nat [(real_ifc,mapped_ifc)] [line | after-auto [line]] source dynamic {real_obj | any} {mapped_obj [interface [ipv6]] | pat-pool mapped_obj [round-robin] [extended] [include-reserve] [block-allocation] [interface [ipv6]] | interface [ipv6]} [destination static {mapped_obj | interface [ipv6]} real_obj] [service mapped_dest_svc_obj real_dest_svc_obj] [unidirectional] [inactive] [description description]
```

Lieu :

- Interfaces : (obligatoire pour les interfaces membres de groupes de ponts.) Précisez les interfaces réelles (*real_ifc*) et mappées (*mapped_ifc*). Assurez-vous d'inclure les parenthèses. En mode routé, si vous ne spécifiez pas les interfaces réelles et mappées, toutes les interfaces sont utilisées. Vous pouvez également spécifier le mot-clé **any** pour l'une des interfaces ou les deux, par exemple (any,outside), mais **any** ne s'applique pas aux interfaces des membres de groupes de ponts.
- Section et ligne : (facultatif) Par défaut, la règle NAT est ajoutée à la fin de la section 1 de la table NAT (voir [Ordre des règles NAT, à la page 141](#)). Si vous souhaitez plutôt ajouter la règle dans la section 3 (après les règles NAT de l'objet réseau), utilisez le mot-clé **after-auto**. Vous pouvez insérer une règle n'importe où dans la section applicable en utilisant l'argument *line*.
- Adresses de source

- **Réel** : un objet réseau, un groupe ou le mot-clé **any**. Utilisez le mot-clé **any** si vous souhaitez traduire tout le trafic de l'interface réelle vers l'interface mappée.
- **Mappé** : configurez l'un des éléments suivants :
 - **Objet réseau** : objet réseau qui contient une adresse d'hôte.
 - **pat-pool mapped-obj** : un objet ou un groupe de réseau qui contient plusieurs adresses.
 - **interface [ipv6]**—(Mode routé uniquement.) L'adresse IP de l'interface mappée est utilisée comme adresse mappée (PAT d'interface). Si vous spécifiez **ipv6**, l'adresse IPv6 de l'interface est utilisée. Pour cette option, vous devez configurer une interface spécifique pour le *mapped_ifc*. (Vous ne pouvez pas préciser **interface** lorsque l'interface mappée est membre d'un groupe de ponts.) Si vous spécifiez ce mot-clé avec un pool PAT ou un objet réseau, vous activez le repli PAT de l'interface. Une fois les adresses IP PAT utilisées, l'adresse IP de l'interface mappée est utilisée.

Pour un pool PAT, vous pouvez spécifier une ou plusieurs des options suivantes :

- **round-robin** : active l'allocation d'adresses à tour de rôle pour un pool PAT. 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.
 - **extended** : active 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-reserve** : inclut les ports réservés, 1-1 023, dans la plage de 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.
 - **block-allocation** : 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 attribuez 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 bloc de port est compatible avec **round-robin**, mais vous ne pouvez pas utiliser l'option **extended**. Vous ne pouvez pas non plus utiliser l'option de rechange de PAT d'interface.
- **Adresses de destination (facultatif)** :
 - **Mappé** : spécifiez un objet ou un groupe réseau, ou pour la NAT d'interface statique avec traduction de port uniquement (interfaces non membres de groupes de ponts uniquement), spécifiez le mot-clé **interface**. Si vous spécifiez **ipv6**, l'adresse IPv6 de l'interface est utilisée. Si vous spécifiez **interface**, veillez à configurer également le mot-clé **service**. Pour cette option, vous devez configurer une

interface spécifique pour le *real_ifc*. Consultez [NAT statique avec traduction de port](#), à la page 172 pour de plus amples renseignements.

- Réelle : spécifiez un objet ou un groupe de réseau. Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.
- Port de destination : (facultatif.) Précisez le mot-clé **service** ainsi que les objets de service mappés et réels. Pour la traduction de port d'identité, utilisez simplement le même objet de service pour les ports réels et mappés.
- Unidirectionnel : (facultatif.) Précisez **unidirectional** pour que les adresses de destination ne puissent pas lancer le trafic vers les adresses source.
- Inactif : (facultatif.) Pour rendre cette règle inactive sans avoir à supprimer la commande, utilisez le mot-clé **inactive**. Pour la réactiver, entrez de nouveau la commande complète sans le mot-clé **inactive**.
- Description : (facultatif.) Fournir une description de 200 caractères maximum en utilisant le mot-clé **description**.

Exemple :

```
hostname(config)# nat (inside,outside) source dynamic MyInsNet interface
destination static Server1 Server1
description Interface PAT for inside addresses when going to server 1
```

Exemples

L'exemple suivant configure la PAT de l'interface pour le réseau interne 192.168.1.0/24 lors de l'accès au serveur Telnet externe 209.165.201.23, et la PAT dynamique à l'aide d'un pool PAT lors de l'accès à tout serveur sur le réseau 203.0.113.0/24.

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0

hostname(config)# object network PAT_POOL
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network TELNET_SVR
hostname(config-network-object)# host 209.165.201.23

hostname(config)# object service TELNET
hostname(config-service-object)# service tcp destination eq 23

hostname(config)# object network SERVERS
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW interface
destination static TELNET_SVR TELNET_SVR service TELNET TELNET
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```


L'exemple suivant configure la PAT de l'interface pour le réseau interne 192.168.1.0/24 lors de l'accès au serveur Telnet IPv6 externe 2001:DB8::23, et la PAT dynamique à l'aide d'un pool PAT lors de l'accès à tout serveur sur le réseau 2001:DB8:AAAA::/96.

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0

hostname(config)# object network PAT_POOL
hostname(config-network-object)# range 2001:DB8:AAAA::1 2001:DB8:AAAA::200

hostname(config)# object network TELNET_SVR
hostname(config-network-object)# host 2001:DB8::23

hostname(config)# object service TELNET
hostname(config-service-object)# service tcp destination eq 23

hostname(config)# object network SERVERS
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW interface ipv6
destination static TELNET_SVR TELNET_SVR service TELNET TELNET
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

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 le mot-clé **round-robin**, mais vous ne pouvez pas inclure **extended**, **include-reserve** ou **interface** (pour l'interface de repli PAT). 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 p-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

(Facultatif) Configurez la taille d'allocation de bloc, qui correspond au nombre de ports dans chaque bloc.

xlate block-allocation size *value*

La plage est de 32 à 4096. La valeur par défaut est 512. Utilisez le formulaire « non » pour revenir à la valeur par défaut.

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.

Étape 2

(Facultatif) Configurez le nombre maximal de blocs qui peuvent être alloués par hôte.

nombre xlate block-allocation maximum-per-host

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. Utilisez le formulaire « non » pour revenir à la valeur par défaut.

Étape 3

(Facultatif) Activez la génération syslog provisoire.

xlate block-allocation pba-interim-logging *seconds*

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*

Exemple :

```
ciscoasa(config)# xlate block-allocation pba-interim-logging 21600
```

Étape 4 Ajoutez des règles NAT qui utilisent l'allocation de bloc de ports de groupement (pool) PAT.

- **PAT de l'objet**

nat [(real_ifc,mapped_ifc)] dynamic pat-pool mapped-obj block-allocation

Exemple :

```
object network mapped-pat-pool
  range 10.100.10.1 10.100.10.2
object network src_host
  host 10.111.10.15
object network src_host
  nat (inside,outside) dynamic
pat-pool mapped-pat-pool block-allocation
```

- **PAT Twice**

nat [(real_ifc,mapped_ifc)] [line | after-auto [line]] source dynamic real_obj pat-poolmapped-obj block-allocation

Exemple :

```
object network mapped-pat-pool
  range 10.100.10.1 10.100.10.2
object network src_network
  subnet 10.100.10.0 255.255.255.0
nat (inside,outside) 1 source dynamic src_network
pat-pool mapped-pat-pool block-allocation
```

Configurer la PAT par session ou la PAT multi-session

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, 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 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 65535/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 :

```
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
xlate per-session permit udp any6 any6 eq domain
```

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 :

```
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
```

Procédure

Créez une règle PAT par session d'autorisation ou de refus. Cette règle est placée au-dessus des règles par défaut, mais en dessous de toute autre règle créée manuellement. Veillez à créer vos règles dans l'ordre dans lequel vous souhaitez qu'elles soient appliquées.

xlate per-session {permit | deny} {tcp | udp} source_ip [operator src_port] destination_ip [operator dest_port]

Pour les adresses IP source et de destination, vous pouvez configurer les éléments suivants :

- **host ip_address** : spécifie une adresse d'hôte IPv4 ou IPv6.
- **ip_address masque** : spécifie une adresse réseau et un masque de sous-réseau IPv4.
- **ipv6-address/prefix-length** : spécifie une adresse réseau et un préfixe IPv6.
- **any4** et **any6** : **any4** spécifie uniquement le trafic IPv4 ; et **any6** le trafic any6.

L'opérateur correspond aux numéros de port utilisés par la source ou la destination. La valeur par défaut est tous les ports. Les opérateurs autorisés sont :

- **lt** : inférieur à
- **gt** : supérieur à
- **eq** : égal à
- **neq** : différent de

- **range** : une plage inclusive de valeurs. Lorsque vous utilisez cet opérateur, spécifiez deux numéros de port, par exemple, **range 100 à 200**.

Exemple

L'exemple suivant crée une règle de refus pour le trafic H.323, afin qu'il utilise la PAT multi-session :

```
hostname(config)# xlate per-session deny tcp any4 209.165.201.7 eq 1720
hostname(config)# xlate per-session deny udp any4 209.165.201.7 range 1718 1719
```

L'exemple suivant permet la distribution de SIP entre les membres d'une grappe en autorisant la PAT par session pour le port UDP du SIP. La PAT par session est la valeur par défaut pour les ports TCP SIP. Vous n'avez donc pas besoin de règle pour TCP, sauf si vous avez modifié les règles par défaut.

```
hostname(config)# xlate per-session permit udp any4 any4 eq sip
```

NAT statique

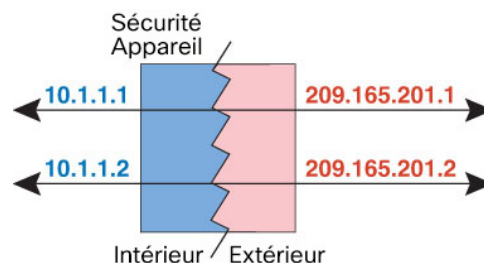
Les rubriques suivantes expliquent la NAT statique et comment la mettre en œuvre.

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.

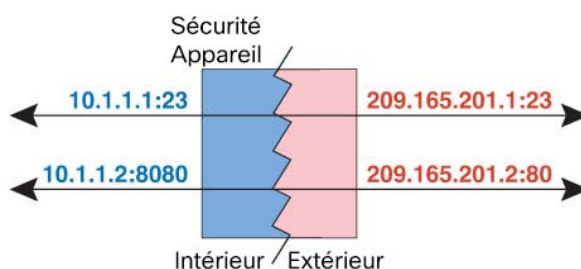
NAT statique avec traduction de port

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 NAT Twice, 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 199.

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

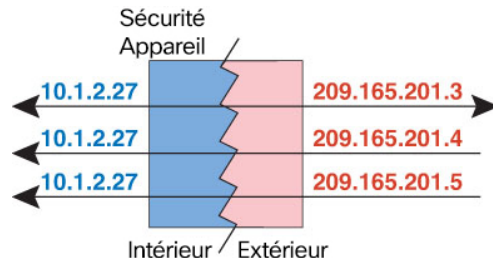
Vous pouvez configurer la NAT statique pour mapper une adresse réelle avec une combinaison adresse d'interface/port. Par exemple, si vous souhaitez rediriger l'accès Telnet pour l'interface externe du périphérique vers un hôte interne, vous pouvez mapper l'adresse IP/le port 23 de l'hôte interne avec 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 souhaitez 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.

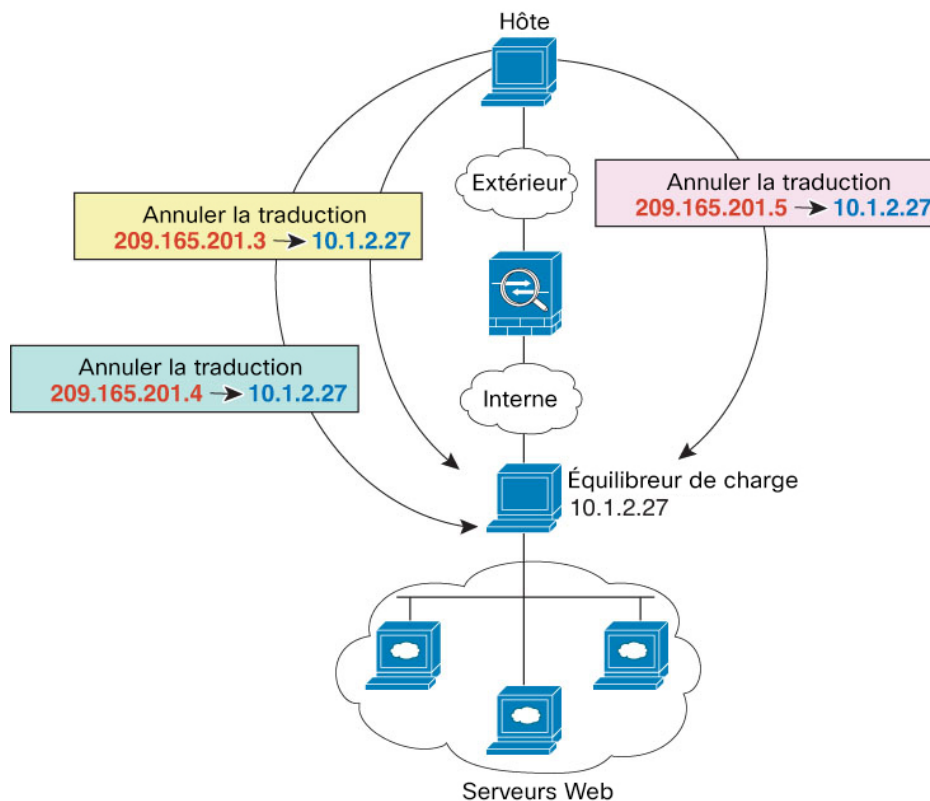
La figure suivante montre un scénario de NAT statique un-à-plusieurs typique. Comme le lancement par l'hôte réel utilise toujours la première adresse mappée, la traduction IP de l'hôte réel/premier IP mappée est techniquement la seule traduction bidirectionnelle.

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 198.

Illustration 14 : Exemple de NAT statique un vers plusieurs

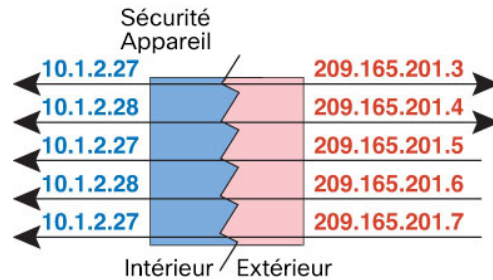


Autres scénarios de mappage (non recommandés)

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.

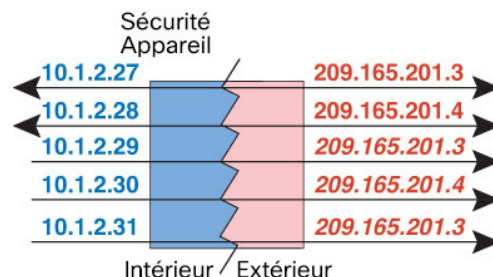
Illustration 15 : NAT statique quelques-uns vers plusieurs

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,) 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** (Facultatif) Créez un objet réseau (commande **object network**), ou un groupe d'objets réseau (commande **object-group network**), pour les adresses mappées.
- 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.

- Étape 2** Créez ou modifiez l'objet réseau pour lequel vous souhaitez configurer la NAT : **object network** *obj_name*
- Exemple :**

```
hostname(config)# object network my-host-obj1
```

- Étape 3** (Ignorer lors de la modification d'un objet qui possède la bonne adresse.) Définissez les adresses IPv4 ou IPv6 réelles que vous souhaitez traduire.

- **host** {*IPv4_address* | *IPv6_address*} : adresse IPv4 ou IPv6 d'un seul hôte. Par exemple, 10.1.1.1 ou 2001:DB8::0DB8:800:200C:417A.
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} : l'adresse d'un réseau. Pour les sous-réseaux IPv4, incluez le masque après un espace, par exemple, 10.0.0.0 255.0.0.0. Pour IPv6, incluez l'adresse et le préfixe comme une seule unité (sans espace), comme par exemple 2001:DB8:0:CD30::/60.
- **range** *start_address end_address* : plage d'adresses. Vous pouvez définir des plages IPv4 ou IPv6. N'incluez pas de masque ni de préfixe.

Exemple :

```
hostname(config-network-object)# subnet 10.2.1.0 255.255.255.0
```

- Étape 4** Configurez la **NAT statique** pour les adresses IP de l'objet. Vous ne pouvez définir qu'une seule règle de NAT pour un objet donné.

```
nat [(real_ifc,mapped_ifc)] static {mapped_inline_host_ip | mapped_obj | interface [ipv6]} [net-to-net] [dns | service {tcp | udp | sctp} real_port mapped_port] [no-proxy-arp]
```

Lieu :

- Interfaces : (obligatoire pour les interfaces membres de groupes de ponts.) Précisez les interfaces réelles (*real_ifc*) et mappées (*mapped_ifc*). Assurez-vous d'inclure les parenthèses. En mode routé, si vous ne spécifiez pas les interfaces réelles et mappées, toutes les interfaces sont utilisées. Vous pouvez également spécifier le mot-clé **any** pour l'une des interfaces ou les deux, par exemple (any,outside), mais **any** ne s'applique pas aux interfaces des membres de groupes de ponts.
- Adresse IP mappée : vous pouvez spécifier l'adresse IP mappée comme l'une des suivantes. 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. Consultez [NAT statique, à la page 171](#).

- ***mapped_inline_host_ip*** : une adresse IP d'hôte en ligne. 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.
- ***mapped_obj*** : un objet ou un groupe de réseau existant. 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.
- ***interface*** : (NAT statique avec traduction de port uniquement.) L'adresse IP de l'interface mappée est utilisée comme adresse mappée. Si vous spécifiez **ipv6**, l'adresse IPv6 de l'interface est utilisée. Pour cette option, vous devez configurer une interface spécifique pour le ***mapped_ifc***. (Vous ne pouvez pas préciser **interface** lorsque l'interface mappée est membre d'un groupe de ponts.) Vous devez utiliser ce mot-clé lorsque vous souhaitez utiliser l'adresse IP de l'interface; vous ne pouvez pas le saisir en ligne ou en tant qu'objet. Assurez-vous de configurer également le mot-clé **service**.
- **Net-to-net** : (facultatif) Pour NAT 46, spécifiez **net-to-net** pour traduire la première adresse IPv4 en première adresse IPv6, la seconde en seconde, etc. Sans cette option, la méthode intégrée à IPv4 est utilisée. Pour une traduction directe de chaque adresse, vous devez utiliser ce mot-clé.
- **DNS** : (facultatif) Le mot clé **dns** traduit les réponses DNS. Assurez-vous que l'inspection DNS est activée (elle est activée par défaut). Consultez [Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 221](#) pour de plus amples renseignements.
- **Traduction de port** : (NAT statique avec traduction de port uniquement.) Précisez **service** avec le mot-clé de protocole souhaité et les ports réels et mappés. Vous pouvez saisir un numéro de port ou un nom de port bien connu (comme **http**).
- **Aucun proxy ARP** : (facultatif) Précisez **no-proxy-arp** pour désactiver le proxy ARP pour les paquets entrants vers les 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 206](#).

Exemple :

```
hostname(config-network-object)#
nat (inside,outside) static MAPPED_IPS service tcp 80 8080
```

Exemples

L'exemple suivant configure la NAT statique pour l'hôte réel 10.1.1.1 sur inside vers 10.2.2.2 sur outside avec la réécriture DNS activée.

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.2.2.2 dns
```

L'exemple suivant configure la NAT statique pour l'hôte réel 10.1.1.1 sur inside vers 10.2.2.2 sur outside à l'aide d'un objet mappé.

```
hostname(config)# object network my-mapped-obj
hostname(config-network-object)# host 10.2.2.2

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-mapped-obj
```

L'exemple suivant configure la NAT statique avec traduction de port pour 10.1.1.1 au port TCP 21 vers l'interface outside au port 2121.

```
hostname(config)# object network my-ftp-server
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static interface service tcp 21 2121
```

L'exemple suivant mappe un réseau IPv4 interne à un réseau IPv6 externe.

```
hostname(config)# object network inside_v4_v6
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) static 2001:DB8::/96
```

L'exemple suivant mappe un réseau IPv6 interne à un réseau IPv6 externe.

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96
hostname(config-network-object)# nat (inside,outside) static 2001:DB8:BBBB::/96
```

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

Créez des objets réseau hôtes ou de plage (commande **object network**), ou des groupes d'objets réseau (commande **object-group network**), pour les adresses réelles source, les adresses mappées source, les adresses réelles de destination et les adresses mappées de destination. Vous pouvez également utiliser un objet réseau FQDN pour l'adresse mappée de destination.

- Si vous souhaitez configurer la NAT de l'interface statique source avec traduction de port uniquement, vous pouvez ignorer l'ajout d'un objet pour les adresses mappées source et préciser le mot-clé **interface** dans la commande **nat**.
- Si vous souhaitez configurer la NAT de l'interface statique de destination avec traduction de port uniquement, vous pouvez ignorer l'ajout d'un objet pour les adresses mappées de destination et préciser le mot-clé **interface** dans la commande **nat**.

Si vous créez des objets, tenez compte des consignes suivantes :

- 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. Pour en savoir plus, consultez [NAT statique, à la page 171](#).

Étape 2 (Facultatif) Créer des objets de service pour :

- Ports de la source *ou* de destination réels
- Ports de la source *ou* de destination mappés

Un objet de service peut contenir à la fois un port source et un port de destination; cependant, vous devriez spécifier *soit* le port source *ou* 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.

Étape 3 Configurer la NAT statique.

```
nat [(real_ifc,mapped_ifc)] [line | {after-object [line]}] source static real_ob [mapped_obj | interface [ipv6]]
[destination static {mapped_obj | interface [ipv6]} real_obj] [service real_src_mapped_dest_svc_obj
mapped_src_real_dest_svc_obj] [net-to-net] [dns] [unidirectional | no-proxy-arp] [inactive] [description
desc]
```

Lieu :

- Interfaces : (obligatoire pour les interfaces membres de groupes de ponts.) Précisez les interfaces réelles (*real_ifc*) et mappées (*mapped_ifc*). Assurez-vous d'inclure les parenthèses. En mode routé, si vous ne spécifiez pas les interfaces réelles et mappées, toutes les interfaces sont utilisées. Vous pouvez également spécifier le mot-clé **Any** pour l'une des interfaces ou les deux, par exemple (toutes, externes), mais **any** ne s'applique pas aux interfaces des membres du groupe de ponts.
- Section et ligne : (facultatif) Par défaut, la règle NAT est ajoutée à la fin de la section 1 de la table NAT (voir [Ordre des règles NAT, à la page 141](#)). Si vous souhaitez plutôt ajouter la règle dans la section 3 (après les règles NAT de l'objet réseau), utilisez le mot-clé **after-auto**. Vous pouvez insérer une règle n'importe où dans la section applicable en utilisant l'argument *line*.
- Adresses de source :
 - Réelle : spécifiez un objet ou un groupe de réseau. N'utilisez pas le mot-clé **any**, qui serait utilisé pour la NAT d'identité.
 - Mappé : spécifiez un autre objet ou groupe de réseau. Pour la NAT d'interface statique avec traduction de port uniquement, vous pouvez spécifier le mot-clé **interface**. Si vous spécifiez **ipv6**, l'adresse IPv6 de l'interface est utilisée. Si vous spécifiez **interface**, veillez à configurer également le mot-clé **service** (dans ce cas, les objets de service ne doivent inclure que le port source). Pour cette option, vous devez configurer une interface spécifique pour le *mapped_ifc*. (Vous ne pouvez pas préciser **interface** lorsque l'interface mappée est membre d'un groupe de ponts.) Consultez [NAT statique avec traduction de port, à la page 172](#) pour de plus amples renseignements.
- Adresses de destination (facultatif) :
 - Mappées : spécifiez un objet ou un groupe de réseau, ou pour la NAT d'interface statique avec traduction de port uniquement, spécifiez le mot-clé **interface**. Si vous spécifiez **ipv6**, l'adresse IPv6 de l'interface est utilisée. Si vous spécifiez **interface**, veillez à configurer également le mot-clé

service (dans ce cas, les objets de service ne doivent inclure que le port de destination). Pour cette option, vous devez configurer une interface spécifique pour le *real_ifc*. (Vous ne pouvez pas préciser **interface** lorsque l'interface mappée est membre d'un groupe de ponts.)

- Réelle : spécifiez un objet ou un groupe de réseau. Pour la NAT d'identité, vous pouvez utiliser le même objet de service pour les ports réels et mappés.
- Ports : (facultatif) Précisez le mot-clé **service** ainsi que les objets de service réels et mappés. Pour la traduction du port source, les objets doivent préciser le service source. L'ordre des objets de service dans la commande de traduction de port source est **service real_obj mapped_obj**. Pour la traduction du port de destination, les objets doivent préciser le service de destination. L'ordre des objets de service pour la traduction du port de destination est **service mapped_obj real_obj**. Dans le cas rare où vous spécifiez à la fois les ports source et de destination dans l'objet, le premier objet de service contient le port source réel/port de destination mappé ; le deuxième objet de service contient le port source mappé/port de destination réel. Pour la traduction de port d'identité, utilisez simplement le même objet de service pour les ports réels et mappés (ports source et/ou de destination, selon votre configuration).
- Réseau à réseau : (facultatif) Pour NAT 46, spécifiez **net-to-net** pour traduire la première adresse IPv4 en première adresse IPv6, la seconde en seconde, etc. Sans cette option, la méthode intégrée à IPv4 est utilisée. Pour une traduction directe de chaque adresse, vous devez utiliser ce mot-clé.
- DNS : (facultatif; pour une règle de source uniquement.) Le mot clé **dns** traduit les réponses DNS. Assurez-vous que l'inspection DNS est activée (elle est activée par défaut). Vous ne pouvez pas configurer le mot-clé **DNS** si vous configurez une adresse **de destination**. Consultez [Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 221](#) pour de plus amples renseignements.
- Unidirectionnel : (facultatif) Précisez **unidirectionnel** pour que les adresses de destination ne puissent pas initier le trafic vers les adresses source.
- Aucun proxy ARP : (facultatif) Précisez **no-proxy-arp** pour désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Consultez [Adresses mappées et routage, à la page 206](#) pour de plus amples renseignements.
- Inactif : (facultatif.) Pour rendre cette règle inactive sans avoir à supprimer la commande, utilisez le mot-clé **inactive**. Pour la réactiver, entrez de nouveau la commande complète sans le mot-clé **inactive**.
- Description : (facultatif.) Fournir une description de 200 caractères maximum à l'aide du mot-clé **description**.

Exemple :

```
hostname(config)# nat (inside,dmz) source static MyInsNet MyInsNet_mapped
destination static Server1 Server1 service REAL_SRC_SVC MAPPED_SRC_SVC
```

Exemples

L'exemple suivant montre l'utilisation de la NAT d'interface statique avec traduction de port. Les hôtes de l'extérieur accèdent à un serveur FTP de l'intérieur en se connectant à l'adresse IP de l'interface externe avec les ports de destination de 65 000 à 65 004. Le trafic n'est pas traduit vers le serveur FTP interne aux adresses 192.168.10.100: de 6 500 à 65 004. Notez que vous devez préciser la plage de ports sources dans l'objet de service (et non le port de destination), car vous souhaitez

traduire l'adresse et le port source comme indiqué dans la commande; le port de destination est quelconque. Étant donné que la NAT statique est bidirectionnelle, « source » et « destination » font référence principalement aux mots-clés de commande; L'adresse et le port source et destination réels d'un paquet dépendent de l'hôte qui a envoyé le paquet. Dans cet exemple, les connexions proviennent de l'extérieur vers l'intérieur, de sorte que l'adresse et le port « source » du serveur FTP sont en fait l'adresse et le port de destination dans le paquet d'origine.

```
hostname(config)# object service FTP_PASV_PORT_RANGE
hostname(config-service-object)# service tcp source range 65000 65004

hostname(config)# object network HOST_FTP_SERVER
hostname(config-network-object)# host 192.168.10.100

hostname(config)# nat (inside,outside) source static HOST_FTP_SERVER interface
service FTP_PASV_PORT_RANGE FTP_PASV_PORT_RANGE
```

L'exemple suivant montre une traduction statique d'un réseau IPv6 vers un autre réseau IPv6 lors de l'accès à un réseau IPv6, et la traduction PAT dynamique vers un pool PAT IPv4 lors de l'accès au réseau IPv4 :

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:BBBB::/96

hostname(config)# object network OUTSIDE_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:CCCC::/96

hostname(config)# object network OUTSIDE_IPv4_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_IPv4_POOL
hostname(config-network-object)# range 10.1.2.1 10.1.2.254

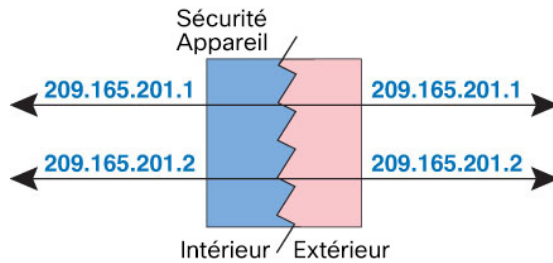
hostname(config)# nat (inside,outside) source static INSIDE_NW MAPPED_IPv6_NW
destination static OUTSIDE_IPv6_NW OUTSIDE_IPv6_NW
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool MAPPED_IPv4_POOL
destination static OUTSIDE_IPv4_NW OUTSIDE_IPv4_NW
```

NAT d'identité

Vous pouvez avoir une configuration NAT dans laquelle vous devez traduire une adresse IP vers elle-même. Par exemple, si vous créez une règle générale qui applique la NAT à tous les réseaux, mais que vous souhaitez exclure un réseau de la NAT, vous pouvez créer une règle NAT statique pour traduire une adresse vers elle-même. La 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** (Facultatif) Créez un objet réseau (commande **object network**), ou un groupe d'objets réseau (commande **object-group network**), pour les adresses mappées.
- 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.
- Étape 2** Créez ou modifiez l'objet réseau pour lequel vous souhaitez configurer la NAT : **object network** *obj_name*. L'objet doit être différent de celui que vous utilisez pour les adresses mappées, même si le contenu doit être le même dans chaque objet.
- Exemple :**
- ```
hostname(config)# object network my-host-obj1
```
- Étape 3** (Ignorer lors de la modification d'un objet qui possède la bonne adresse.) Définissez les adresses réelles IPv4 ou IPv6 que vous souhaitez traduire.
- **host** {IPv4\_address | IPv6\_address} : adresse IPv4 ou IPv6 d'un seul hôte. Par exemple, 10.1.1.1 ou 2001:DB8::0DB8:800:200C:417A.
  - **subnet** {IPv4\_address IPv4\_mask | IPv6\_address/IPv6\_prefix} : l'adresse d'un réseau. Pour les sous-réseaux IPv4, incluez le masque après un espace, par exemple, 10.0.0.0 255.0.0.0. Pour IPv6, incluez l'adresse et le préfixe comme une seule unité (sans espace), comme par exemple 2001:DB8:0:CD30::/60.
  - **range** start\_address end\_address : plage d'adresses. Vous pouvez définir des plages IPv4 ou IPv6. N'incluez pas de masque ni de préfixe.

**Exemple :**

```
hostname(config-network-object)# subnet 10.2.1.0 255.255.255.0
```



**Étape 4** Configurez la **NAT d'identité** pour les adresses IP de l'objet. Vous ne pouvez définir qu'une seule règle de NAT pour un objet donné.

**nat** [(*real\_ifc*,*mapped\_ifc*)] **static** {*mapped\_inline\_host\_ip* | *mapped\_obj*} [**no-proxy-arp**] [**route-lookup**]

Lieu :

- Interfaces : (obligatoire pour les interfaces membres de groupes de ponts.) Précisez les interfaces réelles (*real\_ifc*) et mappées (*mapped\_ifc*). Assurez-vous d'inclure les parenthèses. En mode routé, si vous ne spécifiez pas les interfaces réelles et mappées, toutes les interfaces sont utilisées. Vous pouvez également spécifier le mot-clé **Any** pour l'une des interfaces ou les deux, par exemple (toutes, externes), mais **any** ne s'applique pas aux interfaces des membres du groupe de ponts.
- Adresses IP mappées : veillez à configurer la même adresse IP pour l'adresse mappée et réelle. Utilisez l'un des éléments suivants :
  - *mapped\_inline\_host\_ip* : une adresse IP d'hôte en ligne. Pour les objets hôtes, spécifiez la même adresse. Pour les objets de plage, spécifiez la première adresse dans la plage réelle (le même nombre d'adresses dans la plage sera utilisée). Pour les objets de sous-réseau, spécifiez une adresse dans le sous-réseau réel (toutes les adresses du sous-réseau seront utilisées).
  - *mapped\_obj* : un objet ou un groupe réseau qui comprend les mêmes adresses que l'objet réel.
- Aucun proxy ARP : (facultatif) Précisez **no-proxy-arp** pour désactiver le proxy ARP pour les paquets entrants vers les 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 206](#).
- Recherche de routage : (mode routé uniquement; interfaces précisées.) Précisez **route-lookup** pour déterminer 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 208](#) pour de plus amples renseignements.

### Exemple :

```
hostname(config-network-object)# nat (inside,outside) static MAPPED_IPS
```

### Exemple

L'exemple suivant mappe une adresse d'hôte à elle-même à l'aide d'une adresse mappée en ligne :

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.1.1.1
```

L'exemple suivant mappe une adresse d'hôte à elle-même à l'aide d'un objet réseau :

```
hostname(config)# object network my-host-obj1-identity
hostname(config-network-object)# host 10.1.1.1

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
```

```
hostname(config-network-object)# nat (inside,outside) static my-host-obj1-identity
```

## 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

Créez des objets réseau hôtes ou de plage (commande **object network**), ou des groupes d'objets réseau (commande **object-group network**), pour les adresses réelles source (vous utiliserez généralement le même objet pour les adresses mappées source), les adresses réelles de destination et les adresses mappées de destination. Vous pouvez également utiliser un objet réseau FQDN pour l'adresse mappée de destination.

- Si vous souhaitez effectuer la NAT d'identité pour toutes les adresses, vous pouvez ignorer la création d'un objet pour les adresses réelles source et utiliser à la place les mots-clés **any any** dans la commande **nat**.
- Si vous souhaitez configurer la NAT de l'interface statique de destination avec traduction de port uniquement, vous pouvez ignorer l'ajout d'un objet pour les adresses mappées de destination et préciser le mot-clé **interface** dans la commande **nat**.

Si vous créez des objets, tenez compte des consignes suivantes :

- L'objet ou le groupe peut contenir des hôtes, des plages ou des sous-réseaux.
- Les objets sources 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.

#### Étape 2

(Facultatif) Créer des objets de service pour :

- Ports de la source *ou* de destination réels
- Ports de la source *ou* de destination mappés

Un objet de service peut contenir à la fois un port source et un port de destination; cependant, vous devriez spécifier *soit* le port source *ou* 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.

#### Étape 3

Configurer la **NAT d'identité**.

```
nat [(real_ifc,mapped_ifc)] [line | {after-object [line]}] source static {nw_obj nw_obj | any any} [destination static {mapped_obj | interface [ipv6]} real_obj] [service real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj] [no-proxy-arp] [route-lookup] [inactive] [description desc]
```

Lieu :

- Interfaces : (obligatoire pour les interfaces membres de groupes de ponts.) Précisez les interfaces réelles (*real\_ifc*) et mappées (*mapped\_ifc*). Assurez-vous d'inclure les parenthèses. En mode routé, si vous ne spécifiez pas les interfaces réelles et mappées, toutes les interfaces sont utilisées. Vous pouvez également

spécifier le mot-clé **Any** pour l'une des interfaces ou les deux, par exemple (toutes, externes), mais **any** ne s'applique pas aux interfaces des membres du groupe de ponts.

- **Section et ligne** : (facultatif) Par défaut, la règle NAT est ajoutée à la fin de la section 1 de la table NAT (voir [Ordre des règles NAT, à la page 141](#)). Si vous souhaitez plutôt ajouter la règle dans la section 3 (après les règles NAT de l'objet réseau), utilisez le mot-clé **after-auto**. Vous pouvez insérer une règle n'importe où dans la section applicable en utilisant l'argument *line*.
- **Adresses source** : spécifiez un objet réseau, un groupe ou **any** mot-clé pour les adresses réelles et mappées.
- **Adresses de destination** (facultatif) :
  - **Mappées** : spécifiez un objet ou un groupe de réseau, ou pour la NAT d'interface statique avec traduction de port uniquement, spécifiez le mot-clé **interface**. Si vous spécifiez **ipv6**, l'adresse IPv6 de l'interface est utilisée. Si vous spécifiez **interface**, veillez à configurer également le mot-clé **service** (dans ce cas, les objets de service ne doivent inclure que le port de destination). Pour cette option, vous devez configurer une interface spécifique pour le *real\_ifc*. (Vous ne pouvez pas préciser **interface** lorsque l'interface mappée est membre d'un groupe de ponts.)
  - **Réelles** : spécifiez un objet ou un groupe de réseau. Pour la NAT d'identité, utilisez simplement le même objet ou groupe pour les adresses réelles et mappées.
- **Ports** : (facultatif) Précisez le mot-clé **service** ainsi que les objets de service réels et mappés. Pour la traduction du port source, les objets doivent préciser le service source. L'ordre des objets de service dans la commande de traduction de port source est **service real\_obj mapped\_obj**. Pour la traduction du port de destination, les objets doivent préciser le service de destination. L'ordre des objets de service pour la traduction du port de destination est **service mapped\_obj real\_obj**. Dans le cas rare où vous spécifiez à la fois les ports source et de destination dans l'objet, le premier objet de service contient le port source réel/port de destination mappé ; le deuxième objet de service contient le port source mappé/port de destination réel. Pour la traduction de port d'identité, utilisez simplement le même objet de service pour les ports réels et mappés (ports source et/ou de destination, selon votre configuration).
- **Aucun ARP de proxy** : (facultatif) Précisez **no-proxy-arp** pour désactiver le proxy ARP pour les paquets entrants vers les adresses IP mappées. Consultez [Adresses mappées et routage, à la page 206](#) pour de plus amples renseignements.
- **Recherche de routage** : (facultatif; mode routé uniquement; interfaces précisées.) Précisez **route-lookup** pour déterminer 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 208](#) pour de plus amples renseignements.
- **Inactif** : (facultatif) Pour rendre cette règle inactive sans avoir à supprimer la commande, utilisez le mot-clé **inactive**. Pour la réactiver, entrez de nouveau la commande complète sans le mot-clé **inactive**.
- **Description** : (facultatif) Fournir une description de 200 caractères maximum à l'aide du mot-clé **description**.

#### Exemple :

```
hostname(config)# nat (inside,outside) source static MyInsNet MyInsNet
destination static Server1 Server1
```

# Surveillance de la NAT

Pour surveiller la NAT, utilisez les commandes suivantes :

- **show nat**

Affiche les statistiques sur la NAT, y compris les résultats pour chaque règle NAT.

- **show nat pool**

Affiche les statistiques de pool NAT, y compris les adresses et les ports alloués, et le nombre de fois où ils ont été alloués.

- **show running-config nat**

Affiche la configuration NAT. Vous ne pouvez pas voir les règles NAT d'objets à l'aide de **show running-config object**. Lorsque vous utilisez **show running-config** sans modificateurs, les objets qui comprennent des règles NAT sont affichés deux fois, d'abord avec la configuration de l'adresse de base, puis, plus tard dans la configuration, l'objet avec la règle NAT. L'objet complet, avec l'adresse et la règle NAT, n'est pas affiché comme unité.

- **show xlate**

Affiche les informations de session NAT actuelles.

## 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.<br><br>Nous avons introduit ou modifié les commandes suivantes : <b>nat</b> (mode de configuration object network), <b>show nat</b> , <b>show xlate</b> , <b>show nat pool</b> . |
| NAT Twice                 | 8.3(1)                 | NAT Twice vous permet d'identifier l'adresse source et l'adresse de destination en une seule règle.<br><br>Nous avons modifié ou introduit les commandes suivantes : <b>nat</b> , <b>show nat</b> , <b>show xlate</b> , <b>show nat pool</b> .      |

| 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)          | <p>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.</p> <p>Pour les configurations antérieures à la version 8.3, la migration des règles d'exemption de NAT (la commande <b>nat 0 access-list</b>) 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 : <b>no-proxy-arp</b> et <b>route-lookup</b>. Le mot-clé <b>unidirectionnal</b> 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 <b>no-proxy-arp</b> et <b>route-lookup</b>, pour maintenir les fonctionnalités existantes. Le mot clé <b>unidirectional</b> est supprimé.</p> <p>Nous avons modifié la commande suivante : <b>nat static [no-proxy-arp] [route-lookup]</b>.</p> |
| Affectation d'adresses de pool PAT et round-robin                 | 8.4(2)/8.5(1)          | <p>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.</p> <p>Nous avons modifié les commandes suivantes : <b>nat dynamic [pat-pool mapped_object [round-robin]]</b> and <b>nat source dynamic [pat-pool mapped_object [round-robin]]</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Nom de la caractéristique                                                                | Versions de plateforme | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L'allocation de pool PAT round-robin utilise la même adresse IP pour les hôtes existants | 8.4(3)                 | <p>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.</p> <p>Nous n'avons pas modifié de commandes.</p> <p><i>Cette fonctionnalité n'est pas disponible dans les versions 8.5(1) ou 8.6(1).</i></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Plage uniforme de ports PAT pour un pool PAT                                             | 8.4(3)                 | <p>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 1024 à 65535. Par conséquent, les ports inférieurs à 1024 ont seulement un petit pool PAT.</p> <p>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.</p> <p>Nous avons modifié les commandes suivantes : <b>nat dynamic [pat-pool mapped_object [flat [include-reserve]]]</b> and <b>nat source dynamic [pat-pool mapped_object [flat [include-reserve]]]</b>.</p> <p><i>Cette fonctionnalité n'est pas disponible dans les versions 8.5(1) ou 8.6(1).</i></p> |
| PAT étendue pour un pool PAT                                                             | 8.4(3)                 | <p>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.</p> <p>Nous avons modifié les commandes suivantes : <b>nat dynamic [pat-pool mapped_object [extended]]</b> and <b>nat source dynamic [pat-pool mapped_object [extended]]</b>.</p> <p><i>Cette fonctionnalité n'est pas disponible dans les versions 8.5(1) ou 8.6(1).</i></p>                                                                                                                                                                                                                                                                                                                       |

| 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)                 | <p>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.</p> <p>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 <b>show nat</b>.</p> <p>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 :</p> <ul style="list-style-type: none"> <li>• Ne prend en charge que Cisco IPsec et sécurisés).</li> <li>• 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.</li> <li>• Ne prend pas en charge l'équilibrage de la charge (en raison de problèmes de routage).</li> <li>• Ne prend pas en charge l'itinérance (modification d'adresse IP publique).</li> </ul> <p>Nous avons introduit la commande suivante : <b>nat-assigned-to-public-ip interface</b> (mode de configuration des attributs généraux du groupe de tunnels).</p> |
| Prise en charge de la NAT pour IPv6                                                                                    | 9.0(1)                 | <p>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.</p> <p>Nous avons modifié les commandes suivantes : <b>nat</b> (modes de configuration globale et réseau d'objets), <b>show nat</b>, <b>show nat pool</b>, <b>show xlate</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Prise en charge de la NAT pour les recherches DNS inversées                                                            | 9.0(1)                 | <p>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.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Nom de la caractéristique                                         | Versions de plateforme | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PAT par session                                                   | 9.0(1)                 | <p>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.</p> <p>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.</p> <p>Nous avons introduit les commandes suivantes : <b>xlate per-session</b>, <b>show nat pool</b>.</p> |
| Modèle de validation transactionnelle sur le moteur de règles NAT | 9.3(1)                 | <p>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.</p> <p>Nous avons introduit le mot-clé <b>nat</b> aux commandes suivantes : <b>asp rule-engine transactional-commit</b>, <b>show running-config asp rule-engine transactional-commit</b>, <b>clear configure asp rule-engine transactional-commit</b>.</p> <p>Nous avons ajouté la NAT à l'écran suivant : Configuration &gt; Device Management (Gestion des périphériques) &gt; Advanced (Avancé) &gt; Rule Engine (Moteur de règles).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Améliorations de la NAT de niveau opérateur                       | 9.5(1)                 | <p>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).</p> <p>Nous avons ajouté les commandes suivantes : <b>xlate block-allocation size</b>, <b>xlate block-allocation maximum-per-host</b>. Nous avons ajouté le mot clé <b>block-allocation</b> à la commande <b>nat</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |



| Nom de la caractéristique                                         | Versions de plateforme | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prise en charge de la NAT pour SCTP                               | 9.5(2)                 | <p>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.</p> <p>Nous avons modifié les commandes suivantes : <b>nat static</b> (objet).</p>                                                                                                                                                                                                                                                                                                            |
| Journalisation provisoire pour l'allocation de bloc de ports NAT. | 9.12(1)                | <p>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.</p> <p>Nous avons ajouté la commande suivante : <b>xlate block-allocation pba-interim-logging</b> <i>seconds</i>.</p> |

| Nom de la caractéristique                                                                                                                                                         | Versions de plateforme | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modifications apportées à l'attribution d'adresses PAT dans la mise en grappe. L'option <b>flat</b> de l'ensemble PAT est désormais activée par défaut et n'est pas configurable. | 9.15(1)                | <p>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.</p> <p>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 <b>flat</b> dans une règle d'ensembles de PAT. Le mot clé <b>flat</b> n'est plus pris en charge : l'ensemble de PAT est désormais toujours à plat. Le mot clé <b>include-reserve</b>, qui était auparavant un sous-mot clé de <b>flat</b>, 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.</p> <p>Notez que si vous configurez l'allocation de bloc de ports (l'option d'ensemble de PAT <b>block-allocation</b>), 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.</p> <p>Commandes nouvelles/modifiées : <b>nat, show nat pool</b></p> |

| 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 <b>show nat detail</b> . |
| 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 <code>www.exemple.com</code> , 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 pour la NAT Twice, à la page 200](#)
- [NAT en mode routage et transparent, à la page 204](#)
- [Routage des paquets NAT, à la page 206](#)
- [NAT pour VPN, à la page 209](#)
- [Traduction de réseaux IPv6, à la page 215](#)
- [Réécriture des requêtes et réponses DNS à l'aide de la NAT, à la page 221](#)

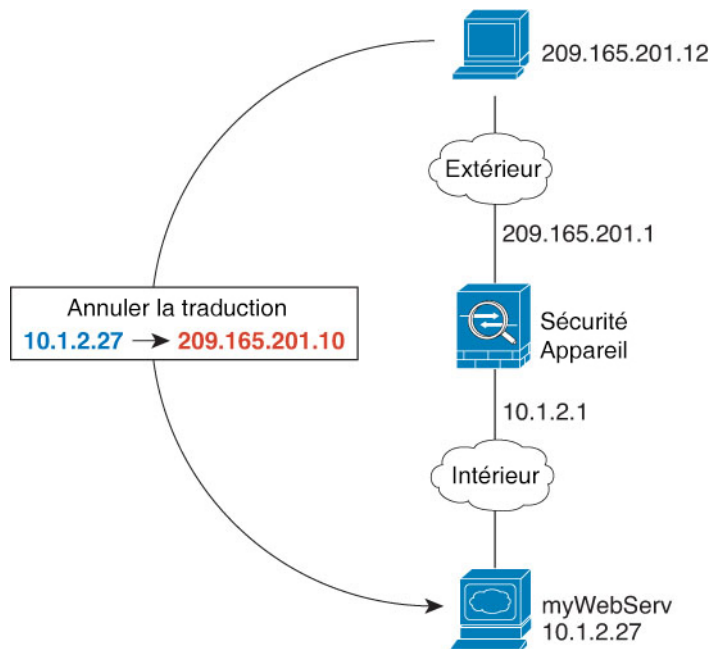
## Exemples de NAT d'objets réseau

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** Créez un objet réseau pour le serveur Web interne.

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 10.1.2.27
```

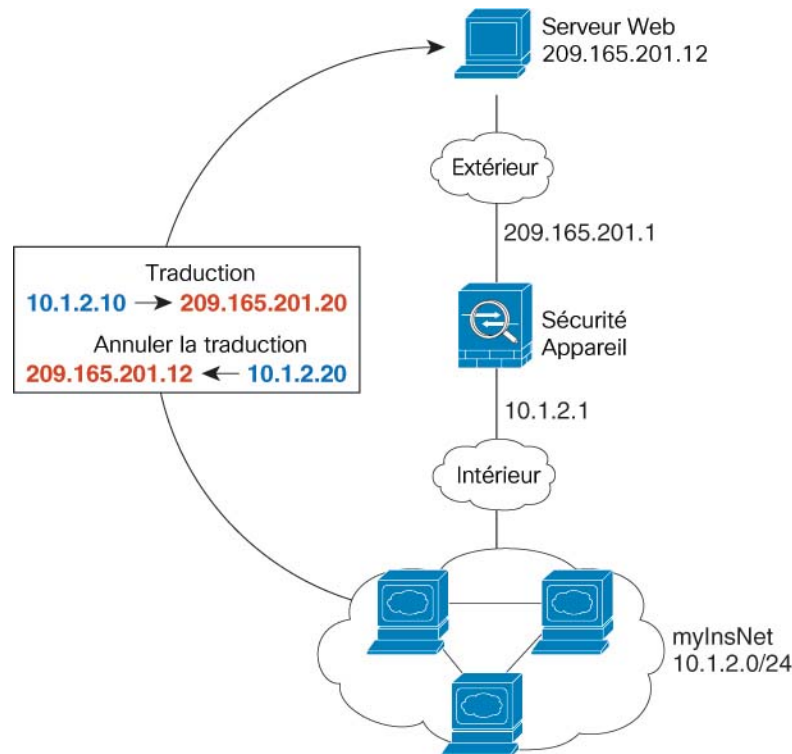
**Étape 2** Configurez la NAT statique pour l'objet :

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

## 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



248773

## Procédure

- Étape 1** Créez un objet réseau pour l'ensemble de NAT dynamique vers lequel vous souhaitez traduire les adresses internes.

```
hostname(config)# object network myNatPool
hostname(config-network-object)# range 209.165.201.20 209.165.201.30
```

- Étape 2** Créez un objet réseau pour le réseau interne.

```
hostname(config)# object network myInsNet
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

- Étape 3** Activez la NAT dynamique pour le réseau interne à l'aide de l'objet pool de NAT dynamique.

```
hostname(config-network-object)# nat (inside,outside) dynamic myNatPool
```

- Étape 4** Créez un objet réseau pour le serveur Web externe.

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 209.165.201.12
```

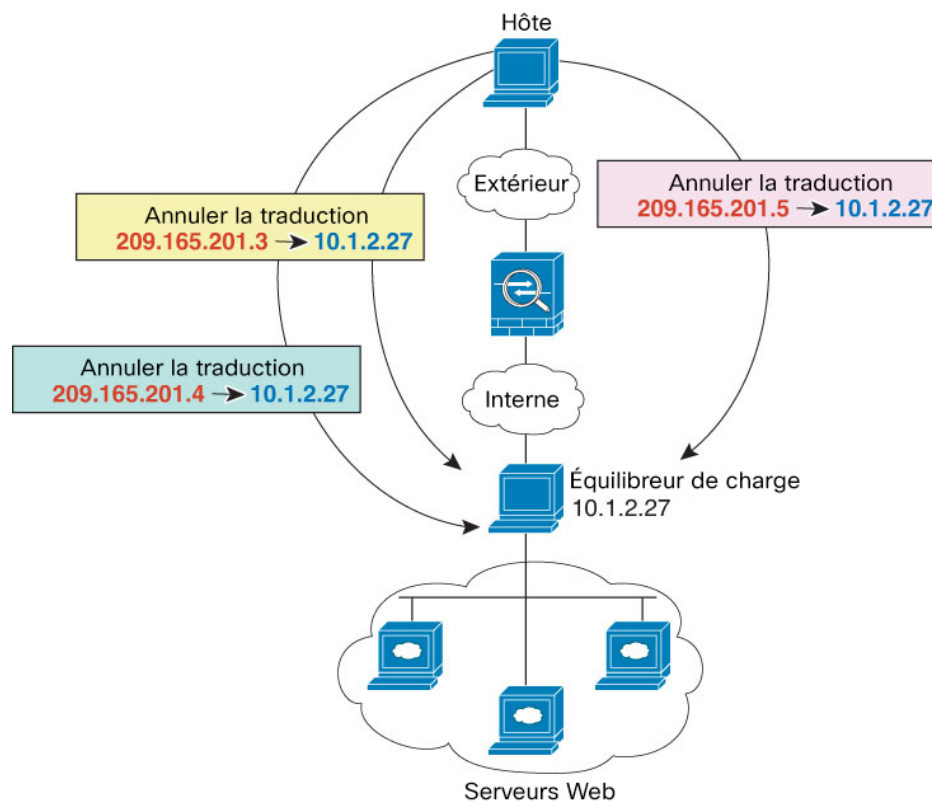
**Étape 5** Configurez la NAT statique pour le serveur Web.

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.20
```

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

L'exemple suivant montre un équilibreur de charge interne qui se traduit 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** Créez un objet réseau pour les adresses auxquelles vous souhaitez mapper l'équilibreur de charge.

```
hostname(config)# object network myPublicIPs
hostname(config-network-object)# range 209.165.201.3 209.265.201.8
```



**Étape 2** Créez un objet réseau pour l'équilibreur de charge.

```
hostname(config)# object network myLBHost
hostname(config-network-object)# host 10.1.2.27
```

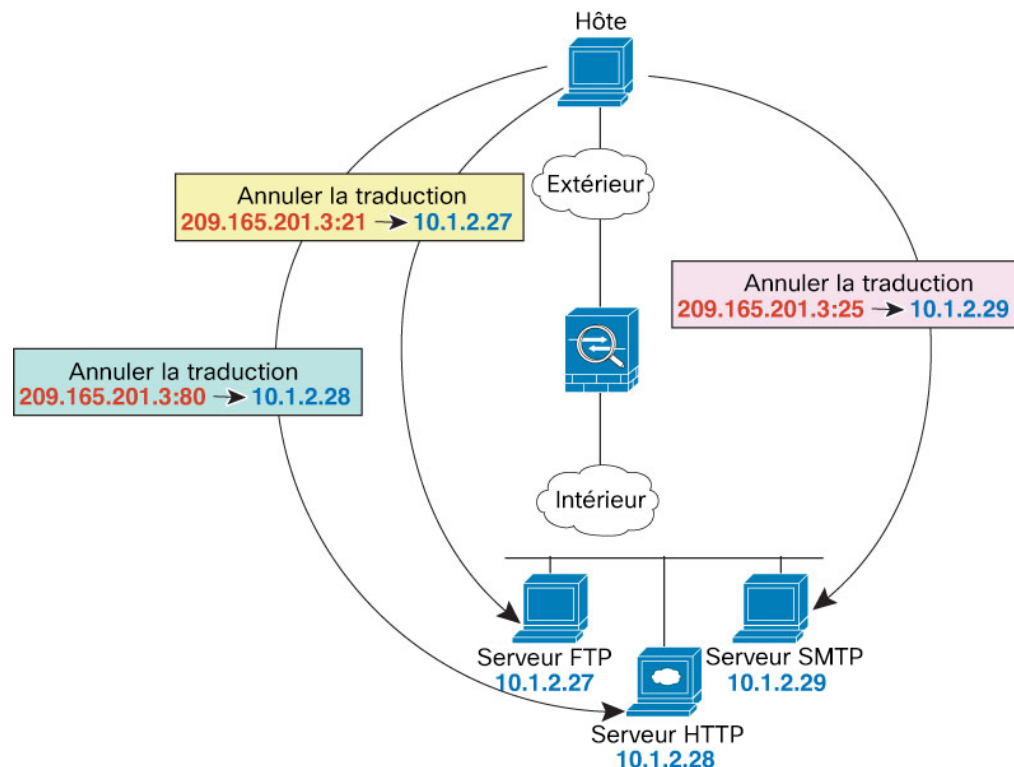
**Étape 3** Configurez la NAT statique pour l'équilibreur de charge appliquant l'objet de plage.

```
hostname(config-network-object)# nat (inside,outside) static myPublicIPs
```

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

L'exemple de NAT statique avec traduction de port statique suivant fournit une adresse unique permettant aux utilisateurs distants d'accéder à FTP, HTTP et SMTP. Ces serveurs sont en fait des périphériques différents sur le réseau réel, mais pour chaque serveur, vous pouvez spécifier des règles NAT statiques avec des règles de traduction de port qui utilisent la même adresse IP mappée, mais des ports différents.

*Illustration 21 : NAT statique avec traduction de port*



## Procédure

**Étape 1** Créez un objet réseau pour le serveur FTP et configurez la NAT statique avec la traduction de port, en mappant le port FTP sur lui-même.

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 10.1.2.27
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp ftp
ftp
```

**Étape 2** Créez un objet réseau pour le serveur HTTP et configurez la NAT statique avec la traduction de port, en mappant le port HTTP sur lui-même.

```
hostname(config)# object network HTTP_SERVER
hostname(config-network-object)# host 10.1.2.28
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp http
http
```

**Étape 3** Créez un objet réseau pour le serveur SMTP et configurez la NAT statique avec la traduction de port, en mappant le port SMTP sur lui-même.

```
hostname(config)# object network SMTP_SERVER
hostname(config-network-object)# host 10.1.2.29
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp smtp
smtp
```

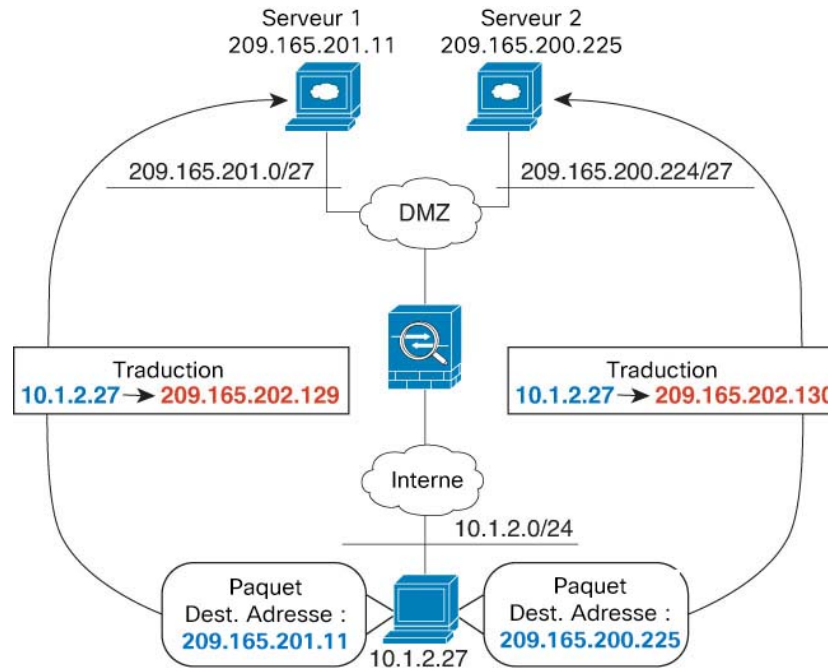
## Exemples pour la NAT Twice

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 209.165.202.129 :port. Lorsque l'hôte accède au serveur à partir de l'adresse 209.165.200.225, l'adresse réelle est traduite en 209.165.202.130 :port.

Illustration 22 : NAT manuelle avec différentes adresses de destination



## Procédure

### Étape 1 Créez un objet réseau pour le réseau interne

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

### Étape 2 Créez un objet réseau pour le réseau DMZ 1

```
hostname(config)# object network DMZnetwork1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224
```

### Étape 3 Ajoutez un objet réseau pour l'adresse PAT :

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

### Étape 4 Configurez la première règle de NAT manuelle

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress1
destination static DMZnetwork1 DMZnetwork1
```

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 5** Ajoutez un objet réseau pour le réseau DMZ 2.

```
hostname(config)# object network DMZnetwork2
hostname(config-network-object)# subnet 209.165.200.224 255.255.255.224
```

**Étape 6** Ajoutez un objet réseau pour l'adresse PAT :

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

**Étape 7** Configurez la deuxième règle NAT manuelle :

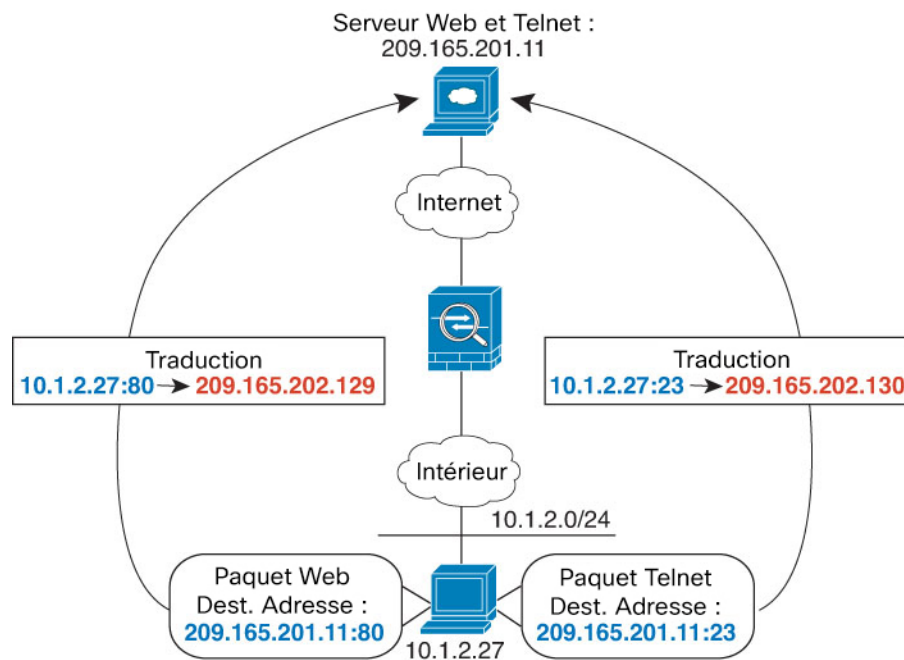
**Exemple :**

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress2
destination static DMZnetwork2 DMZnetwork2
```

## 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 209.165.202.129 :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** Ajoutez un objet réseau pour le réseau interne.

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

**Étape 2** Ajoutez un objet réseau pour le serveur Telnet/Web.

```
hostname(config)# object network TelnetWebServer
hostname(config-network-object)# host 209.165.201.11
```

**Étape 3** Ajoutez un objet réseau pour l'adresse PAT lorsque vous utilisez Telnet.

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

**Étape 4** Ajoutez un objet de service pour Telnet :

```
hostname(config)# object service TelnetObj
hostname(config-network-object)# service tcp destination eq telnet
```

**Étape 5** Configurez la première règle NAT Twice :

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress1
destination static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj
```

Comme vous ne souhaitez pas traduire l'adresse ou le port de destination, vous devez configurer la NAT d'identité pour ceux-ci en spécifiant la même adresse pour les adresses de destination réelles et mappées, et le même port pour le service réel et mappé.

**Étape 6** Ajoutez un objet réseau pour l'adresse PAT lorsque vous utilisez HTTP.

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

**Étape 7** Ajoutez un objet de service pour HTTP :

```
hostname(config)# object service HTTPObj
hostname(config-network-object)# service tcp destination eq http
```

**Étape 8** Configurez la deuxième règle NAT manuelle :

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress2
```

```
destination static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj
```

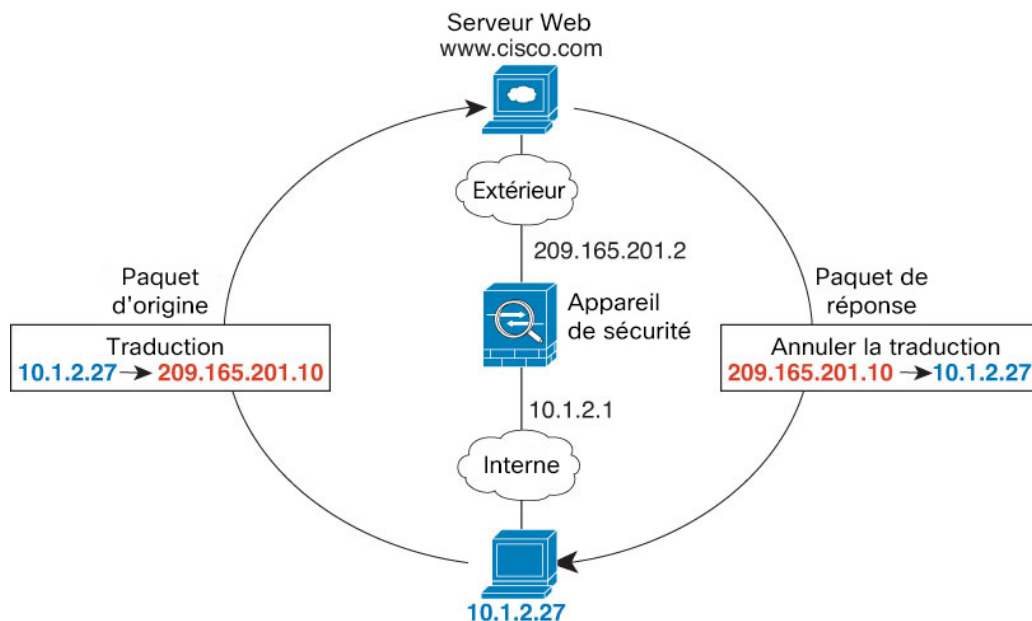
## NAT en mode routage et transparent

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

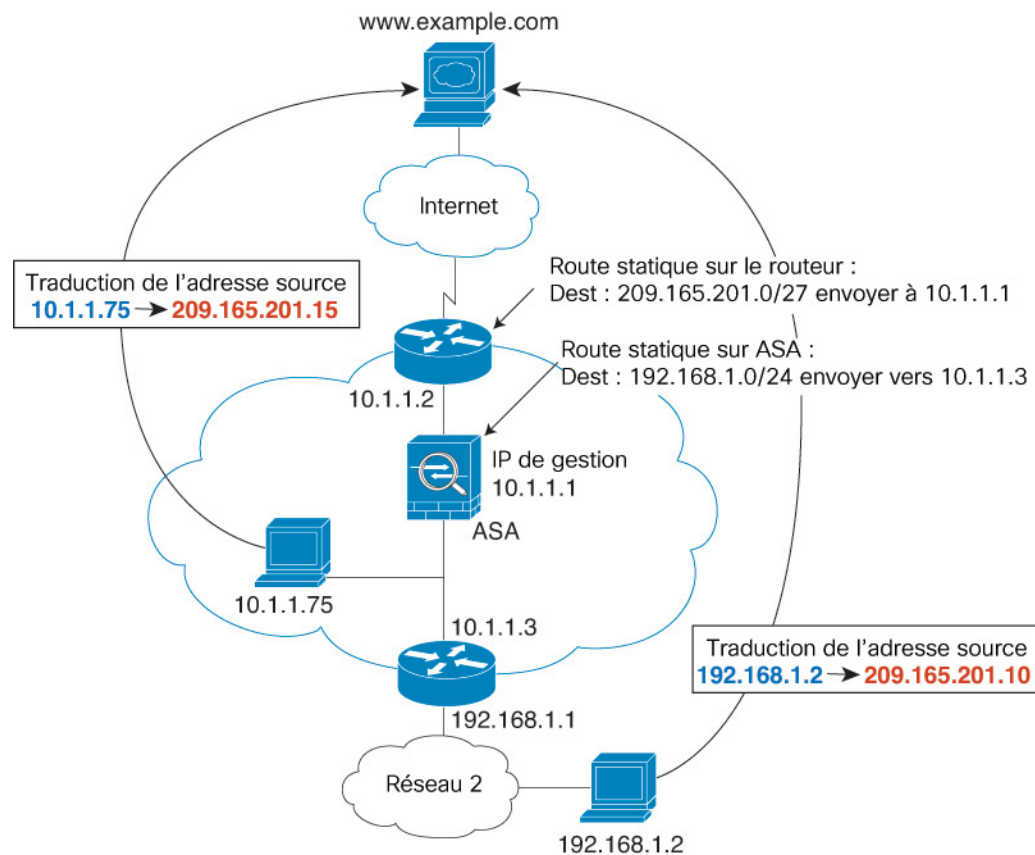
L'utilisation de la NAT en mode transparent élimine le besoin pour les routeurs en amont ou en aval d'effectuer la NAT pour leurs réseaux. Il peut remplir une fonction similaire dans un groupe de ponts en mode routé.

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 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. ASA annule ensuite la traduction de l'adresse mappée, 209.165.201.15, vers l'adresse réelle, 10.1.1.1.75. 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 voie de routage 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 145](#).

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 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. Configurez l'ARP à l'aide de la commande **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 pointent 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 10.1.1.99. Passerelle 1.99 qui peut être redistribuée.

```
route inside 209.165.201.5 255.255.255.255 10.1.1.99
```

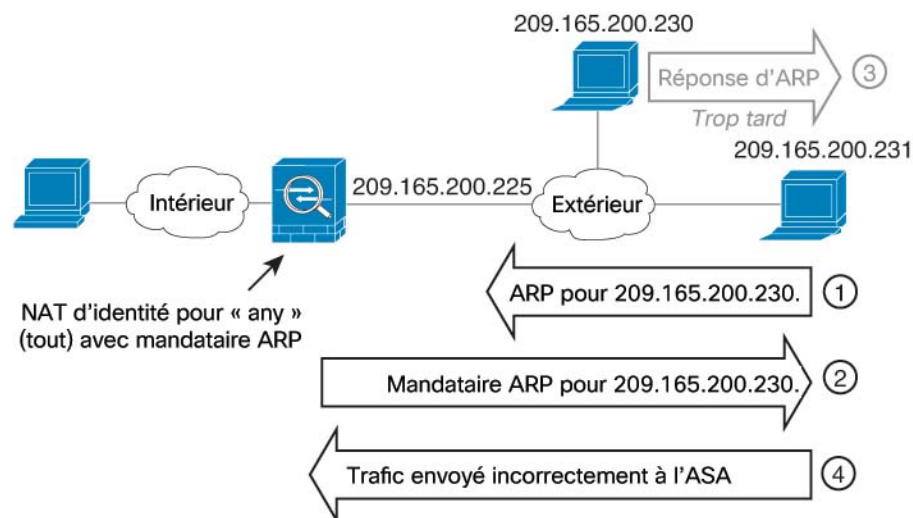
Pour le mode transparent, si l'hôte réel est connecté directement, configurez la voie de routage statique sur le routeur en amont pour pointer vers ASA : spécifiez l'adresse IP du groupe de ponts. Pour les hôtes distants en mode transparent, dans la voie de routage statique sur le routeur en amont, vous 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 fera ensuite passer l'ARP par un serveur mandataire pour l'adresse, même si le paquet n'est pas réellement destiné à l'ASA. (Notez que ce problème se produit même si vous avez une règle NAT Twice ; 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 ASA est reçue avant la réponse effective ARP de l'hôte, le trafic sera envoyé par erreur vers l'ASA.

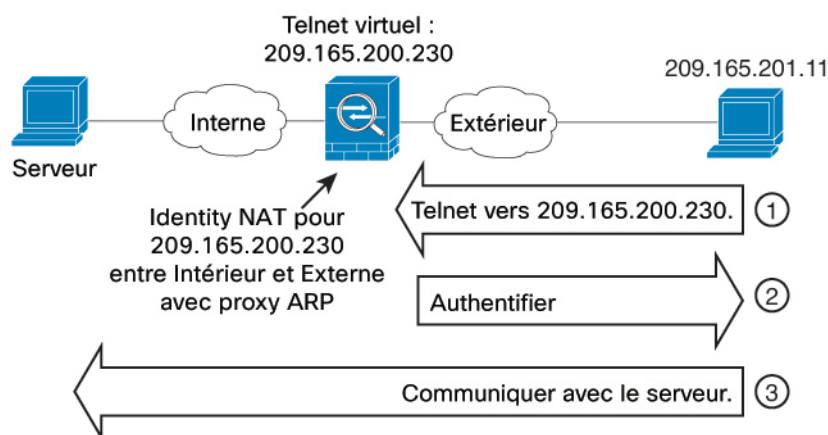
**Illustration 26 : Problèmes de mandataire ARP avec la NAT d'identité**



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.

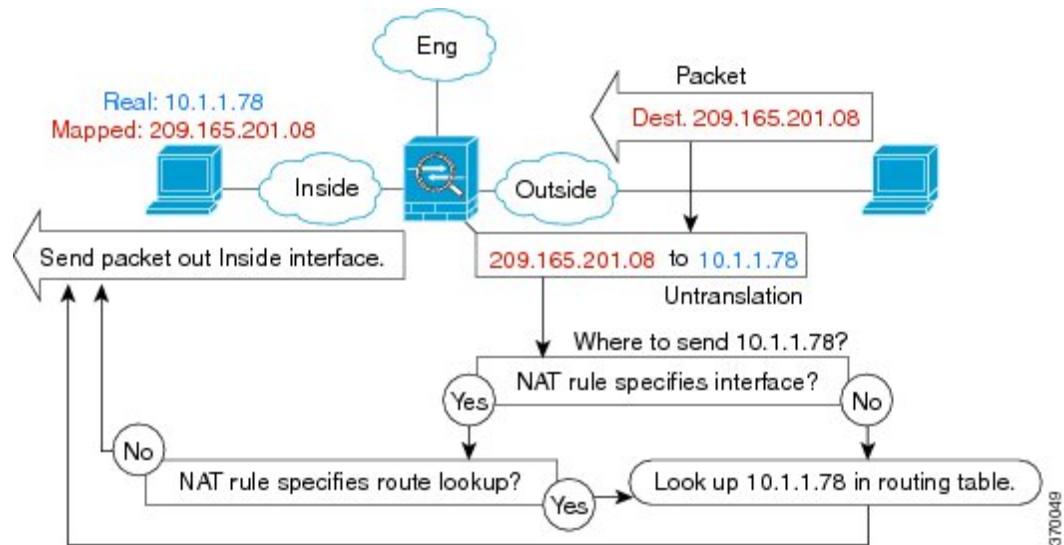
## Détermination de l'interface de sortie

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. 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



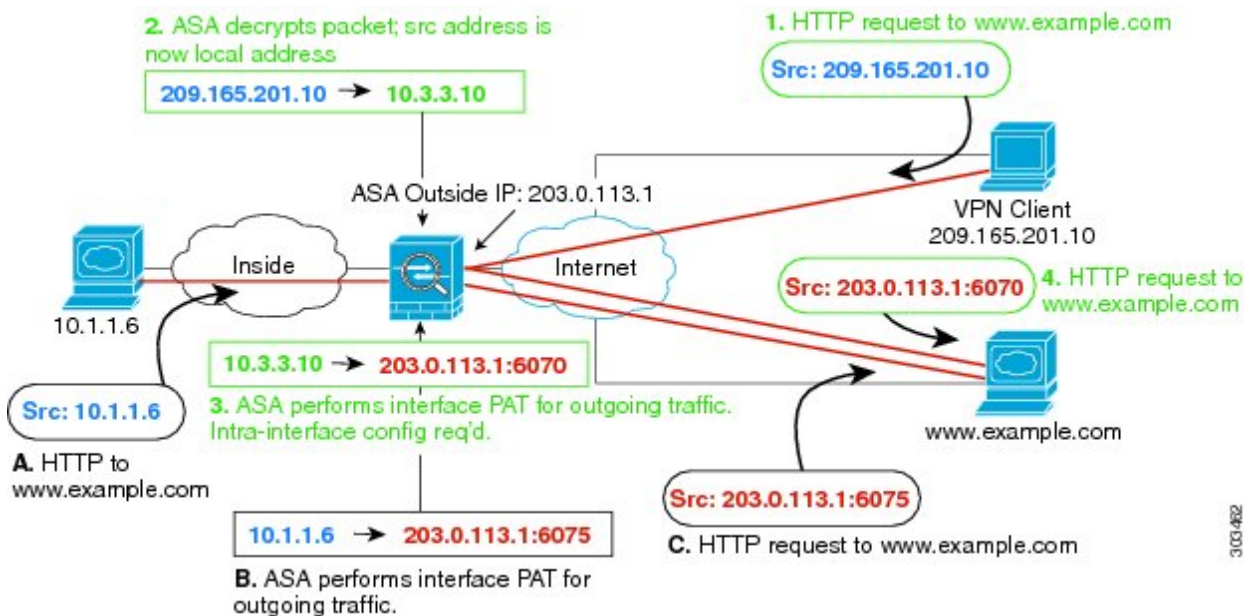
## NAT pour VPN

Les rubriques suivantes expliquent l'utilisation de la NAT avec les différents types de VPN.

### NAT et VPN d'accès à distance

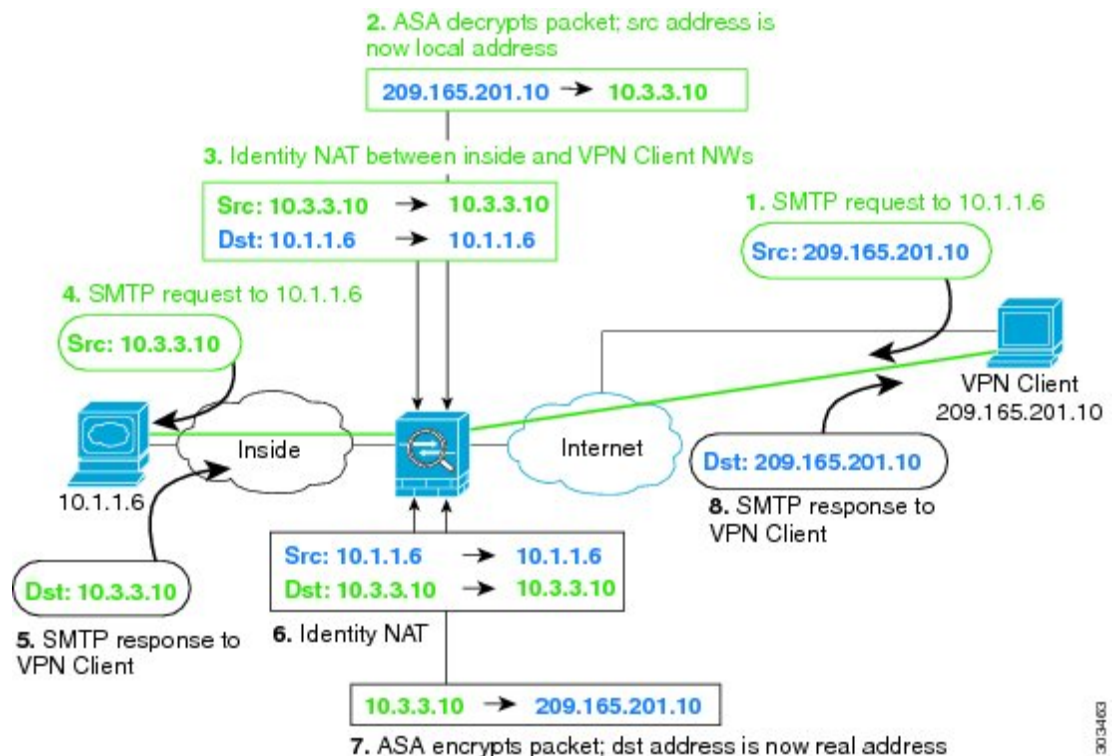
La figure suivante montre un serveur interne (10.1.1.6) et un client VPN (209.165.201.10) qui accèdent à Internet. Sauf si vous configurez la tunnellation fractionnée pour le client VPN (où seul le trafic spécifié passe par le tunnel VPN), le trafic VPN lié à Internet doit également passer par l'ASA. 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

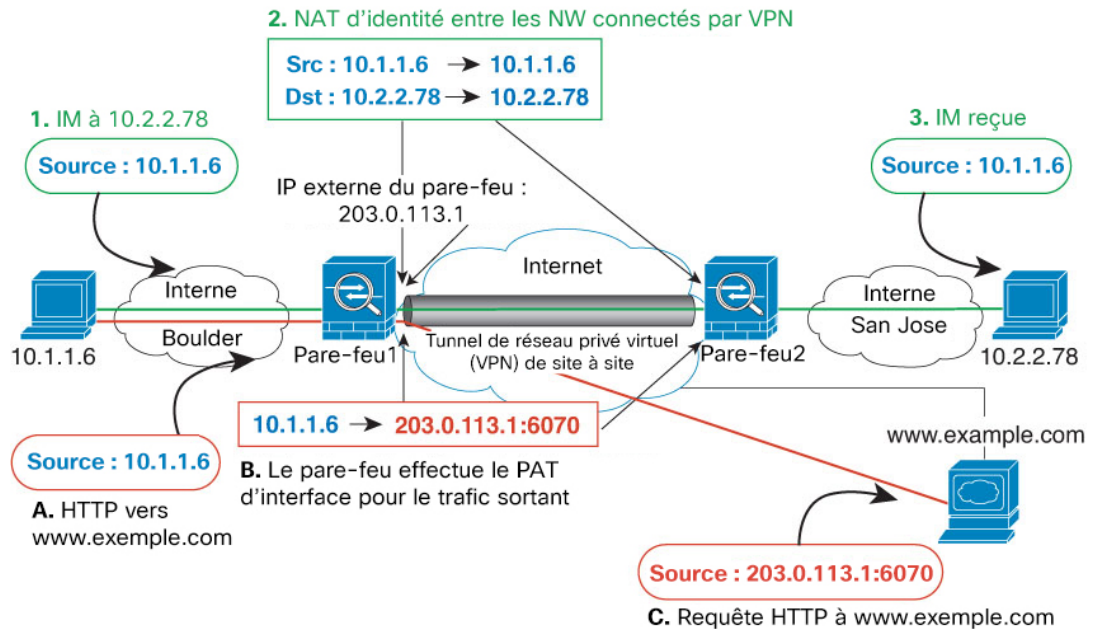
! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static inside_nw inside_nw destination static vpn_local vpn_local
```

## NAT et VPN de site à site

La figure suivante montre un tunnel de site à site connectant les bureaux de Boulder et de San Jose. Pour le trafic que vous souhaitez diriger vers Internet (par exemple, de la section 10.1.1.6 à Boulder vers [www.exemple.com](http://www.exemple.com)), vous avez besoin d'une adresse IP publique fournie par la NAT pour accéder à Internet. L'exemple ci-dessous utilise les règles PAT d'interface. Cependant, pour le trafic que vous souhaitez acheminer par le tunnel VPN (par exemple, de la version 10.1.1.6 à Boulder au 10.2.2.78 à San Jose), vous ne souhaitez

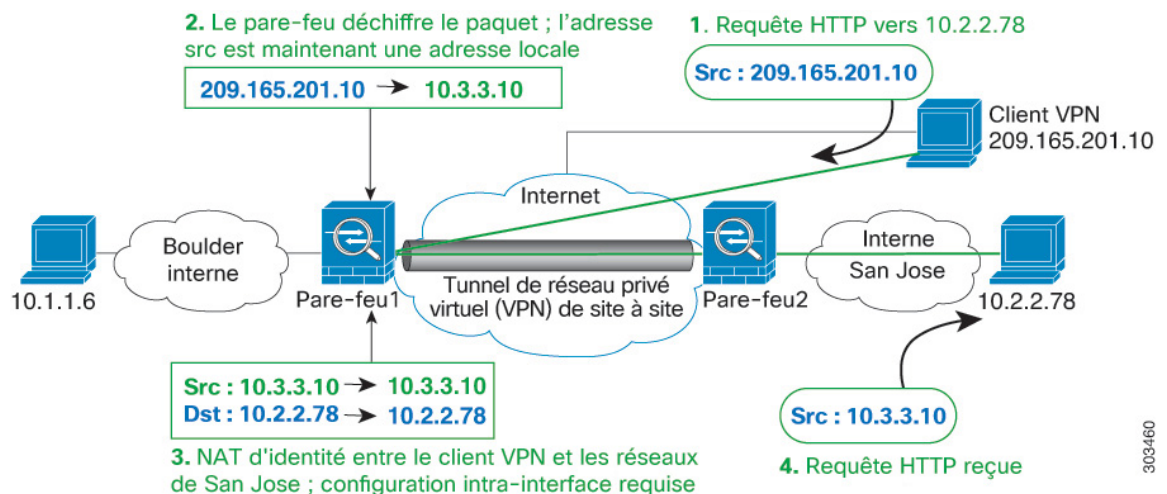
pas effectuer la NAT; vous devez exclure ce trafic en créant une règle NAT d'identité. La NAT d'identité traduit simplement une adresse en la même adresse.

**Illustration 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 tunnellation 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

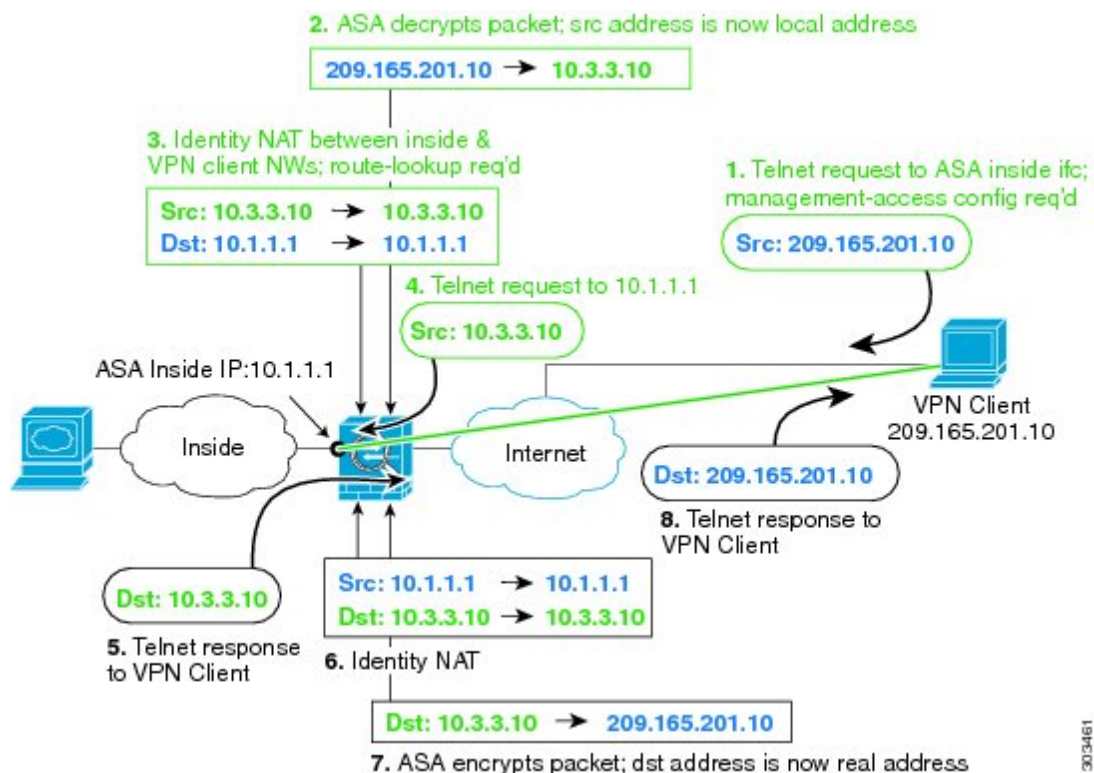
```

## 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 saisi l'ASA (voir la commande **management-access**). 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 209](#) ou [NAT et VPN de site à site, à la page 211](#), 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 208](#) 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 de réseaux IPv6

Dans les cas où vous devez transférer du trafic entre des réseaux IPv6 uniquement et des réseaux IPv4 uniquement, vous devez utiliser la NAT pour convertir les types d'adresses. Même avec deux réseaux IPv6, vous souhaitez peut-être masquer les adresses internes du réseau externe.

Vous pouvez utiliser les types de traduction suivants avec les réseaux IPv6 :

- **NAT64, NAT46** : Traduit les paquets IPv6 en IPv4 et vice versa. Vous devez définir deux politiques, une pour la traduction d'IPv6 à IPv4 et une pour la traduction d'IPv4 à IPv6. Bien que vous puissiez accomplir cela à l'aide d'une seule règle NAT Twice, si le serveur DNS se trouve sur le réseau externe, vous devrez probablement réécrire la réponse DNS. Comme vous ne pouvez pas activer la réécriture DNS sur une règle NAT Twice 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

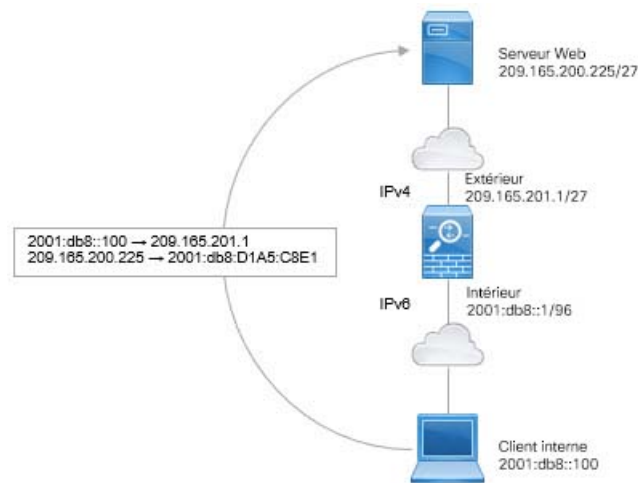
Lorsque le trafic passe d'un réseau IPv6 vers un réseau uniquement IPv4, vous devez convertir l'adresse IPv6 en IPv4 et renvoyer le trafic d'IPv4 à IPv6. Vous devez définir deux ensembles d'adresses, un ensemble d'adresses IPv4 pour lier les adresses IPv6 dans le réseau IPv4 et un ensemble d'adresses 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 NAT Twice, si le serveur DNS se trouve sur le réseau externe, vous devrez probablement réécrire la réponse DNS. Comme vous ne pouvez pas activer la réécriture DNS sur une règle NAT Twice 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 NAT Twice.



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.

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8::/96
```

**Étape 2** Créez la règle NAT Twice pour traduire le réseau IPv6 en IPv4 et inversement.

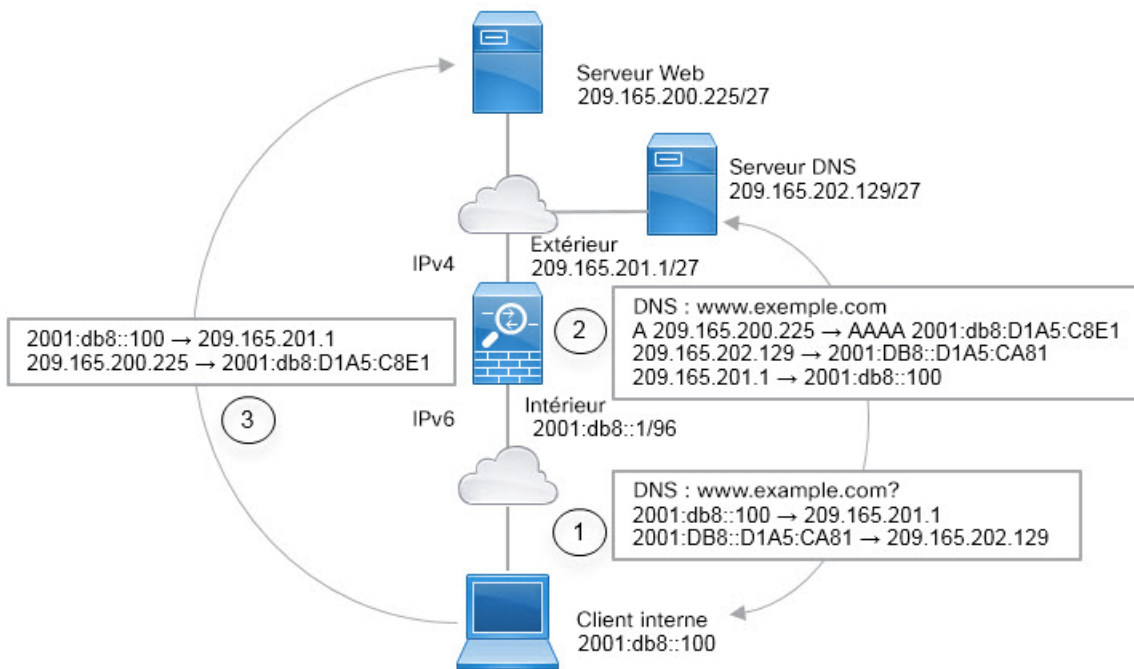
```
hostname(config)# nat (inside,outside) source dynamic inside_v6 interface
destination static inside_v6 any
```

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.

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



Dans cet exemple, vous allez traduire le réseau IPv6 interne en IPv4 à l'aide de l'interface dynamique PAT avec l'adresse IP de l'interface externe. Le trafic IPv4 externe est converti statiquement en adresses sur le réseau 2001:db8::/96, ce qui permet la transmission sur le réseau interne. Vous activez la réécriture DNS sur la règle NAT46, afin que les réponses du serveur DNS externe puissent être converties d'enregistrements A (IPv4) en enregistrements AAAA (IPv6) et les adresses converties d'IPv4 à IPv6.

Voici une séquence typique d'une requête Web où un client à l'adresse 2001:DB8::100 sur le réseau IPv6 interne tente d'ouvrir www.example.com.

1. L'ordinateur du client envoie une requête DNS au serveur DNS à l'adresse 2001:DB8::D1A5:CA81. Les règles NAT effectuent les traductions suivantes pour la source et la destination dans la requête DNS :
  - 2001:DB8::100 sur un port unique sur 209.165.201.1 (règle PAT de l'interface NAT64.)
  - 2001:DB8::D1A5:CA81 à 209.165.202.129 (la règle NAT46. D1A5 : CA81 est l'équivalent IPv6 de 209.165.202.129.)
2. Le serveur DNS répond par un enregistrement A, indiquant que www.example.com est au 209.165.200.225. La règle NAT46, avec la réécriture DNS activée, convertit l'enregistrement A en enregistrement AAAA équivalent au protocole IPv6, et traduit 209.165.200.225 en 2001:db8:D1A5:C8E1 dans l'enregistrement AAAA. De plus, les adresses de source et de destination dans la réponse DNS ne sont pas traduites :
  - 209.165.202.129 to 2001:DB8::D1A5:CA81
  - 209.165.201.1 to 2001:db8::100
3. Le client IPv6 a maintenant l'adresse IP du serveur Web et envoie une requête HTTP à www.example.com à l'adresse 2001:db8:D1A5:C8E1. (D1A5:C8E1 is the IPv6 equivalent of 209.165.200.225.) La source et la destination de la requête HTTP sont traduites :
  - 2001:DB8::100 sur un port unique sur 209.156.101.54 (règle PAT de l'interface NAT64).
  - 2001:db8:D1A5:C8E1 à 209.165.200.225 (la règle NAT46.)

La procédure suivante explique comment configurer cet exemple.

### Procédure

**Étape 1** Créez un objet réseau pour le réseau IPv6 interne et ajoutez la règle NAT64.

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8::/96
hostname(config-network-object)# nat(inside,outside) dynamic interface
```

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 2** Créez un objet réseau pour le réseau traduit IPv6 pour le réseau IPv4 externe et ajoutez la règle NAT46.

```
hostname(config)# object network outside_v4_any
hostname(config-network-object)# subnet 0.0.0.0 0.0.0.0
hostname(config-network-object)# nat(outside,inside) static 2001:db8::/96 dns
```

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.

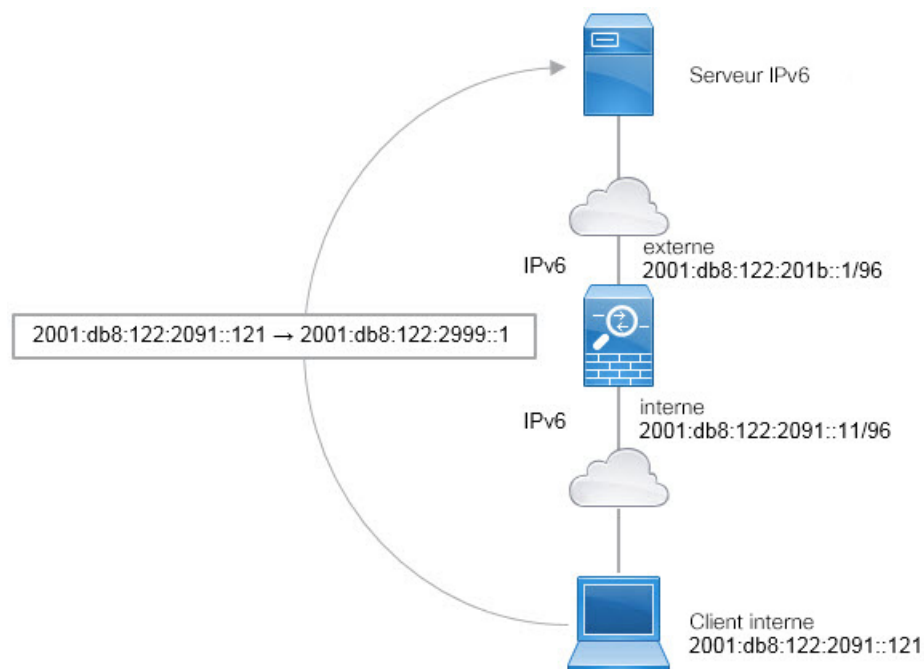
## NAT66 : Traduction d'adresses IPv6 en adresses différentes IPv6

Lorsque vous passez 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 la NAT Twice.

### Exemple NAT66, de 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

Créez l'objet réseau pour le réseau IPv6 interne et ajoutez la règle NAT statique.

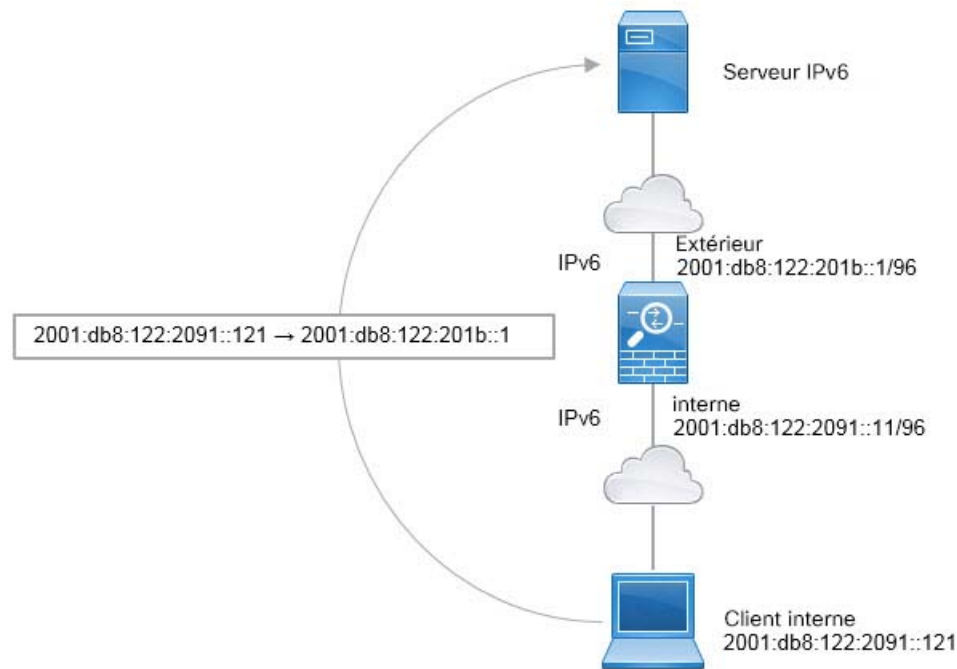
```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8:122:2091::/96
hostname(config-network-object)# nat(inside,outside) static 2001:db8:122:2999::/96
```

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

Créez l'objet réseau pour le réseau IPv6 interne et ajoutez la règle PAT dynamique.

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8:122:2091::/96
hostname(config-network-object)# nat (inside,outside) dynamic interface ipv6
```

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 réponses DNS à l'aide de la NAT

Vous devrez peut-être configurer 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, NAT 66, NAT46 et NAT64.

Voici les principales circonstances dans lesquelles vous devez configurer la réécriture DNS sur une règle NAT.

- La règle est NAT64 ou NAT46 et le serveur DNS se situe sur le réseau externe. Vous devez réécrire le DNS pour convertir les enregistrements DNS A (pour IPv4) et les enregistrements AAAA (pour IPv6).
- Le serveur DNS est à l'extérieur, les clients sont à l'intérieur et certains des noms de domaine complets que les clients utilisent mènent aux autres hôtes internes.
- Le serveur DNS est à l'intérieur et répond par des adresses IP privées, les clients sont à l'extérieur et les clients accèdent aux noms de domaine complets qui pointent vers des serveurs hébergés à l'intérieur.

### Limites de réécriture DNS

Voici quelques limites concernant la réécriture DNS :

- La réécriture DNS ne s'applique pas à la PAT, car plusieurs règles PAT sont applicables pour chaque enregistrement A ou AAAA et que la règle PAT à privilégier est ambiguë.
- Si vous configurez une règle NAT Twice, 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

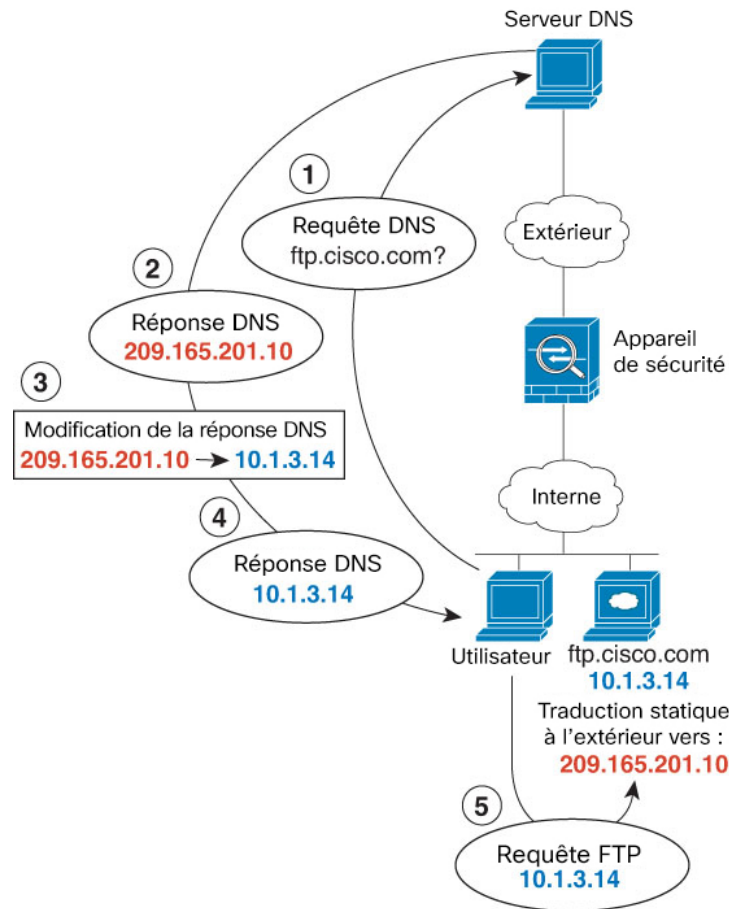
La figure suivante montre un serveur DNS accessible à partir de l'interface externe. Un serveur, ftp.cisco.com, se trouve sur l'interface interne. Vous configurez NAT pour traduire statiquement l'adresse réelle ftp.cisco.com (10.1.3.14) en une adresse mappée (20.165.201.10) visible sur le réseau externe.

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 (20.165.201.10). Le système fait référence à la règle statique pour le serveur interne et traduit l'adresse dans la réponse DNS au format 10.3.1.14. Si vous n'activez pas la modification de la réponse



DNS, l'hôte interne tente d'envoyer le trafic vers l'adresse 209.165.201.10 au lieu d'accéder directement à ftp.cisco.com.



## Procédure

**Étape 1** Créez un objet réseau pour le serveur FTP.

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 10.1.3.14
```

**Étape 2** Configurez la règle NAT statique avec modification DNS.

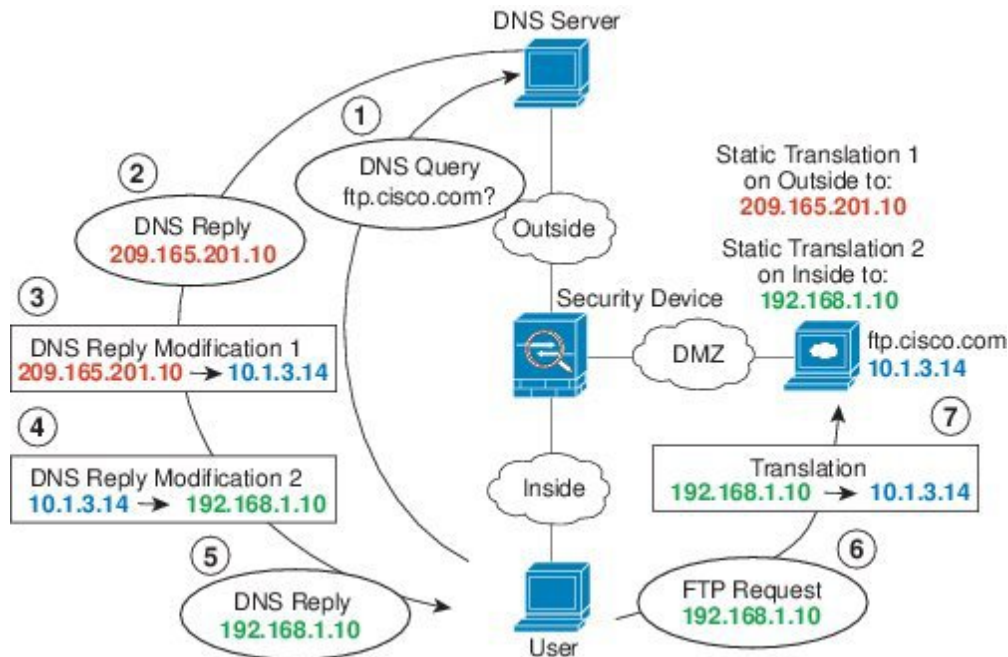
```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10 dns
```

## 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.

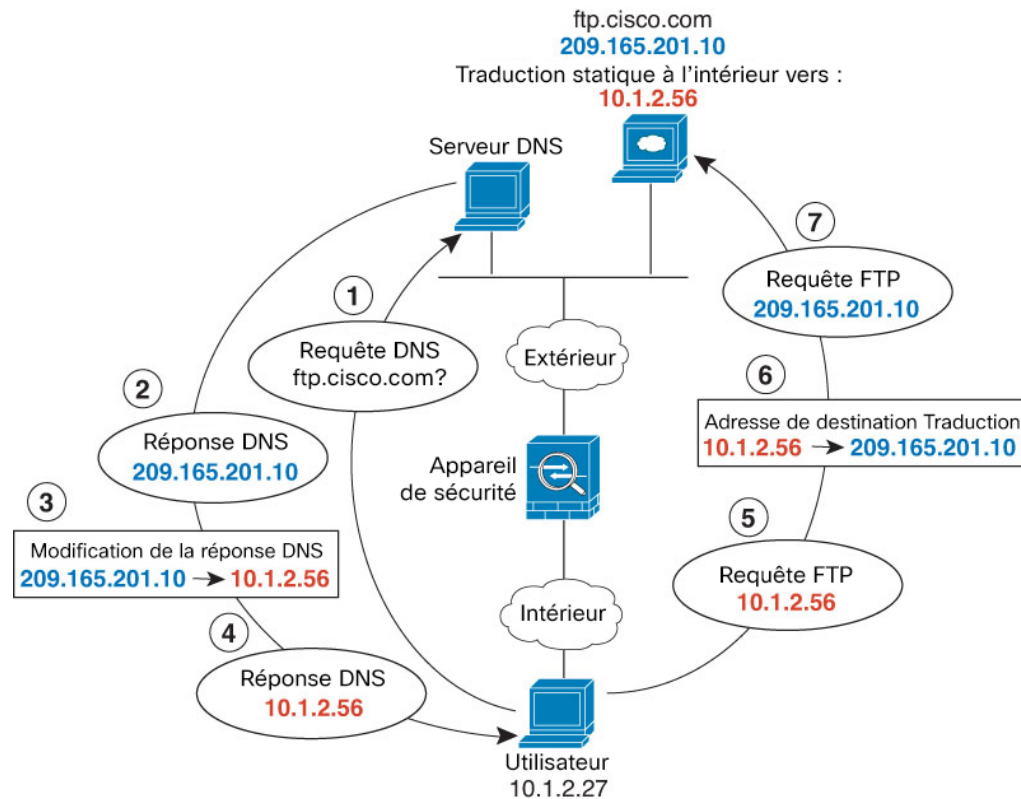
Si l'utilisateur doit accéder à ftp.cisco.com en utilisant l'adresse réelle, aucune autre configuration n'est requise. S'il y a également une règle statique entre l'intérieur et DMZ, vous devez également activer la modification de la réponse DNS sur cette règle. La réponse DNS sera ensuite modifiée deux 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, 209.165.20.10. Comme vous souhaitez que les utilisateurs internes utilisent l'adresse mappée pour ftp.cisco.com (10.1.2.56), vous devez configurer la modification de la réponse DNS pour la traduction statique.



## Procédure

**Étape 1** Créez un objet réseau pour le serveur FTP.

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 209.165.201.10
```

**Étape 2** Configurez la règle NAT statique avec modification DNS.

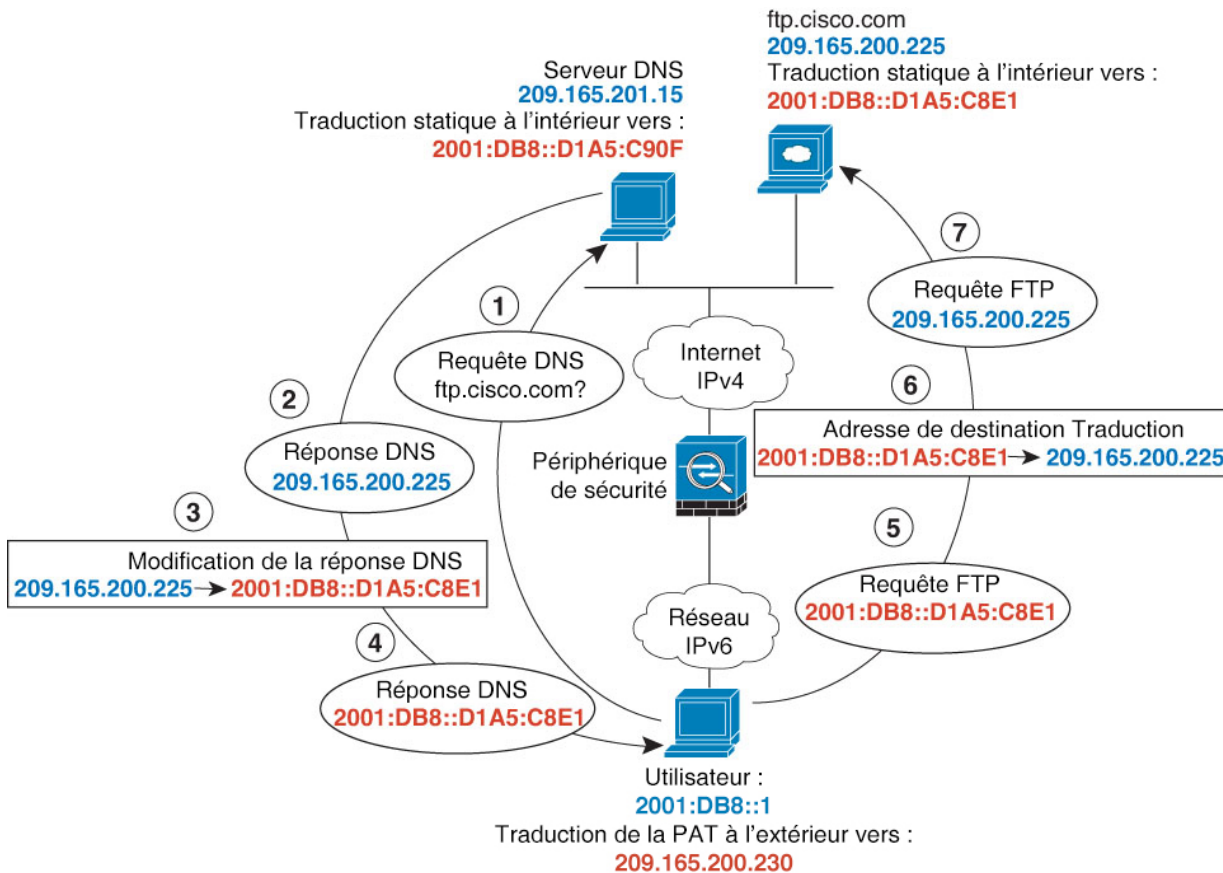
```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.56 dns
```

## 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** Créez un objet réseau pour le serveur FTP et configurez la NAT statique avec modification DNS. Comme il s'agit d'une traduction un à un, incluez l'option **net-to-net** pour NAT46.

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 209.165.200.225
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C8E1/128
net-to-net dns
```

**Étape 2** Créez un objet réseau pour le serveur DNS et configurez la NAT statique. Incluez l'option **rnet-to-net** pour NAT46.

```
hostname(config)# object network DNS_SERVER
hostname(config-network-object)# host 209.165.201.15
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C90F/128
net-to-net
```

**Étape 3** Configurez un pool PAT IPv4 pour traduire le réseau IPv6 interne.

**Exemple :**

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 209.165.200.230 209.165.200.235
```

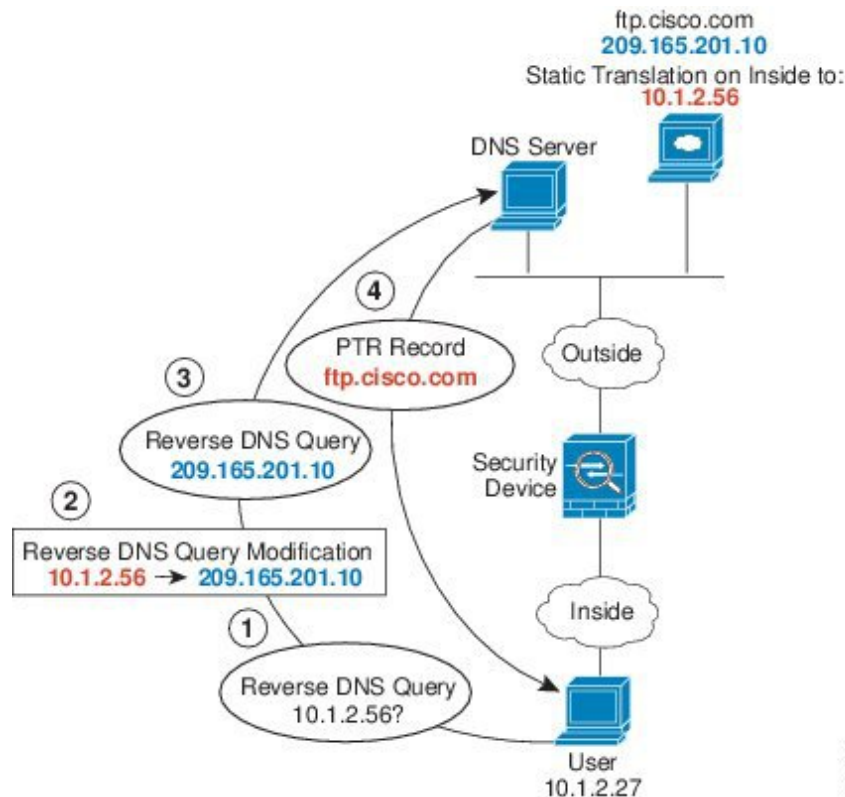
**Étape 4** Créez un objet réseau pour le réseau IPv6 interne, et configurez la NAT dynamique avec un pool PAT.

```
hostname(config)# object network IPv6_INSIDE
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

## 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 retransmis en IPv4 à la périphérie du fournisseur de services.

- [Mappage de l'adresse et du port \(MAP\), à la page 229](#)
- [Lignes directrices pour le mappage de l'adresse et du port \(MAP\), à la page 230](#)
- [Configurer les domaines MAP-T, à la page 232](#)
- [Surveillance MAP, à la page 234](#)
- [Historique du MAP, à la page 235](#)

## 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.

## Mappage de l'adresse et de la traduction 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)

### Lignes directrices sur le mode pare-feu

Vous pouvez configurer MAP en mode routé uniquement. Le mode transparent n'est pas pris en charge.

### Lignes directrices 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 mappage 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)
  - Intercommunication IPsec
  - 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

Créez (ou modifiez) le domaine MAP.

**map-domain** *name*

Où le nom est une chaîne alphanumérique de 48 caractères maximum. Le nom peut également inclure les caractères spéciaux suivants : point (.), barre oblique (/) et deux-points (:).

**Exemple :**

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)#
```

#### Étape 2

Configurez la règle de mappage par défaut.

**default-mapping-rule** *ipv6\_prefix/prefix\_length*

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.

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.

**Exemple :**

```
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
```

#### Étape 3

Configurez 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).

- Entrez en mode de configuration des règles de mappage de base.

**basic-mapping-rule**

- b) Configurer le préfixe IPv4.

**ipv4-prefix** *ipv4\_network\_address netmask*

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.

- c) Configurez le préfixe IPv6.

**ipv6-prefix** *ipv6\_prefix/prefix\_length*

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.

- d) Configurez le port de départ.

**start-port** *number*

Le 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.

- e) Configurez le rapport de port, qui détermine le nombre de ports dans le pool de ports.

**share-ratio** *number*

Précisez le nombre de ports qui doivent faire partie du pool. Le nombre doit être une puissance de 2, de 1 à 65536, comme 1, 2, 4, 8, etc.

### Exemple :

```
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

### Exemple

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
```

```
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

## 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.

La commande **show map-domain** affiche la configuration MAP (semblable à la commande **show running-config map-domain**), mais indique également si une configuration de domaine est valide. Dans l'exemple suivant, il y a deux domaines, 1 et 2. Le résultat explique que le domaine MAP 2 est incomplet et qu'il n'est donc pas actif.

```
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 : l'adresse IP/le port de nœud MAP *adresse IP/port* a un encodage d'ID défini de port incohérent

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 du MAP

| Nom de la caractéristique                                | Versions de plateforme | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mappage de l'adresse et de la traduction du port (MAP-T) | 9.13(1)                | <p>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.</p> <p>Nous avons introduit ou modifié les commandes suivantes : <b>basic-mapping-rule</b>, <b>default-mapping-rule</b>, <b>ipv4-prefix</b>, <b>ipv6-prefix</b>, <b>map-domain</b>, <b>share-ratio</b>, <b>show map-domain</b>, <b>start-port</b>.</p> |





## PARTIE **IV**

# Politiques de service et inspection des applications

- [Politique de service, à la page 239](#)
- [Premiers pas avec l'inspection du protocole de la couche application, à la page 261](#)
- [Inspection des protocoles Internet de base, à la page 283](#)
- [Inspection des protocoles vocaux et vidéo, à la page 327](#)
- [Inspection des réseaux mobiles, à la page 353](#)







## CHAPITRE 11

# Politique de service

Les politiques de service qui utilisent Modular Policy Framework 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 239](#)
- [Lignes directrices pour les politiques de service, à la page 246](#)
- [Par défaut pour les politiques de service, à la page 247](#)
- [Configurer les politiques de service, à la page 249](#)
- [Surveillance des politiques de service, à la page 257](#)
- [Exemples de politiques de service \(cadre de politique modulaire\), à la page 257](#)
- [Historique des politiques de service, à la page 260](#)

## 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 :

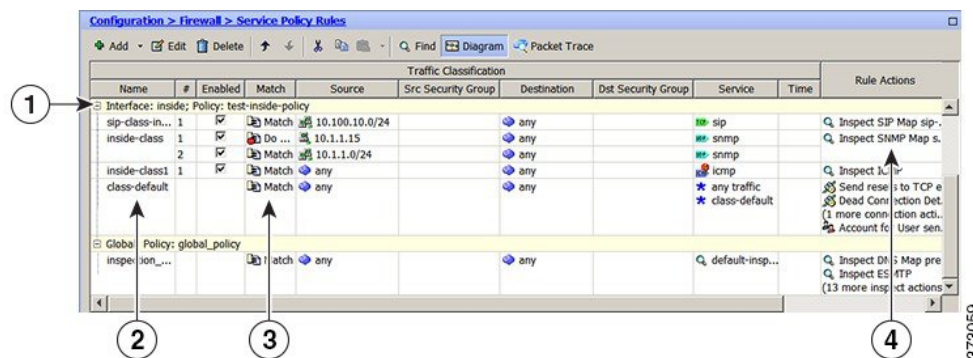
1. La liste des politiques de service, qui est l'ensemble ordonné de règles, et est nommée dans la commande **service-policy**. Dans ASDM, la liste des politiques est représentée sous forme de dossier sur la page des règles de politique de service.

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 | <ul style="list-style-type: none"> <li>• Premiers pas avec l'inspection du protocole de la couche application, à la page 261.</li> <li>• Inspection des protocoles Internet de base, à la page 283.</li> <li>• Inspection des protocoles vocaux et vidéo, à la page 327.</li> <li>• Inspection des réseaux mobiles, à la page 353.</li> </ul> |
| 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 439.                                                                                                                                                                                                                                                                                                            |

| Fonctionnalités                                                                                           | Pour le trafic de transit? | Pour le trafic de gestion? | Voir :                                                                      |
|-----------------------------------------------------------------------------------------------------------|----------------------------|----------------------------|-----------------------------------------------------------------------------|
| File d'attente prioritaire standard QoS                                                                   | Oui                        | Non                        | <a href="#">Qualité de service, à la page 439.</a>                          |
| Limites et délais d'expiration de connexion TCP et UDP et répartition aléatoire du numéro de séquence TCP | Oui                        | Oui                        | <a href="#">Paramètres de connexion, à la page 405.</a>                     |
| normalisation TCP                                                                                         | Oui                        | Non                        | <a href="#">Paramètres de connexion, à la page 405.</a>                     |
| contournement de l'état du TCP                                                                            | Oui                        | Non                        | <a href="#">Paramètres de connexion, à la page 405.</a>                     |
| Statistiques d'utilisateurs pour le pare-feu d'identité                                                   | Oui                        | Oui                        | Consultez la commande <b>user-statistics</b> dans la référence de commande. |

## Sens d'application des fonctionnalités

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 des fonctionnalités**

| 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                    |
| normalisation TCP                                                                                         | 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 de mappage de classe dans une mise en correspondance de politiques pour une interface donnée selon les règles suivantes :

1. Un paquet ne peut correspondre qu'à une seule carte de classe dans la et chaque type de fonctionnalité.
2. Lorsque le paquet correspond à une de carte de trafic pour un type de fonctionnalité, l'ASA ne tente pas de le mettre en correspondance avec les de cartes de trafic ultérieures pour ce type de fonctionnalité.
3. Si le paquet correspond à une de carte de trafic ultérieure pour un type de fonctionnalité différent, l'ASA applique également les actions pour la de carte de trafic ultérieure, si elle est prise en charge. Consultez [Incompatibilité de certaines actions de fonctionnalité, à la page 244](#) 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 de carte de trafic pour les limites de connexion, ainsi qu'à une de carte de trafic pour une inspection d'application, les deux actions sont appliquées.
- Si un paquet correspond à une de carte de trafic pour l'inspection HTTP, mais correspond également à une autre de carte de trafic qui inclut l'inspection HTTP, les actions de la deuxième de carte de trafic ne sont pas appliquées.
- Si un paquet correspond à une de carte de trafic pour l'inspection HTTP, mais correspond également à une autre de carte de trafic qui comprend l'inspection FTP, les actions de la deuxième de carte de trafic ne sont pas appliquées, car les inspections HTTP et FTP ne peuvent pas être combinées.
- Si un paquet correspond à une de carte de trafic pour l'inspection HTTP, mais correspond également à une autre de carte 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 dans une politique de service de sont effectués est indépendant de l'ordre dans lequel les actions apparaissent dans le de la liste des politiques.

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 d'adresse 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 244](#) 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 244](#).

**Remarque**

La commande **match default-inspection-traffic**, 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, vous donnant ainsi la flexibilité d'appliquer des inspections à des ports non standard, par exemple.

Un exemple d'erreur de configuration est si vous configurez plusieurs inspections dans la même liste des politiques et n'utilisez pas le raccourci default-inspection-traffic. Dans le premier exemple, le trafic destiné au port 21 est configuré par erreur pour l'inspection FTP et HTTP. Dans le deuxième exemple, le trafic destiné au port 80 est configuré par erreur pour l'inspection FTP et HTTP. Dans les deux cas d'exemples de configuration incorrecte, seule l'inspection FTP est appliquée, car FTP précède HTTP dans l'ordre des inspections appliquées.

**Exemple 1 : Mauvaise configuration pour les paquets FTP : l'inspection HTTP a également été configurée**

```
class-map ftp
 match port tcp eq 21
class-map http
 match port tcp eq 21 [it should be 80]
policy-map test
 class ftp
 inspect ftp
 class http
 inspect http
```

**Exemple 2 : Mauvaise configuration pour les paquets HTTP : l'inspection FTP a également été configurée**

```
class-map ftp
 match port tcp eq 80 [it should be 21]
class-map http
 match port tcp eq 80
policy-map test
 class ftp
 inspect ftp
 class http
 inspect http
```

## 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 carte de 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 264.

### Lignes directrices pour 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 264.
- 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 des 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 listes des politiques

Consultez les lignes directrices suivantes concernant l'utilisation des listes des politiques :

- Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface. Pour les pare-feu bas de gamme, vous pouvez créer jusqu'à 64 listes des politiques dans la configuration; pour des pare-feu plus puissants, vous pouvez créer jusqu'à 128 listes des politiques.
- Vous pouvez appliquer la même liste des politiques à plusieurs interfaces.
- Vous pouvez identifier jusqu'à 63 cartes de trafic de couche 3/4 dans une liste des politiques de couche 3/4.
- Pour chaque carte de trafic, vous pouvez attribuer plusieurs actions à partir d'un ou de plusieurs types de fonctionnalités, le cas échéant. Consultez [Incompatibilité de certaines actions de fonctionnalité](#), à la page 244.

### 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` ; elle correspond au trafic d'inspection par défaut. Cette classe, 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 classe 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.

```
class-map inspection_default
match default-inspection-traffic
```

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 décrétement 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`.

```
class-map class-default
match any
```

## Configurer les politiques de service

Pour configurer les politiques de service à l'aide du cadre de politique modulaire, procédez comme suit :

### Procédure

#### Étape 1

Identifiez le trafic sur lequel vous souhaitez agir en créant des cartes de trafic 3/4, comme décrit dans [Identifier le trafic \(cartes de trafic de couche 3/4\)](#), à la page 251.

Par exemple, vous pourriez vouloir effectuer des actions sur tout le trafic qui passe par l'ASA ; ou vous pourriez ne souhaitez effectuer que certaines actions sur le trafic de 10.1.1.0/24 vers n'importe quelle adresse de destination.



#### Étape 2

Vous pouvez également effectuer des actions supplémentaires sur une partie du trafic d'inspection.

Si l'une des actions que vous souhaitez effectuer est l'inspection des applications et que vous souhaitez effectuer des actions supplémentaires sur une partie du trafic d'inspection, créez une carte de politique d'inspection. La liste des politiques d'inspection identifie le trafic et précise ce qu'il faut en faire.

Par exemple, vous pourriez vouloir abandonner toutes les requêtes HTTP dont la longueur de corps est supérieure à 1 000 octets.



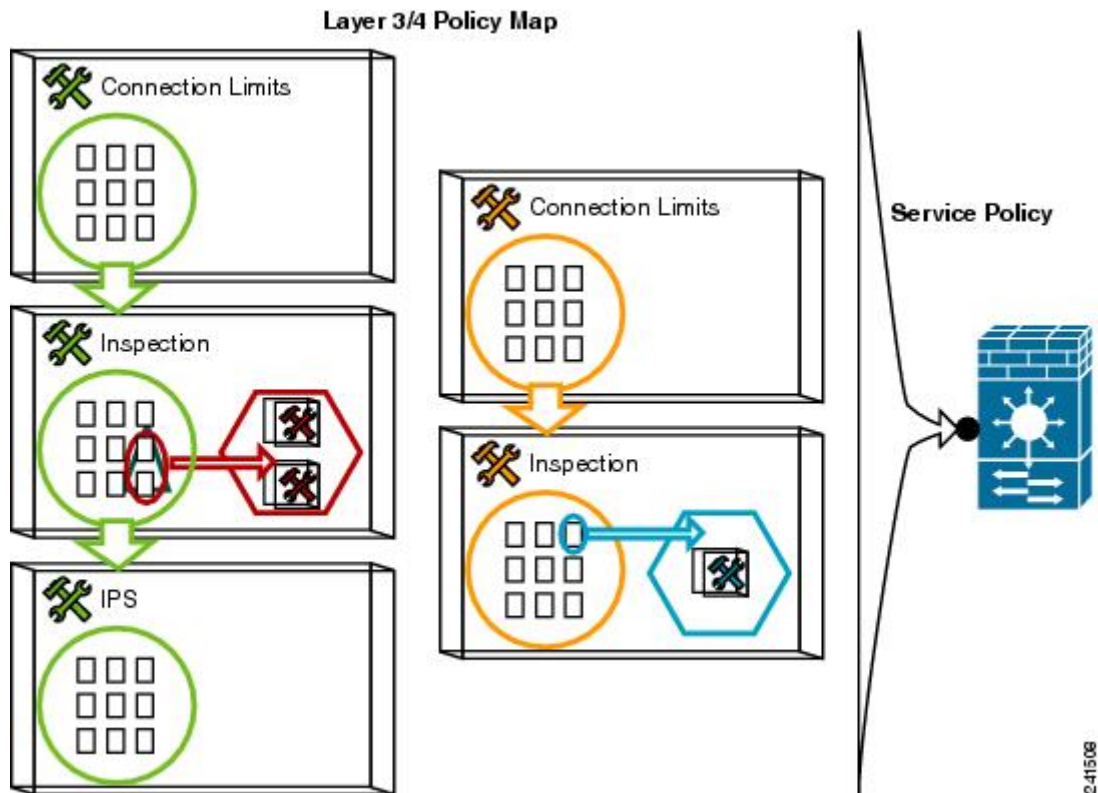
Vous pouvez créer une liste des politiques d'inspection autonome qui identifie le trafic directement à l'aide de commandes **match**, ou vous pouvez créer une carte de classe d'inspection pour la réutilisation ou pour une correspondance plus complexe. Par exemple, vous pouvez mettre en correspondance du texte dans des paquets inspectés à l'aide d'une expression régulière ou d'un groupe d'expressions régulières (une carte de trafic d'expression régulière) et cibler des actions en fonction de critères plus restreints. Par exemple, vous pourriez vouloir abandonner toutes les requêtes HTTP avec une URL contenant le texte « example.com ».



Consultez [Configurer l'inspection du protocole de couche d'application](#), à la page 270.

### Étape 3

Définissez les actions que vous souhaitez effectuer sur chaque carte de classe de couche 3/4 en créant une carte de politiques de couche 3/4, comme décrit dans [Définir les actions \(liste des politiques de couche 3/4\)](#), à la page 254.



### Étape 4

Déterminez sur quelles interfaces vous souhaitez appliquer la liste des politiques ou appliquez-la globalement, comme décrit dans [Appliquer les actions à une interface \(politique de service\)](#), à la page 256.

## Identifier le trafic (cartes de trafic de couche 3/4)

Une carte de classe de couche 3/4 identifie le trafic de couche 3 et 4 auquel vous souhaitez appliquer des actions. Vous pouvez créer plusieurs cartes de classe de couche 3/4 pour chaque carte de politique de couche 3/4.

### Créer une carte de trafic de couche 3/4 pour le trafic de transit

Une carte de trafic de couche 3/4 établit une correspondance du trafic en fonction des protocoles, des ports, des adresses IP et d'autres attributs de couche 3 ou 4.



#### Astuces

Nous vous suggérons d'inspecter le trafic uniquement sur les ports sur lesquels vous attendez un trafic d'application; si vous inspectez tout le trafic, par exemple à l'aide de **match any**, les performances de l'ASA peuvent être affectées.

#### Procédure

##### Étape 1

Créer une ☐ carte de trafic de couche 3/4 : **class-map** *class\_map\_name*

Où *class\_map\_name* est une chaîne d'une longueur maximale de 40 caractères.

Le nom « class-default » est réservé. Tous les types de cartes de trafic utilisent le même espace de nom, de sorte que vous ne pouvez pas réutiliser un nom déjà utilisé par un autre type de carte de trafic. L'interface de ligne de commande passe en mode de configuration class-map.

#### Exemple :

```
hostname(config)# class-map all_udp
```

##### Étape 2

(Facultatif) Ajoutez une description à la carte de trafic.

**description** *string*

#### Exemple :

```
hostname(config-cmap)# description All UDP traffic
```

##### Étape 3

Établissez une correspondance du trafic à l'aide de l'une des commandes suivantes. Sauf indication contraire, vous ne pouvez inclure qu'une seule commande **match** dans la carte de trafic.

- **match any (tout)** : établit une correspondance avec tout le trafic.

```
hostname(config-cmap)# match any
```

- **match access-list** *access\_list\_name* : établit une correspondance avec le trafic spécifié par une ACL étendue.

```
hostname(config-cmap)# match access-list udp
```

- **match port {tcp | udp | sctp} {eq port\_num | range port\_num port\_num}** : correspond aux ports de destination, qu'il s'agisse d'un port unique ou d'une plage de ports contigus, pour le protocole indiqué. Pour les applications qui utilisent plusieurs ports non contigus, utilisez la commande **match access-list** et définissez une ACE pour chaque port.

```
hostname(config-cmap)# match tcp eq 80
```

- **match default-inspection-traffic** : établit une correspondance avec le trafic d'inspection par défaut : les ports TCP et UDP par défaut utilisés par toutes les applications que l'ASA peut inspecter.

```
hostname(config-cmap)# match default-inspection-traffic
```

Cette commande, qui est utilisée dans la politique globale par défaut, est un raccourci spécial de l'interface de ligne de commande qui, lorsqu'il est utilisé dans une liste des politiques, 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 (à l'exception de l'inspection WAAS, qui peut être configurée avec d'autres inspections. Consultez [Incompatibilité de certaines actions de fonctionnalité, à la page 244](#) pour obtenir plus d'informations sur la combinaison d'actions). Normalement, l'ASA n'utilise pas le numéro de port pour déterminer l'inspection appliquée, vous permettant ainsi d'appliquer des inspections à des ports non standard, par exemple.

Consultez [Inspections par défaut et limites de la NAT, à la page 265](#) pour obtenir la liste des ports par défaut. Toutes les applications dont les ports sont inclus dans la commande **match default-inspection-traffic** ne sont pas activées par défaut dans la liste des politiques.

Vous pouvez spécifier une commande **match access-list** avec la commande **match default-inspection-traffic** afin de restreindre le trafic correspondant. Comme la commande **match default-inspection-traffic** spécifie les ports et les protocoles à mettre en correspondance, tous les ports et protocoles figurant dans l'ACL sont ignorés.

- **match dscp value1 [value2] [...] [value8]** : correspond à la valeur DSCP dans un en-tête IP, jusqu'à huit valeurs DSCP.

```
hostname(config-cmap)# match dscp af43 cs1 ef
```

- **match precedence value1 [value2] [value3] [value4]** : correspond à quatre valeurs de priorité, représentées par l'octet TOS dans l'en-tête IP, où les valeurs de priorité peuvent être comprises entre 0 et 7.

```
hostname(config-cmap)# match precedence 1 4
```

- **match rtp starting\_port range** : correspond au trafic RTP, où le *starting\_port* spécifie un port de destination UDP pair entre 2000 et 65534. La *range* spécifie le nombre de ports UDP supplémentaires à mettre en correspondance au-dessus du *starting\_port*, entre 0 et 16 383.

```
hostname(config-cmap)# match rtp 4004 100
```

- **match tunnel-group name** : établit une correspondance avec le trafic du groupe de tunnels VPN auquel vous souhaitez appliquer la QoS.

Vous pouvez également spécifier une autre commande **match** afin d'affiner la correspondance du trafic. Vous pouvez spécifier n'importe laquelle des commandes précédentes, à l'exception de **match any**, **match access-list**, ou **match default-inspection-traffic**. Vous pouvez également saisir la commande **match flow ip destination-address** pour faire correspondre les flux dans le groupe de tunnels vers chaque adresse IP.

```
hostname(config-cmap)# match tunnel-group group1
hostname(config-cmap)# match flow ip destination-address
```

## Exemples

Voici un exemple pour la commande **class-map** :

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp

hostname(config-cmap)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp

hostname(config-cmap)# class-map all_http
hostname(config-cmap)# description "This class-map matches all HTTP traffic"
hostname(config-cmap)# match port tcp eq http

hostname(config-cmap)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
hostname(config-cmap)# match access-list host_foo
```

## Créer une carte de trafic de couche 3/4 pour le trafic de gestion

Pour le trafic de gestion vers l'ASA, vous pouvez effectuer des actions spécifiques à ce type de trafic. Vous pouvez spécifier une carte de trafic de gestion qui peut correspondre à une ACL ou à des ports TCP ou UDP. Les types d'actions disponibles pour une carte de trafic de gestion dans la liste des politiques sont spécialisées dans le trafic de gestion.

### Procédure

**Étape 1** Créez une carte de trafic de gestion : **class-map type management class\_map\_name**

Où *class\_map\_name* est une chaîne d'une longueur maximale de 40 caractères.

Le nom « class-default » est réservé. Tous les types de cartes de trafic utilisent le même espace de nom, de sorte que vous ne pouvez pas réutiliser un nom déjà utilisé par un autre type de carte de trafic. L'interface de ligne de commande passe en mode de configuration class-map.

**Exemple :**

```
hostname(config)# class-map management all_udp
```

**Étape 2** (Facultatif) Ajoutez une description à la carte de trafic.

**description** *string*

**Exemple :**

```
hostname(config-cmap)# description All UDP traffic
```

**Étape 3** Établissez une correspondance du trafic à l'aide de l'une des commandes suivantes.

- **match access-list** *access\_list\_name* : établit une correspondance avec le trafic spécifié par une ACL étendue.

```
hostname(config-cmap)# match access-list udp
```

- **match port** {*tcp* | *udp* | *sctp*} {*eq port\_num* | **range** *port\_num port\_num*} : correspond aux ports de destination, qu'il s'agisse d'un port unique ou d'une plage de ports contigus, pour le protocole indiqué. Pour les applications qui utilisent plusieurs ports non contigus, utilisez la commande **match access-list** et définissez une ACE pour chaque port.

```
hostname(config-cmap)# match tcp eq 80
```

## Définir les actions (liste des politiques de couche 3/4)

Après avoir configuré les cartes de trafic de couche 3/4 pour identifier le trafic, utilisez une liste des politiques de couche 3/4 pour associer des actions à ces cartes.



### Astuces

Le nombre maximal de listes des politiques est de 64, mais vous ne pouvez appliquer qu'une seule liste des politiques par interface.

### Procédure

**Étape 1** Ajoutez la liste des politiques : **policy-map** *policy\_map\_name*

Où *policy\_map\_name* est le nom de la liste des politiques, jusqu'à 40 caractères de longueur. Tous les types de listes des politiques utilisent le même espace de noms, de sorte que vous ne pouvez pas réutiliser un nom déjà utilisé par un autre type de liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.

**Exemple :**



```
hostname(config)# policy-map global_policy
```

**Étape 2** Préciser une carte de trafic de couche 3/4 précédemment configurée : **class** *class\_map\_name*

Où *nclass\_map\_name* est le nom de la carte de trafic.

Consultez [Identifier le trafic \(cartes de trafic de couche 3/4\), à la page 251](#) pour ajouter une carte de trafic.

**Exemple :**

```
hostname(config-pmap)# class all_http
```

**Étape 3** Précisez une ou plusieurs actions pour cette carte de trafic.

Consultez [Fonctionnalités configurées avec les politiques de service, à la page 241](#).

**Remarque**

S'il n'y a pas de commande **match default-inspection-traffic** dans une carte de trafic, au plus une commande **inspect** peut être configurée sous la classe.

**Étape 4** Répétez le processus pour chaque carte de trafic que vous souhaitez inclure dans cette liste des politiques.

## Exemples

Voici un exemple de commande **policy-map** pour une politique de connexion. Il limite le nombre de connexions autorisées pour le serveur Web 10.1.1.1 :

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning
connection to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

L'exemple suivant montre le fonctionnement de la correspondance multiple dans une liste des politiques :

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout idle 0:10:0
```

L'exemple suivant montre comment le trafic correspond à la première carte de trafic disponible et ne correspondra pas aux cartes de trafic ultérieures qui précisent les actions dans le même domaine de fonctionnalité :

```
hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap-c)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout idle 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap-c)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout idle 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap-c)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout idle 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

Lorsqu'une connexion Telnet est lancée, elle correspond à la **classe telnet\_traffic**. De même, si une connexion FTP est initiée, elle correspond à la **classe ftp\_traffic**. Pour toute connexion TCP autre que Telnet et FTP, elle correspondra à la **classe tcp\_traffic**. Même si une connexion Telnet ou FTP peut correspondre à la classe **tcp\_traffic**, l'ASA n'établit pas cette correspondance, car elles ont déjà correspondu à d'autres classes.

## Appliquer les actions à une interface (politique de service)

Pour activer la carte de politiques de couche 3/4, créez une politique de service qui l'applique à une ou plusieurs interfaces ou qui l'applique globalement à toutes les interfaces. Utilisez la commande suivante :

**service-policy** *policy\_map\_name* {**global** | **interface** *interface\_name*} [**fail-close**]

Lieu :

- *policy\_map\_name* est le nom de la liste des politiques.
- **global** crée une politique de service qui s'applique à toutes les interfaces qui n'ont pas de politique particulière.  
 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. Par défaut, la configuration comprend une politique globale qui correspond à tout le trafic d'inspection d'application par défaut et applique l'inspection au trafic globalement. La politique de service par défaut comprend la commande suivante : **service-policy global\_policy global**.
- **interface** *interface\_name* crée une politique de service en associant une carte de politiques à une interface.
- **fail-close** génère un journal système (767001) pour le trafic IPv6 qui est abandonné par les inspections d'applications qui ne prennent pas en charge le trafic IPv6. Par défaut, les journaux système ne sont pas générés.

## Exemples

Par exemple, la commande suivante active la carte de politiques inbound\_policy sur l'interface externe :

```
hostname(config)# service-policy inbound_policy interface outside
```

Les commandes suivantes désactivent la politique globale par défaut et en activent une nouvelle appelée new\_global\_policy.

```
hostname(config)# no service-policy global_policy global
hostname(config)# service-policy new_global_policy global
```

# Surveillance des politiques de service

Pour surveiller les politiques de service, entrez la commande suivante :

- **show service-policy**

Affiche les statistiques de la politique de service.

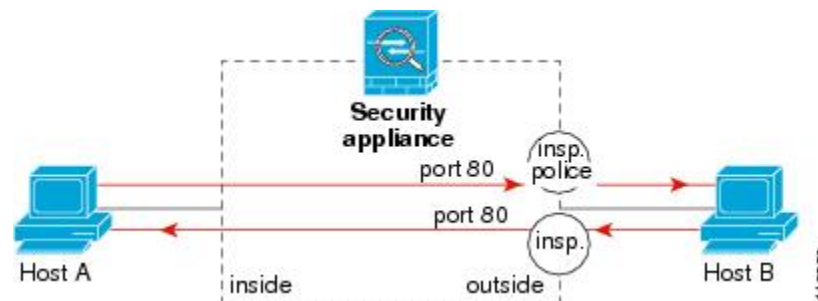
## Exemples de politiques de service (cadre de politique modulaire)

Cette section comprend plusieurs exemples de Modular Policy Framework

## Application de l'inspection et de la régulation QoS au trafic HTTP

Dans cet exemple, toute connexion HTTP (trafic TCP sur le port 80) qui entre dans l'ASA ou en sort par l'interface externe est classée pour l'inspection HTTP. Tout trafic HTTP qui quitte l'interface externe est classé pour le contrôle.

**Illustration 37 : Inspection HTTP et politique QoS**



Consultez les commandes suivantes pour cet exemple :

```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80
```

```

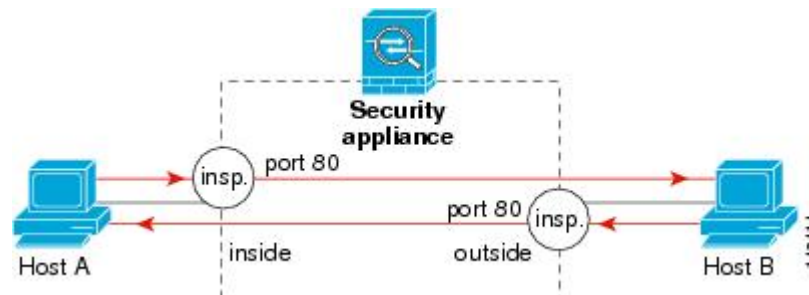
hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config-pmap-c)# police output 250000
hostname(config)# service-policy http_traffic_policy interface outside

```

## Application de l'inspection au trafic HTTP globalement

Dans cet exemple, toute connexion HTTP (trafic TCP sur le port 80) qui entre dans l'ASA par l'intermédiaire d'une interface est classée pour l'inspection HTTP. Comme la politique est une politique globale, l'inspection se produit uniquement lorsque le trafic entre dans chaque interface.

**Illustration 38 : Inspection HTTP globale**



Consultez les commandes suivantes pour cet exemple :

```

hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

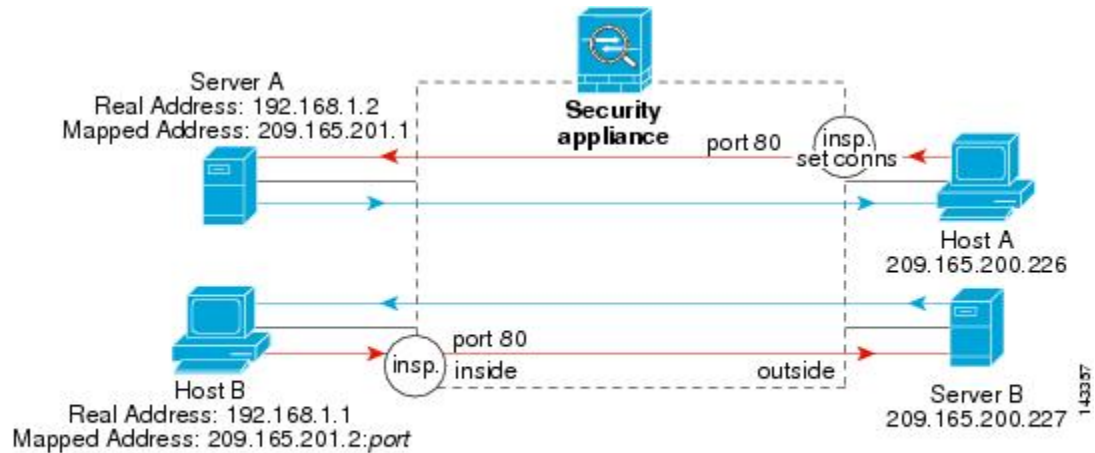
hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config)# service-policy http_traffic_policy global

```

## Application des limites d'inspection et de connexion au trafic HTTP vers des serveurs spécifiques

Dans cet exemple, toute connexion HTTP destinée au serveur A (trafic TCP sur le port 80) qui entre dans l'ASA par l'intermédiaire de l'interface externe est classée pour l'inspection HTTP et les limites de connexion maximales. Les connexions initiées du serveur A à l'hôte A ne correspondent pas à l'ACL dans la carte de trafic, elles ne sont donc pas affectées.

Toute connexion HTTP destinée au serveur B qui entre dans l'ASA par l'intermédiaire de l'interface interne est classée pour l'inspection HTTP. Les connexions initiées du serveur B à l'hôte B ne correspondent pas à l'ACL dans la carte de trafic, elles ne sont donc pas affectées.

**Illustration 39 : Limites d'inspection et de connexion HTTP pour des serveurs spécifiques**

Consultez les commandes suivantes pour cet exemple :

```
hostname(config)# object network obj-192.168.1.2
hostname(config-network-object)# host 192.168.1.2
hostname(config-network-object)# nat (inside,outside) static 209.165.201.1
hostname(config)# object network obj-192.168.1.0
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 209.165.201.2
hostname(config)# access-list serverA extended permit tcp any host 209.165.201.1 eq 80
hostname(config)# access-list ServerB extended permit tcp any host 209.165.200.227 eq 80

hostname(config)# class-map http_serverA
hostname(config-cmap)# match access-list serverA
hostname(config)# class-map http_serverB
hostname(config-cmap)# match access-list serverB

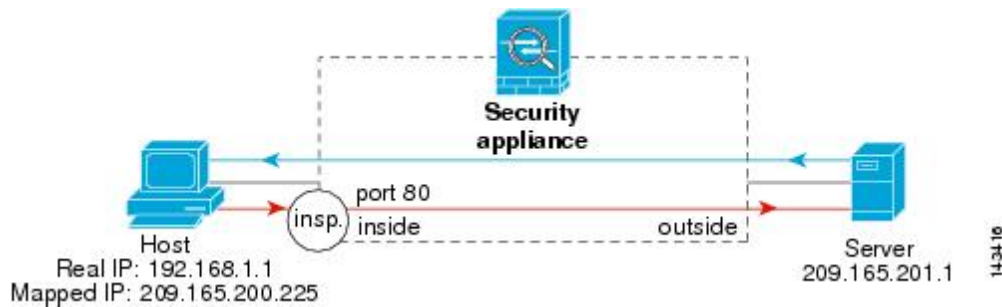
hostname(config)# policy-map policy_serverA
hostname(config-pmap)# class http_serverA
hostname(config-pmap-c)# inspect http
hostname(config-pmap-c)# set connection conn-max 100
hostname(config)# policy-map policy_serverB
hostname(config-pmap)# class http_serverB
hostname(config-pmap-c)# inspect http

hostname(config)# service-policy policy_serverB interface inside
hostname(config)# service-policy policy_serverA interface outside
```

## Application de l'inspection au trafic HTTP avec NAT

Dans cet exemple, l'hôte du réseau interne a deux adresses : l'une est l'adresse IP réelle 192.168.1.1, et l'autre est une adresse IP mappée utilisée sur le réseau externe, 209.165.200.225. Vous devez utiliser l'adresse IP réelle dans la liste de contrôle d'accès dans la carte de trafic. Si vous l'appliquiez à l'interface externe, vous utiliseriez également l'adresse réelle.

Illustration 40 : Inspection HTTP avec NAT



Consultez les commandes suivantes pour cet exemple :

```
hostname(config)# object network obj-192.168.1.1
hostname(config-network-object)# host 192.168.1.1
hostname(config-network-object)# nat (VM1,outside) static 209.165.200.225

hostname(config)# access-list http_client extended permit tcp host 192.168.1.1 any eq 80

hostname(config)# class-map http_client
hostname(config-cmap)# match access-list http_client

hostname(config)# policy-map http_client
hostname(config-pmap)# class http_client
hostname(config-pmap-c)# inspect http

hostname(config)# service-policy http_client interface inside
```

## 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 : <b>class-map type management</b> , et <b>inspect radius-accounting</b> .                                       |
| listes des politiques d'inspection                                          | 7.2(1)   | La liste des politiques d'inspection a été introduite. La commande suivante a été introduite : <b>class-map type inspect</b> .                                                                                                                                          |
| 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 : <b>class-map type regex</b> , <b>regex</b> , <b>match regex</b> .            |
| Match any pour les listes des politiques d'inspection                       | 8.0(2)   | Le mot-clé <b>match any</b> 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 <b>match all</b> 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 261](#)
- [Configurer l'inspection du protocole de couche d'application, à la page 270](#)
- [Configurer les expressions régulières, à la page 277](#)
- [Surveillance des politiques d'inspection, à la page 280](#)
- [Historique de l'inspection des applications, à la page 282](#)

## 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. Ensuite, vous l'ajoutez avec le nouveau nom de liste des politiques.

Par exemple, pour remplacer sip-map1 par sip-map2 dans l'inspection SIP, utilisez la séquence de commandes suivante :

```
hostname(config)# policy-map test
hostname(config-pmap)# class sip
hostname(config-pmap-c)# no inspect sip sip-map1
hostname(config-pmap-c)# inspect sip sip-map2
```

## Comment plusieurs classes de trafic sont gérées

Vous pouvez spécifier plusieurs mappages de classes d'inspection ou correspondances directes dans la liste des politiques 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. Par exemple, les commandes de correspondance suivantes peuvent être saisies dans n'importe quel ordre, mais la commande **match request method get** est mise en correspondance en premier.

```
match request header host length gt 100
 reset
match request method get
 log
```

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. Par exemple, pour un paquet dont la longueur d'en-tête est 1001, il correspondra à la première commande ci-dessous et sera journalisé, puis correspondra à la deuxième commande et sera réinitialisé. Si vous inversez l'ordre des deux commandes **match**, le paquet sera abandonné et la connexion sera réinitialisée avant de pouvoir correspondre à la deuxième commande **dmatch** ; il ne sera jamais journalisé.

```
match request header length gt 100
 log
match request header length gt 1000
 reset
```

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. Par exemple, les trois cartes de trafics suivantes contiennent deux types de commandes **match** : **match request-cmd** (priorité supérieure) et **match filename** (priorité inférieure). La carte de trafic ftp3 comprend les deux commandes, mais elle est classée selon la commande de priorité la plus basse, **match filename**. La carte de trafic ftp1 comprend la commande de priorité la plus élevée, elle est donc mise en correspondance en premier, quel que soit l'ordre dans la liste des politiques. La carte de trafic ftp3 est classée comme étant de la même priorité que la carte de trafic ftp2, qui contient également la commande **match filename**. Elles sont mises en correspondance selon l'ordre dans la liste des politiques : ftp3 puis ftp2.

```
class-map type inspect ftp match-all ftp1
 match request-cmd get
class-map type inspect ftp match-all ftp2
 match filename regex abc
class-map type inspect ftp match-all ftp3
 match request-cmd get
 match filename regex abc

policy-map type inspect ftp ftp
 class ftp3
 log
 class ftp2
```

```

log
class ftp1
log

```

## 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 :

- Diameter
- 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

### Lignes directrices 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 265](#).
- 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.<br>No NAT64.<br>(Mise en grappe) Pas de PAT statique.                      | —        | —                                                                                                                                                                                                        |
| DCERPC                            | TCP/135                                          | No NAT64.                                                                                      | —        | —                                                                                                                                                                                                        |
| Diameter                          | TCP/3868<br>TCP/5868 (pour TCP/TLS)<br>SCTP/3868 | Pas de NAT / PAT.                                                                              | RFC 6733 | Nécessite la licence Carrier (exploitant).                                                                                                                                                               |
| <b>DNS sur UDP</b><br>DNS sur TCP | UDP/53<br>UDP/443<br>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.<br><br>UDP/443 est utilisé uniquement pour les sessions DNScrypt de Cisco Umbrella. |
| <b>FTP</b>                        | TCP/21                                           | (Mise en grappe) Pas de PAT statique.                                                          | RFC 959  | —                                                                                                                                                                                                        |
| GTP                               | UDP/3386 (GTPv0)<br>UDP/2123 (GTPv1+)            | Pas de PAT étendue.<br>Pas de NAT.                                                             | —        | Nécessite la licence Carrier (exploitant).                                                                                                                                                               |

| Application                 | Protocole, port par défaut                  | Limites de la NAT                                                                                                             | Normes                                   | Commentaires                                                                                                                                                                                                                       |
|-----------------------------|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>H.323 H.225 et RAS</b>   | TCP/1720<br>UDP/1718 UDP<br>(RAS) 1718-1719 | (Mise en grappe) Pas de PAT statique.<br>Pas de PAT étendue.<br>Pas de NAT sur les mêmes interfaces de sécurité.<br>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.<br>No NAT64.                                                                                              | —                                        | —                                                                                                                                                                                                                                  |
| Messagerie instantanée (IM) | Varie selon le client                       | Pas de PAT étendue.<br>No NAT64.                                                                                              | RFC 3860                                 | —                                                                                                                                                                                                                                  |
| <b>Options d'adresse IP</b> | RSVP                                        | No NAT64.                                                                                                                     | RFC 791, RFC 2113                        | —                                                                                                                                                                                                                                  |
| Intercommunication IPsec    | UDP/500                                     | Pas de PAT<br>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).                                                                                                                                                                                         |
| MGCP                        | UDP/2427, 2727                              | Pas de PAT étendue.<br>No NAT64.<br>(Mise en grappe) Pas de PAT statique.                                                     | RFC 2705bis-05                           | —                                                                                                                                                                                                                                  |
| MMP                         | TCP/5443                                    | Pas de PAT étendue.<br>No NAT64.                                                                                              | —                                        | —                                                                                                                                                                                                                                  |

| Application                           | Protocole, port par défaut   | Limites de la NAT                                                                                                                                                                                            | Normes               | Commentaires                                                                                                                                                                                                             |
|---------------------------------------|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Serveur de noms NetBIOS</b> sur IP | UDP/133, 138 (ports sources) | Pas de PAT étendue.<br>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.<br>(Mise en grappe) Pas de PAT statique.                                                                                                                                                           | RFC 2637             | —                                                                                                                                                                                                                        |
| Gestion des comptes RADIUS            | UDP/1646                     | No NAT64.                                                                                                                                                                                                    | RFC 2865             | —                                                                                                                                                                                                                        |
| <b>RSH</b>                            | TCP/514                      | Pas de PAT<br>No NAT64.<br>(Mise en grappe) Pas de PAT statique.                                                                                                                                             | Berkeley UNIX        | —                                                                                                                                                                                                                        |
| <b>RTSP</b>                           | TCP/554                      | Pas de PAT étendue.<br>No NAT64.<br>(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).<br><br>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. |
| <b>SIP</b>                            | TCP/5060<br>UDP/5060         | Pas de NAT/PAT sur les interfaces avec des niveaux de sécurité identiques ou inférieurs ou supérieurs.<br><br>Pas de PAT étendue.<br><br>Pas de NAT64 ou NAT46.<br><br>(Mise en grappe) Pas de PAT statique. | RFC 2543             | Ne gère pas les configurations de téléphones IP Cisco téléchargées par TFTP dans certaines circonstances.                                                                                                                |

| Application          | Protocole, port par défaut                                                                                                     | Limites de la NAT                                                                                                                                 | Normes                           | Commentaires                                                                                                                                                                      |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SKINNY (SCCP)</b> | TCP/2000                                                                                                                       | Pas de NAT sur les mêmes interfaces de sécurité.<br>Pas de PAT étendue.<br>Pas de NAT64, NAT46 ou NAT66.<br>(Mise en grappe) Pas de PAT statique. | —                                | Ne gère pas les configurations de téléphones IP Cisco téléchargées par TFTP dans certaines circonstances.                                                                         |
| <b>SMTP et ESMTP</b> | TCP/25                                                                                                                         | No NAT64.                                                                                                                                         | RFC 821, 1123                    | —                                                                                                                                                                                 |
| <b>SNMP</b>          | UDP/161, 162<br>UDP/4161 sur les plateformes qui exécutent également Cisco 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.<br><br>Sur les plateformes FXOS, si vous configurez SNMP, cette inspection est activée automatiquement et vous ne pouvez pas la désactiver. |
| <b>SQL*Net</b>       | TCP/1521                                                                                                                       | Pas de PAT étendue.<br>No NAT64.<br>(Mise en grappe) Pas de PAT statique.                                                                         | —                                | v.1 et v.2.                                                                                                                                                                       |
| <b>STUN</b>          | TCP/3478<br>UDP/3478                                                                                                           | (WebRTC) NAT statique/PAT44 uniquement.<br><br>(Cisco Spark) NAT/PAT 44 et 64 statiques; et NAT/PAT dynamique.                                    | RFC 5245, 5389                   | —                                                                                                                                                                                 |
| <b>Sun RPC</b>       | TCP/111<br>UDP/111                                                                                                             | Pas de PAT étendue.<br>No NAT64.                                                                                                                  | —                                | —                                                                                                                                                                                 |
| <b>TFTP</b>          | UDP/69                                                                                                                         | No NAT64.<br>(Mise en grappe) Pas de PAT statique.                                                                                                | RFC 1350                         | Les adresses IP de charge utile ne sont pas traduites.                                                                                                                            |
| <b>WAAS</b>          | TCP/1- 65535                                                                                                                   | Pas de PAT étendue.<br>No NAT64.                                                                                                                  | —                                | —                                                                                                                                                                                 |
| <b>XDMCP</b>         | UDP/177                                                                                                                        | Pas de PAT étendue.<br>No NAT64.<br>(Mise en grappe) Pas de PAT statique.                                                                         | —                                | —                                                                                                                                                                                 |

| Application | Protocole, port par défaut | Limites de la NAT | Normes   | Commentaires                     |
|-------------|----------------------------|-------------------|----------|----------------------------------|
| 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**.

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 265](#) 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

Sauf si vous ajoutez une inspection à une carte de trafic existante, créez une carte de trafic L3/L4 pour identifier le trafic auquel vous souhaitez appliquer l'inspection.

```
class-map name
match parameter
```

#### Exemple :

```
hostname(config)# class-map dns_class_map
hostname(config-cmap)# match access-list dns
```

Dans la politique globale par défaut, la carte de trafic `inspection_default` est une carte de trafic spéciale qui comprend des ports par défaut pour tous les types d'inspection (**match default-inspection-traffic**). Vous pouvez appliquer plusieurs inspections uniquement à la carte de trafic `inspection_default`; il peut donc suffire



de modifier la politique globale existante qui applique les inspections par défaut. Si vous utilisez cette carte de trafic dans la politique par défaut ou pour une nouvelle politique de service, vous pouvez ignorer cette étape. Pour obtenir des renseignements détaillés sur le choix d'une carte de trafic, consultez [Choix de la bonne classe de trafic pour l'inspection, à la page 275](#).

Pour en savoir plus sur la mise en correspondance des instructions, consultez [Créer une carte de trafic de couche 3/4 pour le trafic de transit, à la page 251](#). Pour l'inspection de comptabilité RADIUS, qui utilise une carte de trafic de gestion de couche 3/4, consultez [Configurer l'inspection de comptabilité RADIUS, à la page 391](#).

**Étape 2** Ajoutez ou modifiez une liste des politiques de couche 3/4 qui définit les actions à appliquer au trafic de la carte de trafic : **policy-map** *name*

**Exemple :**

```
hostname(config)# policy-map global_policy
```

Dans la configuration par défaut, la liste des politiques `global_policy` est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste `global_policy`, saisissez `global_policy` comme nom de politique.

**Étape 3** Déterminez la carte de trafic L3/L4 que vous utilisez pour l'inspection : **class** *name*

**Exemple :**

```
hostname(config-pmap)# class inspection_default
```

Pour modifier la politique par défaut ou pour utiliser la carte de trafic spéciale `inspection_default` dans une nouvelle politique, spécifiez **inspection\_default** comme *nom*. Sinon, vous spécifiez la carte que vous avez créée précédemment au cours de cette procédure.

Vous pouvez combiner plusieurs cartes de trafic dans la même politique si vous le souhaitez, de sorte que vous pouvez créer une carte de trafic pour faire correspondre un certain trafic et une autre pour faire correspondre un trafic différent. Toutefois, si le trafic correspond à une carte de trafic qui contient une commande d'inspection, puis correspond à une autre carte de trafic qui comporte également une commande d'inspection, seule la première carte correspondante est utilisée. Par exemple, SNMP correspond à la carte de trafic `inspection_default`. Pour activer l'inspection SNMP, activez l'inspection SNMP pour la carte par défaut. N'ajoutez pas d'autre carte qui correspond à SNMP.

**Étape 4** Activez l'inspection des applications : **inspect** *protocol*

Le *protocole* est l'une des valeurs suivantes :

**Tableau 11 : Mots-clés du protocole d'inspection**

| Mots-clés                         | Notes                                                                                                                                                                                                                                                                                           |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ctiqbe</b>                     | Consultez <a href="#">Inspection CTIQBE, à la page 327</a> .                                                                                                                                                                                                                                    |
| <b>dcerpc</b> [ <i>map_name</i> ] | Consultez <a href="#">Inspection DCERPC, à la page 283</a> .<br><br>Si vous avez ajouté une liste des politiques d'inspection DCERPC conformément à <a href="#">Configurer une liste des politiques d'inspection DCERPC, à la page 284</a> , identifiez le nom de la liste dans cette commande. |

| Mots-clés                                                 | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>diameter</b> [map_name] [ <b>tls-proxy</b> proxy_name] | <p>Consultez <a href="#">Inspection Diameter, à la page 357</a>.</p> <p>Si vous avez ajouté une liste des politiques d'inspection Diameter conformément à <a href="#">Configurer une liste des politiques d'inspection Diameter, à la page 368</a>, identifiez le nom de la liste dans cette commande.</p> <p><b>tls-proxy</b> proxy_name identifie le serveur proxy TLS à utiliser pour cette inspection. Vous avez besoin d'un serveur proxy TLS uniquement si vous souhaitez activer l'inspection du trafic chiffré.</p>                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>dns</b> [map_name]<br>[dynamic-filter-snoop]           | <p>Consultez <a href="#">Inspection DNS, à la page 287</a>.</p> <p>Si vous avez ajouté une liste des politiques d'inspection DNS en fonction de <a href="#">Configurer la liste des politiques d'inspection DNS, à la page 287</a>, identifiez le nom de la liste dans cette commande. Le nom de la liste des politiques d'inspection DNS par défaut est « preset_dns_map ».</p> <p><b>dynamique-filtre-snoop</b> active la surveillance dynamique des filtres, utilisée exclusivement par le filtre de trafic de réseau de zombies. Incluez ce mot-clé uniquement si vous utilisez le filtrage du trafic de réseau de zombies. 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.</p> |
| <b>esmtplib</b> [map_name]                                | <p>Consultez <a href="#">Inspection SMTP et SMTP étendue, à la page 314</a>.</p> <p>Si vous avez ajouté une liste des politiques d'inspection ESMTPLIB conformément à <a href="#">Configurer une liste des politiques d'inspection ESMTPLIB, à la page 316</a>, identifiez le nom de la liste dans cette commande.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>ftplib</b> [strict [map_name]]                         | <p>Consultez <a href="#">Inspection FTP, à la page 292</a>.</p> <p>Utilisez le mot-clé <b>strict</b> pour renforcer la sécurité des réseaux protégés en empêchant les navigateurs Web d'envoyer des commandes intégrées dans les requêtes FTP. Consultez <a href="#">FTP strict, à la page 292</a> pour de plus amples renseignements.</p> <p>Si vous avez ajouté une liste des politiques d'inspection FTP conformément à <a href="#">Configurer une liste des politiques d'inspection FTP, à la page 293</a>, identifiez le nom de la liste dans cette commande.</p>                                                                                                                                                                                                                                                                                                                                                         |
| <b>gtp</b> [map_name]                                     | <p>Consultez <a href="#">Aperçu de l'inspection GTP, à la page 353</a>.</p> <p>Si vous avez ajouté une liste des politiques d'inspection GTP conformément à <a href="#">Configurer une liste des politiques d'inspection GTP, à la page 362</a>, identifiez le nom de la liste dans cette commande.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>h323 h225</b> [map_name]                               | <p>Consultez <a href="#">Inspection H.323, à la page 328</a>.</p> <p>Si vous avez ajouté une liste des politiques d'inspection H323 conformément à <a href="#">Configurer la liste des politiques d'inspection H.323, à la page 330</a>, identifiez le nom de la liste dans cette commande.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

| Mots-clés                                  | Notes                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>h323 ras</b> [ <i>map_name</i> ]        | Consultez <a href="#">Inspection H.323</a> , à la page 328.<br><br>Si vous avez ajouté une liste des politiques d'inspection H323 conformément à <a href="#">Configurer la liste des politiques d'inspection H.323</a> , à la page 330, identifiez le nom de la liste dans cette commande.                                                                |
| <b>http</b> [ <i>map_name</i> ]            | Consultez <a href="#">Inspection HTTP</a> , à la page 296.<br><br>Si vous avez ajouté une liste des politiques d'inspection HTTP conformément à <a href="#">Configurer une liste des politiques d'inspection HTTP</a> , à la page 297, identifiez le nom de la liste dans cette commande.                                                                 |
| <b>ICMP</b>                                | Consultez <a href="#">Inspection ICMP</a> , à la page 301.                                                                                                                                                                                                                                                                                                |
| <b>icmp error</b>                          | Consultez <a href="#">Inspection des erreurs ICMP</a> , à la page 301.                                                                                                                                                                                                                                                                                    |
| <b>ils</b>                                 | Consultez <a href="#">Inspection ILS</a> , à la page 302.                                                                                                                                                                                                                                                                                                 |
| <b>im</b> [ <i>map_name</i> ]              | Consultez <a href="#">Inspection de la messagerie instantanée</a> , à la page 303.<br><br>Si vous avez ajouté une liste des politiques d'inspection de messagerie instantanée, identifiez le nom de la liste dans cette commande.                                                                                                                         |
| <b>ip-options</b> [ <i>map_name</i> ]      | Consultez <a href="#">Inspection des options IP</a> , à la page 306.<br><br>Si vous avez ajouté une liste des politiques d'inspection des options IP conformément à <a href="#">Configurer une liste des politiques d'inspection des options IP</a> , à la page 307, identifiez le nom de la liste dans cette commande.                                   |
| <b>ipsec-pass-thru</b> [ <i>map_name</i> ] | Consultez <a href="#">Inspection IPsec Pass Through</a> , à la page 308.<br><br>Si vous avez ajouté une liste des politiques d'inspection de transmission directe IPsec conformément à <a href="#">Configurer une liste des politiques d'inspection de transmission directe IPsec</a> , à la page 309, identifiez le nom de la liste dans cette commande. |
| <b>ipv6</b> [ <i>map_name</i> ]            | Consultez <a href="#">Inspection IPv6</a> , à la page 310.<br><br>Si vous avez ajouté une liste des politiques d'inspection IPv6 conformément à <a href="#">Configurer une liste des politiques d'inspection IPv6</a> , à la page 310, identifiez le nom de la liste dans cette commande.                                                                 |
| <b>lisp</b> [ <i>map_name</i> ]            | 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.<br><br>Si vous avez ajouté une liste des politiques d'inspection LISP, identifiez le nom de la liste dans cette commande.                                                      |
| <b>m3ua</b> [ <i>map_name</i> ]            | Consultez <a href="#">Inspection M3UA</a> , à la page 358.<br><br>Si vous avez ajouté une liste des politiques d'inspection M3UA conformément à <a href="#">Configurer une liste des politiques d'inspection M3UA</a> , à la page 385, identifiez le nom de la liste dans cette commande.                                                                 |

| Mots-clés                                                             | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>mgcp</b> [ <i>map_name</i> ]                                       | Consultez <a href="#">Inspection MGCP</a> , à la page 333.<br><br>Si vous avez ajouté une liste des politiques d'inspection MGCP conformément à <a href="#">Configurer une liste des politiques d'inspection MGCP</a> , à la page 335, identifiez le nom de la liste dans cette commande.                                                                                                                                                                                                                      |
| <b>netbios</b> [ <i>map_name</i> ]                                    | Consultez <a href="#">Inspection NetBIOS</a> , à la page 312.<br><br>Si vous avez ajouté une liste des politiques d'inspection NetBIOS, identifiez le nom de la liste dans cette commande.                                                                                                                                                                                                                                                                                                                     |
| <b>pptp</b>                                                           | Consultez <a href="#">Inspection PPTP</a> , à la page 313.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>radius-accounting</b> <i>map_name</i>                              | Consultez <a href="#">Aperçu de l'inspection de comptabilité RADIUS</a> , à la page 360.<br><br>Le mot-clé <b>radius-accounting</b> est uniquement disponible pour une carte de trafic de gestion. Vous devez spécifier une liste des politiques d'inspection de comptabilité RADIUS; voir <a href="#">Configurer une liste des politiques d'inspection de comptabilité RADIUS</a> , à la page 391.                                                                                                            |
| <b>rsh</b>                                                            | Consultez <a href="#">Inspection RSH</a> , à la page 314.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>rtsp</b> [ <i>map_name</i> ]                                       | Consultez <a href="#">Inspection RTSP</a> , à la page 336.<br><br>Si vous avez ajouté une liste des politiques d'inspection RTSP conformément à <a href="#">Configurer une liste des politiques d'inspection RTSP</a> , à la page 337, identifiez le nom de la liste dans cette commande.                                                                                                                                                                                                                      |
| <b>sctp</b> [ <i>map_name</i> ]                                       | Consultez <a href="#">Inspection de la couche application SCTP</a> , à la page 356.<br><br>Si vous avez ajouté une liste des politiques d'inspection SCTP conformément à <a href="#">Configurer une liste des politiques d'inspection SCTP</a> , à la page 367, identifiez le nom de la liste dans cette commande.                                                                                                                                                                                             |
| <b>sip</b> [ <i>map_name</i> ] [ <b>tls-proxy</b> <i>proxy_name</i> ] | Consultez <a href="#">Inspection SIP</a> , à la page 340.<br><br>Si vous avez ajouté une liste des politiques d'inspection SIP conformément à <a href="#">Configurer une liste des politiques d'inspection SIP</a> , à la page 342, identifiez le nom de la liste dans cette commande.<br><br><b>tls-proxy</b> <i>proxy_name</i> identifie le serveur proxy TLS à utiliser pour cette inspection. Vous avez besoin d'un serveur proxy TLS uniquement si vous souhaitez activer l'inspection du trafic chiffré. |
| <b>Skinny</b> [ <i>map_name</i> ]                                     | Consultez <a href="#">Inspection Skinny (SCCP)</a> , à la page 346.<br><br>Si vous avez ajouté une liste des politiques d'inspection Skinny conformément à <a href="#">Configurer une liste des politiques d'inspection Skinny (SCCP)</a> , à la page 348, identifiez le nom de la liste dans cette commande.                                                                                                                                                                                                  |
| <b>snmp</b> [ <i>map_name</i> ]                                       | Consultez <a href="#">Inspection SNMP</a> , à la page 319.<br><br>Si vous avez ajouté une liste des politiques d'inspection SNMP, identifiez le nom de la liste dans cette commande.                                                                                                                                                                                                                                                                                                                           |
| <b>sqlnet</b>                                                         | Consultez <a href="#">Inspection SQL*Net</a> , à la page 320.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Mots-clés     | Notes                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>stun</b>   | Consultez <a href="#">Inspection STUN</a> , à la page 349.                                                                                                                                                                                                                                                                                                                       |
| <b>sunrpc</b> | Consultez <a href="#">Inspection Sun RPC</a> , à la page 320.<br><br>La carte de trafic par défaut comprend le port UDP 111; si vous souhaitez activer l'inspection Sun RPC 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 la commande <b>inspect sunrpc</b> à cette carte. |
| <b>tftp</b>   | Consultez <a href="#">Inspection TFTP</a> , à la page 322.                                                                                                                                                                                                                                                                                                                       |
| <b>WAAS</b>   | Active l'analyse TCP de l'option 33. À utiliser lors du déploiement des produits de services d'applications pour zone étendue.                                                                                                                                                                                                                                                   |
| <b>xdmcp</b>  | Consultez <a href="#">Inspection XDMCP</a> , à la page 322.                                                                                                                                                                                                                                                                                                                      |
| <b>vlan</b>   | Consultez <a href="#">Inspection VXLAN</a> , à la page 323.                                                                                                                                                                                                                                                                                                                      |

**Remarque**

Si vous modifiez la politique globale par défaut (ou toute politique en cours d'utilisation) afin d'utiliser une liste des politiques d'inspection différente, vous devez supprimer l'ancienne inspection avec la commande **no inspect protocol**, puis la rajouter avec le nouveau nom de la liste des politiques d'inspection.

**Exemple :**

```
hostname(config-class)# no inspect sip
hostname(config-class)# inspect sip sip-map
```

**Étape 5**

Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée `global_policy`), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

**service-policy** *polycymap\_name* {**global** | **interface** *interface\_name*}

**Exemple :**

```
hostname(config)# service-policy global_policy global
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

## Choix de la bonne classe de trafic pour l'inspection

La carte de trafic par défaut de la couche 3/4 pour le trafic de transit est appelée « `inspection_default` ». Elle fait correspondre le trafic à l'aide d'une commande **match** spéciale, **match default-inspection-traffic**, pour faire correspondre les protocoles et les ports par défaut pour chaque protocole d'application. Cette classe de

trafic (ainsi que **match any**, qui n'est généralement pas utilisé pour l'inspection) correspond au trafic IPv4 et IPv6 pour les inspections qui prennent en charge IPv6. Consultez [Lignes directrices relatives à l'inspection des applications, à la page 264](#) pour obtenir la liste des inspections activées pour IPv6.

Vous pouvez spécifier une commande **match access-list** avec la commande **match default-inspection-traffic** pour restreindre le trafic correspondant à des adresses IP spécifiques. Comme la commande **match default-inspection-traffic** spécifie les ports à mettre en correspondance, tous les ports dans l'ACL sont ignorés.



#### Astuces

Nous vous suggérons d'inspecter le trafic uniquement sur les ports sur lesquels vous attendez un trafic d'application; si vous inspectez tout le trafic, par exemple à l'aide de **match any**, les performances de l'ASA peuvent être affectées.

Si vous souhaitez faire correspondre des ports non standard, créez une nouvelle carte de trafic pour les ports non standard. Consultez [Inspections par défaut et limites de la NAT, à la page 265](#) pour connaître les ports standard de chaque moteur d'inspection. Vous pouvez combiner plusieurs cartes de trafic dans la même politique si vous le souhaitez, de sorte que vous pouvez créer une carte de trafic pour faire correspondre un certain trafic et une autre pour faire correspondre un trafic différent. Toutefois, si le trafic correspond à une carte de trafic qui contient une commande d'inspection, puis correspond à une autre carte de trafic qui comporte également une commande d'inspection, seule la première carte correspondante est utilisée. Par exemple, SNMP correspond à la carte `inspection_default`. Pour activer l'inspection SNMP, activez l'inspection SNMP pour la carte par défaut. N'ajoutez pas d'autre carte qui correspond à SNMP.

Par exemple, pour limiter l'inspection au trafic de 10.1.1.0 à 192.168.1.0 à l'aide de la carte de trafic par défaut, saisissez les commandes suivantes :

```
hostname(config)# access-list inspect extended permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
hostname(config)# class-map inspection_default
hostname(config-cmap)# match access-list inspect
```

Affichez l'ensemble de la carte de trafic en utilisant la commande suivante :

```
hostname(config-cmap)# show running-config class-map inspection_default
!
class-map inspection_default
 match default-inspection-traffic
 match access-list inspect
!
```

Pour inspecter le trafic FTP sur le port 21 ainsi que sur le port 1056 (port non standard), créez une liste de contrôle d'accès qui spécifie les ports et affectez-la à une nouvelle carte de trafic :

```
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 21
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 1056
hostname(config)# class-map new_inspection
hostname(config-cmap)# match access-list ftp_inspect
```

# 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

Utilisez **Ctrl+V** pour échapper tous les caractères spéciaux de l'interface de ligne de commande, comme un point d'interrogation (?) ou un onglet. Par exemple, tapez **d[Ctrl+V]?g** pour saisir **d?g** dans la configuration.

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

À des fins d'optimisation, l'ASA effectue la recherche sur l'URL désobfusquée. La désobfuscation remplace plusieurs barres obliques (/) consécutives par une seule. 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, <b>d.g</b> 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, <b>d(o a)g</b> correspond à dog et dag, mais <b>do ag</b> 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, <b>ab(xy){3}z</b> correspond à abxyxyz. |

| Caractères  | Description                          | Remarques                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | Alternance                           | Correspond à l'une ou l'autre des expressions qu'il sépare. Par exemple, <b>dog cat</b> 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, <b>lo?se</b> 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, <b>lo*se</b> correspond à lse, lose, loose, etc.                                                                                                                                                                                                                                                                   |
| +           | Plus                                 | Un quantificateur qui indique qu'il y a au moins 1 de l'expression précédente. Par exemple, <b>lo+se</b> correspond à lose et loose, mais pas à lse.                                                                                                                                                                                                                                                                              |
| {x} ou {x,} | Quantificateur de répétition minimal | Répétez au moins x fois. Par exemple, <b>ab(xy){2,}z</b> correspond à abxyxyz, abxyxyxyz, etc.                                                                                                                                                                                                                                                                                                                                    |
| [abc]       | Classe de caractères                 | Correspond à l'un des caractères entre crochets. Par exemple, <b>[abc]</b> 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, <b>[^abc]</b> correspond à tout caractère autre que a, b ou c. <b>[^A-Z]</b> 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. <b>[a-z]</b> correspond à n'importe quelle lettre minuscule. Vous pouvez combiner les caractères et les plages : <b>[abcq-z]</b> correspond à a, b, c, q, r, s, t, u, v, w, x, y, z, de même que <b>[a-cq-z]</b> .<br><br>Le caractère de tiret (-) est littéral uniquement s'il s'agit du dernier ou du premier caractère entre crochets : <b>[abc-]</b> ou <b>[-abc]</b> . |
| « »         | 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, <b>\[</b> correspond au crochet gauche.                                                                                                                                                                                                                                                                                             |
| char        | Caractères                           | Lorsque le caractère n'est pas un metacaractère, correspond au caractère littéral.                                                                                                                                                                                                                                                                                                                                                |
| \r          | Retour chariot                       | Correspond à un retour chariot 0x0d.                                                                                                                                                                                                                                                                                                                                                                                              |
| \n          | Nouvelle ligne                       | Correspond à une nouvelle ligne 0x0a.                                                                                                                                                                                                                                                                                                                                                                                             |



| Caractères | Description                | Remarques                                                                                                                    |
|------------|----------------------------|------------------------------------------------------------------------------------------------------------------------------|
| \t         | Onglet                     | Correspond à une tabulation 0x09.                                                                                            |
| \f         | Saut de page               | Correspond à un saut de page 0x0c.                                                                                           |
| \xNN       | 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

Testez une expression régulière pour vous assurer qu'elle correspond à ce que vous pensez qu'elle correspondra : **test regex** *input\_text regular\_expression*

Où l'argument *input\_text* est une chaîne que vous souhaitez mettre en correspondance à l'aide de l'expression régulière, jusqu'à 201 caractères de longueur. L'argument *regular\_expression* peut comporter jusqu'à 100 caractères.

Utilisez **Ctrl+V** pour échapper tous les caractères spéciaux de l'interface de ligne de commande. Par exemple, pour saisir un onglet dans le texte d'entrée de la commande **test regex**, vous devez saisir **test regex «test[Ctrl+V Tab]» «test\b»**.

Si l'expression régulière correspond au texte d'entrée, le message suivant s'affiche :

```
INFO: Regular expression match succeeded.
```

Si l'expression régulière ne correspond pas au texte d'entrée, le message suivant s'affiche :

```
INFO: Regular expression match failed.
```

### Étape 2

Pour ajouter une expression régulière après l'avoir testée, saisissez la commande suivante : **regex name** *regular\_expression*

Où l'argument *name* peut comporter jusqu'à 40 caractères de longueur. L'argument *regular\_expression* peut comporter jusqu'à 100 caractères.

## Exemples

L'exemple suivant crée deux expressions régulières à utiliser dans une liste des politiques d'inspection :

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
```

## 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** Créez la carte de trafic d'expressions régulières : **class-map type regex match-any** *class\_map\_name*
- Où *class\_map\_name* est une chaîne d'une longueur maximale de 40 caractères. Le nom « class-default » est réservé. Tous les types de cartes de trafic utilisent le même espace de nom, de sorte que vous ne pouvez pas réutiliser un nom déjà utilisé par un autre type de carte de trafic.
- Le mot-clé **match-any** spécifie que le trafic correspond à la carte de classes s'il correspond à au moins une des expressions régulières.
- Étape 2** (Facultatif) Ajoutez une description à la carte de trafic : **description** *string*
- Étape 3** Déterminez les expressions régulières que vous souhaitez inclure en entrant la commande suivante pour chaque expression régulière : **match regex** *regex\_name*
- 

### Exemples

L'exemple suivant crée deux expressions régulières et les ajoute à une carte de trafic d'expressions régulières. Le trafic correspond à la carte de trafic s'il comprend la chaîne « example.com » ou « example2.com ».

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex url_example
hostname(config-cmap)# match regex url_example2
```

## Surveillance des politiques d'inspection

Pour surveiller les politiques de service d'inspection, entrez les commandes suivantes. 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 ctique**

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 : <b>class-map type inspect</b> .                                                                                                                                          |
| 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 : <b>class-map type regex</b> , <b>regex</b> , <b>match regex</b> .            |
| match any pour les listes des politiques d'inspection | 8.0(2)   | Le mot-clé <b>match any</b> 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 <b>match all</b> 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 261.

- [Inspection DCERPC](#), à la page 283
- [Inspection DNS](#), à la page 287
- [Inspection FTP](#), à la page 292
- [Inspection HTTP](#), à la page 296
- [Inspection ICMP](#), à la page 301
- [Inspection des erreurs ICMP](#), à la page 301
- [Inspection ILS](#), à la page 302
- [Inspection de la messagerie instantanée](#), à la page 303
- [Inspection des options IP](#), à la page 306
- [Inspection IPsec Pass Through](#), à la page 308
- [Inspection IPv6](#), à la page 310
- [Inspection NetBIOS](#), à la page 312
- [Inspection PPTP](#), à la page 313
- [Inspection RSH](#), à la page 314
- [Inspection SMTP et SMTP étendue](#), à la page 314
- [Inspection SNMP](#), à la page 319
- [Inspection SQL\\*Net](#), à la page 320
- [Inspection Sun RPC](#), à la page 320
- [Inspection TFTP](#), à la page 322
- [Inspection XDMCP](#), à la page 322
- [Inspection VXLAN](#), à la page 323
- [Historique de l'inspection du protocole Internet de base](#), à la page 323

## 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.

### Procédure

---

**Étape 1** (Facultatif) Créez une carte de trafic d'inspection DCERPC.

Pour le trafic que vous identifiez dans cette carte de trafic, vous spécifiez les actions à prendre sur le trafic dans la liste des politiques d'inspection.

Si vous souhaitez effectuer différentes actions pour chaque commande **match**, vous devez identifier le trafic directement dans la liste des politiques.

- a) Créez la carte de trafic : **class-map type inspect dcerpc [match-all | match-any] class\_map\_name**

Où *class\_map\_name* est le nom de la carte de trafic. Le mot-clé **match-all** est le mot-clé par défaut. Il spécifie que le trafic doit correspondre à tous les critères pour correspondre à la carte de trafic. Le mot-clé **match-any** spécifie que le trafic correspond à la carte de trafic s'il correspond à au moins un énoncé **match**. L'interface de ligne de commande passe en mode de configuration class-map.

- b) Précisez le trafic sur lequel vous souhaitez effectuer des actions à l'aide de la commande **match** suivante. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

- **matchuuid type[not]** : correspond à l'identifiant unique universel (UUID) du message DCERPC. Le *type* peut être l'un des suivants :
  - **ms-rpc-epm**: correspond aux messages EPM Microsoft RPC.
  - **ms-rpc-isystemactivator**: correspond aux messages ISystemMapper.
  - **ms-rpc-oxidresolver**: correspond aux messages OxidResolver.

- c) Saisissez **exit** pour quitter le mode de configuration de carte de trafic.

## Étape 2

Créer une liste des politiques d'inspection DCERPC : **policy-map type inspect dcerpc policy\_map\_name**

Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.

## Étape 3

(Facultatif) Ajoutez une description à la liste des politiques : **description chaîne**

## Étape 4

Pour appliquer les actions au trafic correspondant, procédez comme suit.

- a) Précisez le trafic sur lequel vous souhaitez effectuer des actions en utilisant l'une des méthodes suivantes :
- Si vous avez créé une carte de trafic DCERPC, spécifiez-la en entrant la commande suivante : **class class\_map\_name**
  - Précisez le trafic directement dans la liste des politiques à l'aide de l'une des commandes **match** décrites pour les cartes de trafic DCERPC. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.
- b) Précisez l'action que vous souhaitez effectuer sur le trafic correspondant en saisissant l'une des commandes suivantes :
- **reset [log]** : abandonne le paquet, ferme la connexion et envoie une réinitialisation TCP au serveur ou au client.
  - **log** : envoie un message de journal système. Vous pouvez utiliser cette option seule ou avec l'une des autres actions.

Vous pouvez spécifier plusieurs commandes **class** ou **match** dans la carte de politiques.

**Exemple :**

```
hostname(config)# policy-map type inspect dcerpc dcerpc-map
hostname(config-pmap)# match uuid ms-rpc-epm
hostname(config-pmap-c)# log
```

**Étape 5** Pour configurer les paramètres qui influent sur le moteur d'inspection, procédez comme suit :

a) Entrez en mode de configuration des paramètres :

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option :

- **timeout pinhole** *hh:mm:ss* : configure le délai d'expiration pour les passages DCERPC et remplace le délai d'expiration du point d'épingle du système global de deux minutes. Le délai d'expiration peut être compris entre 00:00:01 et 119:00:00.
- **endpoint-mapper** [**epm-service-only**] [**lookup-operation** [**timeout** *hh:mm:ss*]] : configure les options pour le trafic du mappeur de point de terminaison. Le mot-clé **epm-service-only** applique le service de mappage de point de terminaison lors de la liaison afin que seul le trafic de service soit traité. Le mot-clé **lookup-operation** active l'opération de recherche du service de mappage de point de terminaison. Vous pouvez configurer le délai d'expiration des passages générés par l'opération de recherche. Si aucun délai d'expiration n'est configuré pour l'opération de recherche, la commande **timeout pinhole** ou la valeur par défaut est utilisée.

## Exemples

L'exemple suivant montre comment définir une liste des politiques d'inspection DCERPC avec le délai d'expiration configuré pour les passages DCERPC.

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# timeout pinhole 0:10:00

hostname(config)# class-map dcerpc
hostname(config-cmap)# match port tcp eq 135

hostname(config)# policy-map global-policy
hostname(config-pmap)# class dcerpc
hostname(config-pmap-c)# inspect dcerpc dcerpc-map

hostname(config)# service-policy global-policy global
```

## 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 270](#).



# 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.

Consultez les commandes d'inspection DNS par défaut suivantes :

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 message-length maximum 512
 dns-guard
 protocol-enforcement
 nat-rewrite
policy-map global_policy
 class inspection_default
 inspect dns preset_dns_map
! ...
service-policy global_policy global
```

## 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 ne convient pas à votre réseau.

### 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** (Facultatif) Créez une carte de trafic d'inspection DNS en procédant comme suit.

Une carte de trafic regroupe plusieurs correspondances de trafic. Vous pouvez également identifier les commandes **match** directement dans la liste des politiques. La différence entre la création d'une carte de classe et la définition de la correspondance de trafic directement dans la liste des politiques d'inspection est que la carte de classe vous permet de créer des critères de correspondance plus complexes, et vous pouvez réutiliser les cartes de classe.

Pour spécifier le trafic qui ne doit pas correspondre à la carte de trafic, utilisez la commande **match not**. Par exemple, si la commande **match not** spécifie la chaîne « example.com », tout trafic qui inclut « example.com » ne correspond pas à la carte de classes.

Pour le trafic que vous identifiez dans cette carte de trafic, vous spécifiez les actions à prendre sur le trafic dans la liste des politiques d'inspection.

Si vous souhaitez effectuer différentes actions pour chaque commande **match**, vous devez identifier le trafic directement dans la liste des politiques.

a) Créez la carte de trafic : **class-map type inspect dns [match-all | match-any] class\_map\_name**

Où *class\_map\_name* est le nom de la carte de trafic. Le mot-clé **match-all** est le mot-clé par défaut. Il spécifie que le trafic doit correspondre à tous les critères pour correspondre à la carte de trafic. Le mot-clé **match-any** spécifie que le trafic correspond à la carte de trafic s'il correspond à au moins un énoncé **match**. L'interface de ligne de commande passe en mode de configuration class-map, où vous pouvez saisir une ou plusieurs commandes **match**.

b) (Facultatif) : Ajoutez une description à la carte de trafic : **description string**

Où *string* est la description de la carte de trafic (jusqu'à 200 caractères).

c) Précisez le trafic pour lequel vous souhaitez effectuer des actions à l'aide de l'une des commandes **match** suivantes. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

- **match [not] header-flag [eq] {f\_name [f\_name...] | f\_value}** : correspond à l'indicateur DNS. L'argument *f\_name* est le nom d'indicateur DNS, l'un des suivants : **AA** (réponse faisant autorité), **QR** (requête), **RA** (récursivité disponible), **RD** (récursivité souhaitée), **TC** (truncation). L'argument *f\_value* est la valeur 16 bits en hexadécimal commençant par 0x, de 0x0 à 0xffff. Le mot-clé **eq** spécifie une correspondance exacte (match all) ; sans le mot-clé **eq**, le paquet n'a besoin de correspondre qu'à l'un des en-têtes spécifiés (match any). Par exemple, **match header-flag AA QR**.
- **match [not] dns-type {eq {t\_name | t\_value} | range t\_value1 t\_value2}** : correspond au type DNS. L'argument *t\_name* est le nom de type DNS, l'un des suivants : **A** (adresse IPv4), **AXFR** (transfert de zone complet), **CNAME** (nom canonique), **IXFR** (transfert de zone incrémentiel), **NS** (serveur de noms faisant autorité), **SOA** (début d'une zone d'autorité) ou **TSIG** (signature de transaction). Les arguments *t\_value* sont des valeurs quelconques dans le champ de type DNS (0 à 65 535). Le mot-clé **range** spécifie une plage et le mot-clé **eq** spécifie une correspondance exacte. Par exemple : **match dns-type eq A**.
- **match [not] dns-class {eq {in | c\_value} | range c\_value1 c\_value2}** : correspond à la classe DNS. La carte est soit **in** (pour Internet) ou *c\_value*, une valeur quelconque de 0 à 65 535 dans le champ

de carte DNS. Le mot-clé **range** spécifie une plage et le mot-clé **eq** spécifie une correspondance exacte. Par exemple : **match dns-class eq in**.

- **match [not] {question | resource-record {answer | authority | additional}}** : correspond à une question DNS ou à un enregistrement de ressource. Le mot-clé **question** spécifie la partie question d'un message DNS. Le mot-clé **resource-record** spécifie l'une de ces sections de l'enregistrement de ressource : **answer**, **authority**, ou **additional**. Par exemple : **match resource-record answer**.
- **match [not] domain-name regex {regex\_name | class class\_name}** : correspond à la liste de noms de domaine du message DNS avec l'expression régulière ou la liste d'expressions régulières spécifiée.

d) Saisissez **exit** pour quitter le mode de configuration **class-map**.

## Étape 2

Créer une liste des politiques d'inspection DNS : **policy-map type inspect dns policy\_map\_name**

Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration **policy-map**.

## Étape 3

(Facultatif) Ajoutez une description à la liste des politiques : **description string**

## Étape 4

Pour appliquer les actions au trafic correspondant, procédez comme suit.

- Précisez le trafic sur lequel vous souhaitez effectuer des actions en utilisant l'une des méthodes suivantes :
  - Si vous avez créé une carte de trafic DNS, spécifiez-la en entrant la commande suivante : **class class\_map\_name**
  - Précisez le trafic directement dans la liste des politiques à l'aide de l'une des commandes **match** décrites pour les cartes de trafic DNS. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.
- Précisez l'action que vous souhaitez effectuer sur le trafic correspondant en saisissant l'une des commandes suivantes :
  - **drop [log]** : abandonne tous les paquets qui correspondent.
  - **drop-connection [log]** : abandonne le paquet et ferme la connexion.
  - **mask [log]** : masque la partie correspondante du paquet. Cette action est disponible uniquement pour les correspondances d'indicateurs d'en-tête.
  - **log** : envoie un message de journal système. Vous pouvez utiliser cette option seule ou avec l'une des autres actions.
  - **enforce-tsig [drop] [log]** : applique la présence de l'enregistrement de ressource TSIG dans un message. Vous pouvez abandonner un paquet sans l'enregistrement de ressource TSIG, le journaliser, ou l'abandonner et le journaliser. Vous pouvez utiliser cette option en conjonction avec l'action de masque pour les correspondances d'indicateurs d'en-tête ; dans le cas contraire, cette action est exclusive avec les autres actions.

Vous pouvez spécifier plusieurs commandes **class** ou **match** dans la liste des politiques. Pour en savoir plus sur l'ordre des commandes **class** et **match**, consultez [Comment plusieurs classes de trafic sont gérées, à la page 262](#).

### Exemple :

```
hostname(config)# policy-map type inspect dns dns-map
hostname(config-pmap)# class dns-class-map
```

```
hostname(config-pmap-c) # drop
hostname(config-pmap-c) # match header-flag eq aa
hostname(config-pmap-c) # drop log
```

**Étape 5** Pour configurer les paramètres qui influent sur le moteur d'inspection, procédez comme suit :

a) Entrez dans le mode de configuration des paramètres.

```
hostname(config-pmap) # parameters
hostname(config-pmap-p) #
```

b) Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option.

- **dnsencrypt** : 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.
- **dns-guard** : active 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.
- **id-mismatch count number duration seconds action log** : active la journalisation pour les non-concordances d'ID DNS excessives, où les arguments **count number duration seconds** spécifient le nombre maximal d'instances de non-concordance par seconde avant l'envoi d'un journal de messages système.
- **id-randomization** : randomise l'identifiant DNS pour une requête DNS.
- **message-length maximum {length | client {length | auto} | server {length | auto}}** : définit la longueur maximale du message DNS, de 512 à 65 535 octets. Vous pouvez également définir la longueur maximale des messages client ou serveur. Le mot-clé **auto** définit la longueur maximale selon la valeur indiquée dans l'enregistrement de ressource.
- **nat-rewrite** : traduit l'enregistrement DNS en fonction de la configuration NAT.
- **protocol-enforcement** : active la vérification du format du message DNS, y compris la longueur du nom de domaine de 255 caractères maximum, la longueur d'étiquette de 63 caractères, la compression et la vérification des pointeurs en boucle.
- **tcp-inspection** : 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.
- **tsig enforced action [{drop} [log]}** : nécessite la présence d'un enregistrement de ressource TSIG. Vous pouvez **abandonner** un paquet non conforme, **journaliser** le paquet ou les deux.
- **umbrella [tag Umbrella\_policy] [fail-open]** : active Cisco Umbrella et spécifie éventuellement le nom de la politique Cisco Umbrella (**tag**) à appliquer au périphérique. Si vous ne spécifiez pas de politique, la politique par défaut est appliquée. Pour en savoir plus, consultez [Cisco Umbrella, à la page 103](#).

Incluez le mot-clé **fail-open** si vous souhaitez que la résolution DNS fonctionne si le serveur DNS Cisco Umbrella n'est pas disponible. En cas d'échec en mode ouvert, si le serveur DNS Cisco Umbrella n'est pas disponible, 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 Umbrella sont de nouveau disponibles, la liste des politiques reprend leur utilisation. Si vous n'incluez pas cette option, les requêtes DNS continuent d'être acheminées au résolveur Cisco Umbrella inaccessible, de sorte qu'elles ne recevront pas de réponse.

### Exemple :

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)# dns-guard
hostname(config-pmap-p)# message-length maximum 1024
hostname(config-pmap-p)# nat-rewrite
hostname(config-pmap-p)# protocol-enforcement
```

### Exemple

L'exemple suivant montre comment utiliser une nouvelle carte de politiques d'inspection dans la configuration globale par défaut :

```
regex domain_example "example\.com"
regex domain_foo "foo\.com"

! define the domain names that the server serves
class-map type inspect regex match-any my_domains
 match regex domain_example
 match regex domain_foo

! Define a DNS map for query only
class-map type inspect dns match-all pub_server_map
 match not header-flag QR
 match question
 match not domain-name regex class my_domains

policy-map type inspect dns new_dns_map
 class pub_server_map
 drop log
 match header-flag RD
 mask log
 parameters
 message-length maximum client auto
 message-length maximum 512
 dns-guard
 protocol-enforcement
 nat-rewrite

policy-map global_policy
 class inspection_default
 no inspect dns preset_dns_map
 inspect dns new_dns_map
 service-policy global_policy global
```

### 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 270.

## 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 le protocole FTP strict, incluez l'option stricte avec la commande **inspect ftp**.

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 carte de politique d'inspection FTP. Vous pouvez ensuite appliquer la liste lorsque vous activez l'inspection FTP.

### 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** (Facultatif) Créez une carte de trafic d'inspection FTP en procédant comme suit.

Une carte de trafic regroupe plusieurs correspondances de trafic. Vous pouvez également identifier les commandes **match** directement dans la liste des politiques. La différence entre la création d'une carte de classe et la définition de la correspondance de trafic directement dans la liste des politiques d'inspection est que la carte de classe vous permet de créer des critères de correspondance plus complexes, et vous pouvez réutiliser les cartes de classe.

Pour spécifier le trafic qui ne doit pas correspondre à la carte de trafic, utilisez la commande **match not**. Par exemple, si la commande **match not** spécifie la chaîne « example.com », tout trafic qui inclut « example.com » ne correspond pas à la carte de classes.

Pour le trafic que vous identifiez dans cette carte de trafic, vous spécifiez les actions à prendre sur le trafic dans la liste des politiques d'inspection.

Si vous souhaitez effectuer différentes actions pour chaque commande **match**, vous devez identifier le trafic directement dans la liste des politiques.

a) Créez la carte de trafic : **class-map type inspect ftp [match-all | match-any] class\_map\_name**

Où *class\_map\_name* est le nom de la carte de trafic. Le mot-clé **match-all** est le mot-clé par défaut. Il spécifie que le trafic doit correspondre à tous les critères pour correspondre à la carte de trafic. Le mot-clé **match-any** spécifie que le trafic correspond à la carte de trafic s'il correspond à au moins un énoncé **match**. L'interface de ligne de commande passe en mode de configuration class-map, où vous pouvez saisir une ou plusieurs commandes **match**.

b) (Facultatif) : Ajoutez une description à la carte de trafic : **description string**

Où *string* est la description de la carte de trafic (jusqu'à 200 caractères).

c) Précisez le trafic pour lequel vous souhaitez effectuer des actions à l'aide de l'une des commandes **match** suivantes. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

- **match [not] filename regex {regex\_name | class class\_name}** : correspond au nom de fichier dans le transfert FTP avec l'expression régulière ou la liste d'expressions régulières spécifiée.
- **match [not] filetype regex {regex\_name | class class\_name}** : correspond au type de fichier dans le transfert FTP par rapport à l'expression régulière ou à la liste d'expressions régulières spécifiée.
- **match [not] request-command ftp\_command [ ftp\_command...]** correspond à la commande FTP, à l'une ou à plusieurs des commandes suivantes :
  - **APPE** : ajouter à un fichier.



- **CDUP** : passe au répertoire parent du répertoire de travail actuel.
- **DELE** : pour supprimer 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.
- **match [not] server regex** {*regex\_name* | **class** *class\_name*} : correspond au nom du serveur FTP avec l'expression régulière ou la liste d'expressions régulières spécifiée.
- **correspondance [not] nom d'utilisateur regex** {*regex\_name* | **class** *class\_name*} : correspond au nom d'utilisateur FTP avec l'expression régulière ou la classe d'expression régulière spécifiée.

d) Saisissez **exit** pour quitter le mode de configuration class-map.

**Étape 2** Créez une liste des politiques d'inspection FTP : **policy-map type inspect ftp** *policy\_map\_name*

Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration de liste des politiques.

**Étape 3** (Facultatif) Ajoutez une description à la liste des politiques : **description** *string*

**Étape 4** Pour appliquer les actions au trafic correspondant, procédez comme suit.

- a) Précisez le trafic sur lequel vous souhaitez effectuer des actions en utilisant l'une des méthodes suivantes :
- Si vous avez créé une carte de trafic FTP, spécifiez-la en entrant la commande suivante : **class** *class\_map\_name*
  - Précisez le trafic directement dans la liste des politiques à l'aide de l'une des commandes **match** décrites pour les cartes de trafic FTP. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.
- b) Précisez l'action que vous souhaitez effectuer sur le trafic correspondant en entrant la commande suivante :
- **reset [log]** : abandon du paquet, fermeture de la connexion et envoi d'une réinitialisation TCP au serveur ou au client. Ajoutez le mot-clé **log** pour envoyer un message de journal système.

Vous pouvez spécifier plusieurs commandes **class** ou **match** dans la liste des politiques. Pour en savoir plus sur l'ordre des commandes **class** et **match**, consultez [Comment plusieurs classes de trafic sont gérées, à la page 262](#).

**Étape 5** Pour configurer les paramètres qui influent sur le moteur d'inspection, procédez comme suit :

- a) Entrez dans le mode de configuration des paramètres.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

- b) Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option :

- **mask-banner** : masque la bannière de message d'accueil à partir du serveur FTP.
- **masque-syst-reply** : masque la réponse à la commande **syst**.

---

### Exemple

Avant de soumettre un nom d'utilisateur et un mot de passe, tous les utilisateurs FTP reçoivent une bannière de message d'accueil. Par défaut, cette bannière comprend des informations de version utiles aux pirates qui tentent d'identifier les faiblesses d'un système. L'exemple suivant montre comment masquer cette bannière :

```
hostname(config)# policy-map type inspect ftp mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner

hostname(config)# class-map match-all ftp-traffic
hostname(config-cmap)# match port tcp eq ftp

hostname(config)# policy-map ftp-policy
hostname(config-pmap)# class ftp-traffic
hostname(config-pmap-c)# inspect ftp strict mymap

hostname(config)# service-policy ftp-policy interface inside
```

### 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 270.

## 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 tunnellation 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 tunnellenées 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.

### 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 classe d'expression régulière.

### Procédure

#### Étape 1

(Facultatif) Créez une carte de trafic d'inspection HTTP en procédant comme suit.

Une carte de trafic regroupe plusieurs correspondances de trafic. Vous pouvez également identifier les commandes **match** directement dans la liste des politiques. La différence entre la création d'une carte de classe et la définition de la correspondance de trafic directement dans la liste des politiques d'inspection est que la carte de classe vous permet de créer des critères de correspondance plus complexes, et vous pouvez réutiliser les cartes de classe.

Pour spécifier le trafic qui ne doit pas correspondre à la carte de classe, utilisez la commande **match not**. Par exemple, si la commande **match not** spécifie la chaîne « example.com », tout trafic qui inclut « example.com » ne correspond pas à la carte de trafic.

Pour le trafic que vous identifiez dans cette carte de trafic, vous spécifiez les actions à prendre sur le trafic dans la liste des politiques d'inspection.

Si vous souhaitez effectuer différentes actions pour chaque commande **match**, vous devez identifier le trafic directement dans la liste des politiques.

- a) Créez la carte de trafic : **class-map type inspect http [match-all | match-any] class\_map\_name**

Où *class\_map\_name* est le nom de la carte de trafic. Le mot-clé **match-all** est le mot-clé par défaut. Il spécifie que le trafic doit correspondre à tous les critères pour correspondre à la carte de trafic. Le mot-clé **match-any** spécifie que le trafic correspond à la carte de trafic s'il correspond à au moins un énoncé **match**. L'interface de ligne de commande passe en mode de configuration class-map, où vous pouvez saisir une ou plusieurs commandes **match**.

- b) (Facultatif) : Ajoutez une description à la carte de trafic : **description string**

Où *string* est la description de la carte de trafic (jusqu'à 200 caractères).

- c) Précisez le trafic pour lequel vous souhaitez effectuer des actions à l'aide de l'une des commandes **match** suivantes. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

- **match [not] req-resp content-type mismatch** : correspond au trafic avec un champ content-type dans la réponse HTTP qui ne correspond pas au champ accept dans le message de demande HTTP correspondant.
- **match [not] request args regex {regex\_name | class class\_name}** : correspond au texte trouvé dans les arguments du message de demande HTTP par rapport à l'expression régulière ou à la liste d'expressions régulières spécifiée.
- **match [not] request body {regex {regex\_name | class class\_name} | length gt bytes}** : correspond au texte trouvé dans le corps du message de demande HTTP avec l'expression régulière ou la liste d'expressions régulières spécifiée, ou aux messages dans lesquels le corps de demande est supérieur à la longueur spécifiée.
- **match [not] request header {field | regex regex\_name} regex {regex\_name | class class\_name}** : correspond au contenu d'un champ dans l'en-tête du message de demande HTTP avec l'expression régulière ou la liste d'expressions régulières spécifiée. Vous pouvez spécifier le nom du champ explicitement ou faire correspondre le nom du champ à une expression régulière. Les noms des champs sont : 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.
- **match [not] request header {field | regex {regex\_name | class class\_name}} {length gt bytes | count gt number}** : correspond à la longueur des champs spécifiés dans l'en-tête du message de demande HTTP, ou au nombre total de champs (count) dans l'en-tête. Vous pouvez spécifier le nom du champ explicitement ou faire correspondre le nom de champ à une expression régulière ou à une liste d'expressions régulières. Les noms de champs sont répertoriés dans la puce précédente.
- **match [not] request header {length gt bytes | count gt number | non-ascii}** : correspond à la longueur totale de l'en-tête du message de demande HTTP, ou au nombre total de champs (count) dans l'en-tête, ou aux en-têtes qui ont des caractères non ASCII.
- **match [not] request method {method | regex {regex\_name | class class\_name}}** : correspond à la méthode de demande HTTP. Vous pouvez spécifier la méthode explicitement ou la faire correspondre

à une expression régulière ou à une liste d'expressions régulières. Les méthodes sont : 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.

- **match [not] request uri** {**regex** {*regex\_name* | **class** *class\_name*} | **length gt bytes**} : correspond au texte trouvé dans l'URI du message de demande HTTP avec l'expression régulière ou la liste d'expressions régulières spécifiée, ou aux messages dans lesquels l'URI de demande est supérieur à la longueur spécifiée.
- **match [not] response body** {**active-x** | **java-applet** | **regex** {*regex\_name* | **class** *class\_name*} } : correspond au texte trouvé dans le corps du message de réponse HTTP par rapport à l'expression régulière ou à la liste d'expressions régulières spécifiée, ou commente les balises d'applet Java et d'objet ActiveX afin de les filtrer.
- **match [not] response body length gt bytes** : correspond aux messages de réponse HTTP dans lesquels le corps est supérieur à la longueur spécifiée.
- **match [not] response header** {*field* | **regex** *regex\_name*} **regex** {*regex\_name* | **class** *class\_name*} : correspond au contenu d'un champ dans l'en-tête du message de réponse HTTP avec l'expression régulière ou la liste d'expressions régulières spécifiée. Vous pouvez spécifier le nom du champ explicitement ou faire correspondre le nom du champ à une expression régulière. Les noms des champs 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.
- **match [not] response header** {*field* | **regex** {*regex\_name* | **class** *class\_name*} } {**length gt bytes** | **count gt number**} : correspond à la longueur des champs spécifiés dans l'en-tête du message de réponse HTTP ou au nombre total de champs (count) dans l'en-tête. Vous pouvez spécifier le nom du champ explicitement ou faire correspondre le nom de champ à une expression régulière ou à une liste d'expressions régulières. Les noms de champs sont répertoriés dans la puce précédente.
- **match [not] response header** {**length gt bytes** | **count gt number** | **non-ascii**} : correspond à la longueur totale de l'en-tête du message de réponse HTTP, ou au nombre total de champs (count) dans l'en-tête, ou aux en-têtes qui ont des caractères non ASCII.
- **match [not] response status-line regex** {*regex\_name* | **class** *class\_name*} : correspond au texte trouvé dans la ligne d'état du message de réponse HTTP par rapport à l'expression régulière ou à la classe d'expressions régulières spécifiée.

d) Saisissez **exit** pour quitter le mode de configuration de carte de trafic.

## Étape 2

Créez une liste des politiques d'inspection HTTP : **policy-map type inspect http** *policy\_map\_name*

Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.

## Étape 3

(Facultatif) Ajoutez une description à la liste des politiques : **description** *chaîne*

## Étape 4

Pour appliquer les actions au trafic correspondant, procédez comme suit.

- Précisez le trafic sur lequel vous souhaitez effectuer des actions en utilisant l'une des méthodes suivantes :
  - Si vous avez créé une carte de trafic HTTP, spécifiez-la en entrant la commande suivante : **class** *class\_map\_name*

- Précisez le trafic directement dans la liste des politiques à l'aide de l'une des commandes **match** décrites pour les cartes de trafic HTTP. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.
- b) Précisez l'action que vous souhaitez effectuer sur le trafic correspondant en saisissant l'une des commandes suivantes :
- **drop-connection [log]** : abandonner le paquet et fermer la connexion.
  - **reset [log]** : abandonne le paquet, ferme la connexion et envoie une réinitialisation TCP au serveur ou au client.
  - **log** : envoie un message de journal système. Vous pouvez utiliser cette option seule ou avec l'une des autres actions.

Vous pouvez spécifier plusieurs commandes **class** ou **match** dans la carte de politiques. Pour en savoir plus sur l'ordre des commandes **class** et **match**, consultez [Comment plusieurs classes de trafic sont gérées, à la page 262](#).

## Étape 5

Pour configurer les paramètres qui influent sur le moteur d'inspection, procédez comme suit :

- a) Entrez en mode de configuration des paramètres :

```
hostname(config-pmap) # parameters
hostname(config-pmap-p) #
```

- b) Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option :
- **body-match-maximum number** : définit le nombre maximal de caractères dans le corps d'un message HTTP qui doivent être recherchés dans une correspondance de corps. Par défaut, c'est de 200 octets. Un grand nombre aura un impact considérable sur les performances.
  - **protocol-violation action {drop-connection [log] | reset [log] | log}** : vérifie les violations du protocole HTTP. Vous devez également choisir l'action à prendre en cas de violations (abandon de la connexion, réinitialisation ou journalisation) et activer ou désactiver la journalisation.
  - **spoof-server string** : remplace le champ d'en-tête Server par une chaîne. Les flux WebVPN ne sont pas soumis à la commande spoof-server.

## Exemple

L'exemple suivant montre comment définir une liste des politiques d'inspection HTTP qui autorisera et journalisera toute connexion HTTP qui tente d'accéder à « www.xyz.com/\*.asp » ou « www.xyz[0-9][0-9].com » avec les méthodes « GET » ou « PUT ». Toutes les autres combinaisons d'URL/méthode seront autorisées silencieusement.

```
hostname(config)# regex url1 "www\.xyz\.com/\.*\\.asp"
hostname(config)# regex url2 "www\.xyz[0-9][0-9]\.com"
hostname(config)# regex get "GET"
hostname(config)# regex put "PUT"
```

```
hostname(config)# class-map type regex match-any url_to_log
hostname(config-cmap)# match regex url1
hostname(config-cmap)# match regex url2
hostname(config-cmap)# exit

hostname(config)# class-map type regex match-any methods_to_log
hostname(config-cmap)# match regex get
hostname(config-cmap)# match regex put
hostname(config-cmap)# exit

hostname(config)# class-map type inspect http http_url_policy
hostname(config-cmap)# match request uri regex class url_to_log
hostname(config-cmap)# match request method regex class methods_to_log
hostname(config-cmap)# exit

hostname(config)# policy-map type inspect http http_policy
hostname(config-pmap)# class http_url_policy
hostname(config-pmap-c)# log
```

### 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 270.

## 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 270.

## 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 270.

## 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 270.

# 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 carte de politique 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.

## 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

(Facultatif) Créez une carte de trafic d'inspection IM en procédant comme suit.

Une carte de trafic regroupe plusieurs correspondances de trafic. Vous pouvez également identifier les commandes **match** directement dans la liste des politiques. La différence entre la création d'une carte de classe et la définition de la correspondance de trafic directement dans la liste des politiques d'inspection est que la carte de classe vous permet de créer des critères de correspondance plus complexes, et vous pouvez réutiliser les cartes de classe.

Pour spécifier le trafic qui ne doit pas correspondre à la carte de trafic, utilisez la commande **match not**. Par exemple, si la commande **match not** spécifie la chaîne « example.com », tout trafic qui inclut « example.com » ne correspond pas à la carte de trafic.

Pour le trafic que vous identifiez dans cette carte de trafic, vous spécifiez les actions à prendre sur le trafic dans la liste des politiques d'inspection.

Si vous souhaitez effectuer différentes actions pour chaque commande **match**, vous devez identifier le trafic directement dans la liste des politiques.

a) Créez la carte de trafic : **class-map type inspect im [match-all | match-any] class\_map\_name**

Où *nclass\_map\_name* est le nom de la carte de trafic. Le mot-clé **match-all** est le mot-clé par défaut. Il spécifie que le trafic doit correspondre à tous les critères pour correspondre à la carte de trafic. Le mot-clé **match-any** spécifie que le trafic correspond à la carte de trafic s'il correspond à au moins un énoncé **match**. L'interface de ligne de commande passe en mode de configuration class-map, où vous pouvez saisir une ou plusieurs commandes **match**.

- b) (Facultatif) : Ajoutez une description à la carte de trafic : **description string**  
Où *string* est la description de la carte de trafic (jusqu'à 200 caractères).
- c) Précisez le trafic pour lequel vous souhaitez effectuer des actions à l'aide de l'une des commandes **match** suivantes. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.
- **match [not] protocol {im-yahoo | im-msn}** : correspond à un protocole IM spécifique, Yahoo ou MSN.
  - **match [not] service {chat | file-transfer | webcam | voice-chat | conference | games}** : correspond au service d'IM spécifique.
  - **match [not] login-name regex {regex\_name | class class\_name}** : correspond au nom de connexion du client source du message IM en fonction de l'expression régulière ou de la liste d'expressions régulières spécifiée.
  - **match [not] peer-login-name regex {regex\_name | class class\_name}** : correspond au nom de connexion de l'homologue de destination du message IM en fonction de l'expression régulière ou de la liste d'expressions régulières spécifiée.
  - **match [not] ip-address ip\_address mask** : correspond à l'adresse IP source et au masque du message IM.
  - **match [not] peer-ip-address ip\_address mask** : correspond à l'adresse IP de destination et au masque du message IM.
  - **match [not] version regex {regex\_name | class class\_name}** : correspond à la version du message IM en fonction de l'expression régulière ou de la liste d'expressions régulières spécifiée.
  - **match [not] filename regex {regex\_name | class class\_name}** : correspond au nom de fichier du message IM en fonction de l'expression régulière ou de la liste d'expressions régulières spécifiée. Cette correspondance n'est pas prise en charge pour le protocole MSN IM.
- d) Saisissez **exit** pour quitter le mode de configuration de carte de trafic.

**Étape 2** Créez une liste des politiques d'inspection IM : **policy-map type inspect im policy\_map\_name**

Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration de liste des politiques.

**Étape 3** (Facultatif) Ajoutez une description à la liste des politiques : **description string**

**Étape 4** Pour appliquer les actions au trafic correspondant, procédez comme suit.

- a) Précisez le trafic sur lequel vous souhaitez effectuer des actions en utilisant l'une des méthodes suivantes :
- Si vous avez créé une carte de trafic IM, spécifiez-la en entrant la commande suivante : **class class\_map\_name**
  - Précisez le trafic directement dans la liste des politiques à l'aide de l'une des commandes **match** décrites pour les cartes de classe IM. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.
- b) Précisez l'action que vous souhaitez effectuer sur le trafic correspondant en entrant la commande suivante :
- **drop-connection [log]** : abandonner le paquet et fermer la connexion.

- **reset [log]** : abandonne le paquet, ferme la connexion et envoie une réinitialisation TCP au serveur ou au client.
- **log** : envoie un message de journal système. Vous pouvez utiliser cette option seule ou avec l'une des autres actions.

Vous pouvez spécifier plusieurs commandes **class** ou **match** dans la liste des politiques. Pour en savoir plus sur l'ordre des commandes **class** et **match**, consultez [Comment plusieurs classes de trafic sont gérées](#), à la page 262.

## Exemple

L'exemple suivant montre comment définir une liste des politiques d'inspection IM.

```
hostname(config)# regex loginname1 "ying@yahoo.com"
hostname(config)# regex loginname2 "Kevin@yahoo.com"
hostname(config)# regex loginname3 "rahul@yahoo.com"
hostname(config)# regex loginname4 "darshant@yahoo.com"
hostname(config)# regex yahoo_version_regex "1\\.0"
hostname(config)# regex gif_files ".*\\.gif"
hostname(config)# regex exe_files ".*\\.exe"

hostname(config)# class-map type regex match-any yahoo_src_login_name_regex
hostname(config-cmap)# match regex loginname1
hostname(config-cmap)# match regex loginname2

hostname(config)# class-map type regex match-any yahoo_dst_login_name_regex
hostname(config-cmap)# match regex loginname3
hostname(config-cmap)# match regex loginname4

hostname(config)# class-map type inspect im match-any yahoo_file_block_list
hostname(config-cmap)# match filename regex gif_files
hostname(config-cmap)# match filename regex exe_files

hostname(config)# class-map type inspect im match-all yahoo_im_policy
hostname(config-cmap)# match login-name regex class yahoo_src_login_name_regex
hostname(config-cmap)# match peer-login-name regex class yahoo_dst_login_name_regex

hostname(config)# class-map type inspect im match-all yahoo_im_policy2
hostname(config-cmap)# match version regex yahoo_version_regex

hostname(config)# class-map im_inspect_class_map
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map type inspect im im_policy_all
hostname(config-pmap)# class yahoo_file_block_list
hostname(config-pmap-c)# match service file-transfer
hostname(config-pmap)# class yahoo_im_policy
hostname(config-pmap-c)# drop-connection
hostname(config-pmap)# class yahoo_im_policy2
hostname(config-pmap-c)# reset
hostname(config)# policy-map global_policy_name
hostname(config-pmap)# class im_inspect_class_map
hostname(config-pmap-c)# inspect im im_policy_all
```

**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 270.

## 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-parameters/ip-parameters.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 (Alerte de routeur) 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 106 012 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.

Voici la configuration de la liste des politiques :

```
policy-map type inspect ip-options _default_ip_options_map
description Default IP-OPTIONS policy-map
```

```
parameters
router-alert action allow
```

## 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 carte de politiques d'inspection d'options IP pour préciser comment vous souhaitez gérer chaque type d'option.

### Procédure

- Étape 1** Créez une liste des politiques d'inspection des options IP : **policy-map type inspect ip-options**  
*policy\_map\_name*
- Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.
- Étape 2** (Facultatif) Ajoutez une description à la liste des politiques : **description chaîne**
- Étape 3** Entrez en mode de configuration des paramètres :

```
hostname(config-pmap) # parameters
hostname(config-pmap-p) #
```

- Étape 4** Déterminez les options que vous souhaitez autoriser.
- Vous pouvez inspecter les options suivantes. Dans tous les cas, l'action **allow** autorise les paquets qui contiennent l'option sans modification; l'action **clear** autorise les paquets mais supprime l'option de l'en-tête.
- Utilisez la forme **no** de la commande pour supprimer l'option de la liste. Tout paquet qui contient une option que vous n'incluez pas dans la liste est abandonné, même si le paquet contient des options autorisées ou effacées par ailleurs.
- 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>.
- **default action {allow | clear}** : définit l'action par défaut pour toute option qui n'est pas explicitement incluse dans la liste. Si vous ne définissez pas d'action par défaut d'autorisation ou d'effacement, les paquets qui contiennent des options non autorisées sont abandonnés
  - **basic-security action {allow | clear}** : autorise ou efface l'option Security (SEC).
  - **commercial-security action {allow | clear}** : autorise ou efface l'option de sécurité commerciale (CIPSO).
  - **eoool action {allow | clear}** : autorise ou efface l'option de fin de liste d'options.
  - **exp-flow-control action {allow | clear}** : autorise ou efface l'option de contrôle de flux expérimental (FINN).
  - **exp-measurement action {allow | clear}** : autorise ou efface l'option de mesure expérimentale (ZSU).
  - **extended-security action {allow | clear}** : autorise ou efface l'option de sécurité étendue (E-SEC).
  - **imi-traffic-descriptor action {allow | clear}** : autorise ou efface l'option de descripteur de trafic IMI (IMITD).
  - **noop action {allow | clear}** : autorise ou efface l'option Aucune opération.

- **quick-start action** {allow | clear} : autorise ou efface l'option de démarrage rapide (QS).
- **record-route action** {allow | clear} : autorise ou efface l'option de routage d'enregistrement (RR).
- **router-alert action** {allow | clear} : autorise ou efface l'option d'alerte de routeur (RTRALT).
- **timestamp action** {allow | clear} : autorise ou efface l'option d'horodatage (TS).
- **{0-255} action** {allow | clear} : autorise ou efface l'option identifiée par le 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>.

### 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 270.

## 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 carte 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 carte de politiques d'inspection que si vous souhaitez des valeurs différentes ou si vous souhaitez définir des valeurs HA.

### Procédure

- 
- Étape 1** Créer une liste des politiques d'inspection IPsec Pass Through : **policy-map type inspect ipsec-pass-thru** *policy\_map\_name*
- Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration de liste des politiques.
- Étape 2** (Facultatif) Ajoutez une description à la liste des politiques : **description** *string*
- Étape 3** Pour configurer les paramètres qui influent sur le moteur d'inspection, procédez comme suit :
- Entrez en mode de configuration des paramètres :
 

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```
  - Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option :
    - esp per-client-max** *number* **timeout** *time* : autorise les tunnels ESP et définit le nombre maximal de connexions autorisées par client et le délai d'inactivité (au format hh:mm:ss). Pour autoriser un nombre illimité de connexions, spécifiez 0 pour le nombre.
    - ah per-client-max** *number* **délai d'expiration** *temps* : autorise les tunnels AH. Les paramètres ont la même signification que pour la commande esp.
- 

### Exemple

L'exemple suivant montre comment utiliser les listes de contrôle d'accès pour identifier le trafic IKE, définir une carte de paramètres IPsec Pass Thru, définir une politique et appliquer la politique à l'interface externe :

```
hostname(config)# access-list ipsecpassthruacl permit udp any any eq 500
hostname(config)# class-map ipsecpassthru-traffic
hostname(config-cmap)# match access-list ipsecpassthruacl
hostname(config)# policy-map type inspect ipsec-pass-thru iptmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
hostname(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
```

```
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class ipsecpassthru-traffic
hostname(config-pmap-c)# inspect ipsec-pass-thru iptmap
hostname(config)# service-policy inspection_policy interface outside
```

## 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 carte de politique d'inspection, la carte de politique 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.

Voici la configuration de la liste des politiques :

```
policy-map type inspect ipv6 _default_ipv6_map
description Default IPV6 policy-map
parameters
verify-header type
verify-header order
match header routing-type range 0 255
drop log
```

## 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** Créer une liste des politiques d'inspection IPv6 : **policy-map type inspect ipv6 *policy\_map\_name***

Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.



**Étape 2**

(Facultatif) Ajoutez une description à la liste des politiques : **description string**

**Étape 3**

(Facultatif) Abandonnez ou journalisez le trafic en fonction des en-têtes des messages IPv6.

a) Identifier le trafic en fonction de l'en-tête IPv6 : **match header type**

Où *type* est l'un des suivants :

- **ah** : correspond à l'en-tête de l'extension d'authentification IPv6.
- **count gt number** : spécifie le nombre maximal d'en-têtes d'extension IPv6, de 0 à 255.
- **destination-option** : correspond à l'en-tête d'extension IPv6 destination-option.
- **esp** : correspond à l'en-tête d'extension ESP (IPv6 Encapsulation Security Payload).
- **fragment** : correspond à l'en-tête d'extension fragment IPv6.
- **hop-by-hop** : correspond à l'en-tête d'extension IPv6 hop-by-hop.
- **routing-address count gt number** : définit le nombre maximal d'adresses d'en-tête de routage IPv6 de type 0, supérieur à un nombre entre 0 et 255.
- **routing-type {eq | range} number** : correspond au type d'en-tête de routage IPv6, de 0 à 255. Pour une plage, séparez les valeurs par un espace, par exemple, **30 40**.

b) Précisez l'action à effectuer sur les paquets correspondants. Vous pouvez abandonner le paquet et éventuellement le consigner, ou tout simplement le consigner. Si vous n'entrez pas d'action, le paquet est journalisé.

- **drop [log]** : abandon de tous les paquets qui correspondent.
- **log** : envoie un message de journal système. Vous pouvez utiliser cette option seule ou avec l'une des autres actions.

c) Répétez le processus jusqu'à ce que vous identifiiez tous les en-têtes que vous souhaitez abandonner ou journaliser.

**Étape 4**

Configurez les paramètres qui influent sur le moteur d'inspection.

a) Entrez dans le mode de configuration des paramètres.

```
hostname(config-pmap) # parameters
hostname(config-pmap-p) #
```

b) Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option :

- **verify-header type** : autorise uniquement les en-têtes d'extension IPv6 connus.
- **verify-header order** : applique l'ordre des en-têtes d'extension IPv6 tel qu'il est défini dans la RFC 2460.

### Exemple

L'exemple suivant crée une liste des politiques d'inspection qui supprimera et consignera tous les paquets IPv6 avec les en-têtes saut par saut, option de destination, adresse de routage et type de routage 0. Il applique également l'ordre et le type d'en-tête.

```
policy-map type inspect ipv6 ipv6-pm
 parameters
 verify-header type
 verify-header order
 match header hop-by-hop
 drop log
 match header destination-option
 drop log
 match header routing-address count gt 0
 drop log
 match header routing-type eq 0
 drop log

policy-map global_policy
 class class-default
 inspect ipv6 ipv6-pm
 !
service-policy global_policy global
```

### 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 270.

## 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. Elle 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

- 
- |                |                                                                                                                                                                                                                                                                     |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Étape 1</b> | Créer une liste des politiques d'inspection NetBIOS : <b>policy-map type inspect netbios</b> <i>policy_map_name</i><br>Où <i>policy_map_name</i> est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map. |
| <b>Étape 2</b> | (Facultatif) Ajouter une description à la liste des politiques : <b>description</b> <i>chaîne</i>                                                                                                                                                                   |
| <b>Étape 3</b> | Entrez dans le mode de configuration des paramètres.                                                                                                                                                                                                                |

```
hostname(config-pmap) # parameters
hostname(config-pmap-p) #
```

#### Étape 4

Précisez l'action à entreprendre pour les violations du protocole NETBIOS : **protocol-violation action {drop [log] | log}**

Où l'action **drop** abandonne le paquet. L'action **log** envoie un message de journal système lorsque cette liste des politiques correspond au trafic.

---

#### Exemple

```
hostname(config)# policy-map type inspect netbios netbios_map
hostname(config-pmap) # parameters
hostname(config-pmap-p) # protocol-violation drop log

hostname(config)# policy-map netbios_policy
hostname(config-pmap) # class inspection_default
hostname(config-pmap-c) # no inspect netbios
hostname(config-pmap-c) # inspect netbios netbios_map
```

#### 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 270.

## Inspection PPTP

PPTP est un protocole de tunnellation 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 270.

## 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 270.

## 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 la configurer que si vous souhaitez un traitement différent de celui fourni par la carte 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><LR>).
- 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.
- 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.

Voici la configuration de la liste des politiques :

```
policy-map type inspect esmtp _default_esmtp_map
description Default ESMTP policy-map
parameters
mask-banner
no mail-relay
```

```

no special-character
allow-tls
match cmd line length gt 512
drop-connection log
match cmd RCPT count gt 100
drop-connection log
match body line length gt 998
log
match header line length gt 998
drop-connection log
match sender-address length gt 320
drop-connection log
match MIME filename length gt 255
drop-connection log
match ehlo-reply-parameter others
mask

```

## 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 classe d'expression régulière.

### Procédure

- 
- Étape 1** Créez une liste des politiques d'inspection ESMTP : **policy-map type inspect esmtp** *policy\_map\_name*  
Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration de la liste des politiques.
- Étape 2** (Facultatif) Ajoutez une description à la liste des politiques : **description** *string*
- Étape 3** Pour appliquer les actions au trafic correspondant, procédez comme suit.
- Précisez le trafic pour lequel vous souhaitez effectuer des actions à l'aide de l'une des commandes **match** suivantes. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.
    - match [not] body {length | line length} gt bytes** : correspond aux messages dans lesquels la longueur ou la longueur d'une ligne dans un message de corps ESMTP est supérieure au nombre d'octets spécifié.
    - match [not] cmd Verb Verb1 [Verb2...]** : 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.
    - match [not] cmd line length gt bytes** : correspond aux messages dans lesquels la longueur d'une ligne dans le verbe de commande est supérieure au nombre d'octets spécifié.

- **match [not] cmd rcpt count gt count** : correspond aux messages dans lesquels le nombre de destinataires est supérieur au nombre spécifié.
- **match [not] ehlo-reply-parameter parameter [parameter2...]** : 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.
- **match [not] header {length | line length} gt bytes** : correspond aux messages dans lesquels la longueur ou la longueur d'une ligne dans un en-tête ESMTP est supérieure au nombre d'octets spécifié.
- **match [not] header to-fields count gt count** : correspond aux messages dans lesquels le nombre de champs To dans l'en-tête est supérieur au nombre spécifié.
- **match [not] invalid-recipients count gt number** : correspond aux messages dans lesquels le nombre de destinataires non valides est supérieur au nombre spécifié.
- **match [not] mime filetype regex {regex\_name | class class\_name}** : correspond au type de fichier MIME ou multimédia avec l'expression régulière ou la liste d'expressions régulières spécifiée.
- **match [not] mime filename length gt bytes** : correspond aux messages dans lesquels le nom de fichier est plus long que le nombre d'octets spécifié.
- **match [not] mime encoding type [type2...]** : correspond au type d'encodage MIME. Vous pouvez spécifier un ou plusieurs des types suivants : 7bit, 8bit, base64, binary, others, quoted-printable.
- **match [not] sender-address regex {regex\_name | class class\_name}** : fait correspondre l'adresse courriel de l'expéditeur à l'expression régulière ou à la liste d'expressions régulières spécifiée.
- **match [not] sender-address length gt bytes** : correspond aux messages dans lesquels l'adresse de l'expéditeur est supérieure au nombre d'octets spécifié.

b) Précisez l'action que vous souhaitez effectuer sur le trafic correspondant en saisissant l'une des commandes suivantes :

- **drop-connection [log]** : abandonner le paquet et fermer la connexion.
- **mask [log]** : masque la partie correspondante du paquet. Cette action est disponible uniquement pour **ehlo-reply-parameter** et **cmd verb**.
- **reset [log]** : abandonne le paquet, ferme la connexion et envoie une réinitialisation TCP au serveur ou au client.
- **log** : envoie un message de journal système. Vous pouvez utiliser cette option seule ou avec l'une des autres actions.
- **rate-limit message\_rate** : limite le débit de messages en paquets par seconde. Cette option est disponible uniquement avec **cmd verb**, où vous pouvez l'utiliser comme seule action ou vous pouvez l'utiliser en conjonction avec l'action **mask**.

Vous pouvez spécifier plusieurs commandes **match** dans la liste des politiques. Pour en savoir plus sur l'ordre des commandes **match**, consultez [Comment plusieurs classes de trafic sont gérées, à la page 262](#).

#### Étape 4

Pour configurer les paramètres qui influent sur le moteur d'inspection, procédez comme suit :

a) Entrez en mode de configuration des paramètres :

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

- b) Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option :
- **mail-relay domain-name action {drop-connection [log] | log}** : identifie un nom de domaine pour le relais de messagerie. Vous pouvez soit abandonner la connexion et éventuellement la journaliser, soit la journaliser.
  - **mask-banner** : masque la bannière du serveur ESMTP.
  - **special-character action {drop-connection [log] | log}** : identifie l'action à prendre pour les messages qui comprennent 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.
  - **allow-tls [action log]** : 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 spécifiez **no allow-tls**, le système supprime l'indication STARTTLS de la connexion de session et force une connexion en texte brut.

## Exemple

L'exemple suivant montre comment définir une liste des politiques d'inspection ESMTP.

```
hostname(config)# regex user1 "user1@cisco.com"
hostname(config)# regex user2 "user2@cisco.com"
hostname(config)# regex user3 "user3@cisco.com"
hostname(config)# class-map type regex senders_black_list
hostname(config-cmap)# description "Regular expressions to filter out undesired senders"
hostname(config-cmap)# match regex user1
hostname(config-cmap)# match regex user2
hostname(config-cmap)# match regex user3

hostname(config)# policy-map type inspect esmtp advanced_esmtp_map
hostname(config-pmap)# match sender-address regex class senders_black_list
hostname(config-pmap-c)# drop-connection log

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect esmtp advanced_esmtp_map

hostname(config)# service-policy outside_policy interface outside
```

## 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 270](#).



# 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

Créez une liste SNMP.

Utilisez la commande **snmp-map** *map\_name* pour créer la liste et passer en mode de configuration de liste SNMP, puis la commande **deny version** *version* pour identifier les versions à refuser. La version peut être 1, 2, 2c ou 3.

### Exemple :

L'exemple suivant refuse les versions SNMP 1 et 2 :

```
hostname(config)# snmp-map sample_map
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# deny version 2
```

## 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 270.

## 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 270.

## 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** Configurez les propriétés du service Sun RPC.

**sunrpc-server** *interface\_name ip\_address mask* **service** *service\_type* **protocol** {**tcp** | **udp**} *port*[-*port*]  
**timeout** *hh:mm:ss*

Lieu :

- *interface\_name* : l'interface par laquelle le trafic passe vers le serveur.
- *ip\_address mask* : l'adresse du serveur Sun RPC.
- **service** *service\_type* : le type de service sur le serveur, qui est le mappage entre un type de service spécifique et le numéro de port utilisé pour le service. 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** {**tcp** | **udp**} : si le service utilise TCP ou UDP.
- *port*[-*port*] : le port ou la plage de ports utilisés par le service. Pour spécifier une plage de ports, séparez les numéros de ports de début et de fin dans la plage par un tiret (par exemple, 111-113).
- **timeout** *hh:mm:ss* : délai d'inactivité du passage ouvert pour la connexion par l'inspection Sun RPC.

#### Exemple :

Par exemple, pour créer un délai d'expiration de 30 minutes pour le serveur Sun RPC avec l'adresse IP 192.168.100.2, saisissez la commande suivante. Dans cet exemple, le serveur Sun RPC se trouve sur l'interface interne en utilisant le port TCP 111.

```
hostname(config)# sunrpc-server inside 192.168.100.2 255.255.255.255
service 100003 protocol tcp 111 timeout 00:30:00
```

**Étape 2** (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**. 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 270](#).

## 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 270](#).

# 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-traffic`, 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.<br><br>Nous n'avons pas modifié de commandes.                                                                                                                                                                                                         |
| Inspection des paquets VXLAN                                                                            | 9.4(1)   | L'ASA peut inspecter l'en-tête VXLAN pour faire respecter le format standard.<br><br>Nous avons introduit la commande suivante : <b>inspect vxlan</b> .                                                                                                                                                                                                                                                                                                                                                          |
| 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 <b>no allow-tls</b> , la commande n'est pas modifiée.<br><br>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)   | <p>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.</p> <p>Nous avons ajouté les commandes suivantes : <b>basic-security</b>, <b>commercial-security</b>, <b>default</b>, <b>exp-flow-control</b>, <b>exp-measure</b>, <b>extended-security</b>, <b>imi-traffic-description</b>, <b>quick-start</b>, <b>record-route</b>, <b>timestamp</b>, et <b>{0-255}</b> (qui indique un numéro de type d'option IP).</p>                                                                  |
| Améliorations de l'inspection DCERPC et du filtrage des UUID | 9.5(2)   | <p>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.</p> <p>Nous avons introduit la commande suivante : <b>match [not] uuid</b>. Nous avons modifié la commande suivante : <b>class-map type inspect</b>.</p>                                                                                                                                                                                                                                                                                                         |
| Inspection DNS sur TCP                                       | 9.6(2)   | <p>Vous pouvez désormais inspecter le trafic DNS sur TCP (TCP/53).</p> <p>Nous avons ajouté la commande suivante : <b>tcp-inspection</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Prise en charge de Cisco Umbrella                            | 9.10(1)  | <p>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.</p> <p>Nous avons ajouté ou modifié les commandes suivantes : <b>umbrella</b> (modes de configuration des paramètres globaux et de liste des politiques), <b>token</b>, <b>public-key</b>, <b>timeout edns</b>, <b>dnscrypt</b>, <b>show service-policy inspect dns detail</b>.</p> |

| Nom de la caractéristique                                                | Versions | Renseignements sur les fonctionnalités                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Améliorations de Cisco Umbrella.                                         | 9.12(1)  | <p>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.</p> <p>Nous avons ajouté ou modifié les commandes suivantes : <b>local-domain-bypass</b>, <b>resolver</b>, <b>umbrella fail-open</b>.</p> |
| Inspection XDMCP désactivée par défaut dans les nouvelles installations. | 9.15(1)  | <p>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.</p>                                                                                                                                                                                                                          |







## 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 261.

- [Inspection CTIQBE](#), à la page 327
- [Inspection H.323](#), à la page 328
- [Inspection MGCP](#), à la page 333
- [Inspection RTSP](#), à la page 336
- [Inspection SIP](#), à la page 340
- [Inspection Skinny \(SCCP\)](#), à la page 346
- [Inspection STUN](#), à la page 349
- [Historique de l'inspection des protocoles vocaux et vidéo](#), à la page 350

## 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 270.

## Limites de l'inspection CTIQBE

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 tunnellation 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 la configurer que si vous souhaitez un traitement autre que celui par défaut.

Les sections suivantes décrivent l'inspection des applications H.323.

## Aperçu 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 avec un paquet passant par l'inspection H.323 est marquée comme une connexion H.323 et expire avec le délai H.323, comme configuré avec la commande **timeout**.



#### 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. Pour activer l'appel de configuration entre les terminaux H.323, entrez la commande **ras-rcf-pinholes enable** en mode de configuration des paramètres lors de la création d'une liste des politiques d'inspection H.323.

## 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.

### 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 classe d'expression régulière.

### Procédure

#### Étape 1

(Facultatif) Créez une carte de trafic d'inspection H.323 en procédant comme suit.

Une carte de trafic regroupe plusieurs correspondances de trafic. Vous pouvez également identifier les commandes **match** directement dans la liste des politiques. La différence entre la création d'une carte de classe et la définition de la correspondance de trafic directement dans la liste des politiques d'inspection est que la carte de classe vous permet de créer des critères de correspondance plus complexes, et vous pouvez réutiliser les cartes de classe.

Pour spécifier le trafic qui ne doit pas correspondre à la carte de classe, utilisez la commande **match not**. Par exemple, si la commande **match not** spécifie la chaîne « example.com », tout trafic qui inclut « example.com » ne correspond pas à la carte de trafic.

Pour le trafic que vous identifiez dans cette carte de trafic, vous spécifiez les actions à prendre sur le trafic dans la liste des politiques d'inspection.

Si vous souhaitez effectuer différentes actions pour chaque commande **match**, vous devez identifier le trafic directement dans la liste des politiques.

- a) Créez la carte de trafic : **class-map type inspect h323 [match-all | match-any] class\_map\_name**

Où *class\_map\_name* est le nom de la carte de trafic. Le mot-clé **match-all** est le mot-clé par défaut. Il spécifie que le trafic doit correspondre à tous les critères pour correspondre à la carte de trafic. Le mot-clé **match-any** spécifie que le trafic correspond à la carte de trafic s'il correspond à au moins un des critères. L'interface de ligne de commande passe en mode de configuration class-map, où vous pouvez saisir une ou plusieurs commandes **match**.

- b) (Facultatif) : Ajoutez une description à la carte de trafic : **description string**

Où *string* est la description de la carte de trafic (jusqu'à 200 caractères).

- c) Précisez le trafic pour lequel vous souhaitez effectuer des actions à l'aide de l'une des commandes **match** suivantes. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

- **match [not] called-party regex {regex\_name | class class\_name}** : met en correspondance l'appelé avec l'expression régulière ou la liste d'expressions régulières spécifiée.
- **match [not] calling-party regex {regex\_name | class class\_name}** : met en correspondance l'appelant avec l'expression régulière ou la liste d'expressions régulières spécifiée.
- **match [not] media-type {audio | data | video}** : correspond au type de média.

- Étape 2** Créer une liste des politiques d'inspection H.323 : **policy-map type inspect h323 policy\_map\_name**

Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.

- Étape 3** (Facultatif) Ajoutez une description à la liste des politiques : **description string**

- Étape 4** Pour appliquer les actions au trafic correspondant, procédez comme suit.

Vous pouvez spécifier plusieurs commandes **class** ou **match** dans la liste des politiques. Pour en savoir plus sur l'ordre des commandes **class** et **match**, consultez [Comment plusieurs classes de trafic sont gérées, à la page 262](#).

- a) Précisez le trafic sur lequel vous souhaitez effectuer des actions en utilisant l'une des méthodes suivantes :

- Si vous avez créé une carte de trafic H.323, spécifiez-la en entrant la commande suivante : **class class\_map\_name**
- Précisez le trafic directement dans la liste des politiques à l'aide de l'une des commandes **match** décrites pour les cartes de trafic H.323. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

- b) Précisez l'action que vous souhaitez effectuer sur le trafic correspondant en saisissant l'une des commandes suivantes :

- **drop [log]** : abandonner le paquet. Pour les correspondances de type de support, vous pouvez inclure le mot-clé **log** pour envoyer un message de journal système.
- **drop-connection** : abandonner le paquet et fermer la connexion. Cette option est disponible pour la correspondance de l'appelé ou de l'appelant.
- **reset** : abandonner le paquet, fermer la connexion et envoyer une réinitialisation TCP au serveur ou au client. Cette option est disponible pour la correspondance de l'appelé ou de l'appelant.

**Étape 5** Pour configurer les paramètres qui influent sur le moteur d'inspection, procédez comme suit :

a) Entrez en mode de configuration des paramètres :

```
hostname(config-pmap) # parameters
hostname(config-pmap-p) #
```

b) Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option :

- **ras-rcf-pinholes enable** : active la configuration des appels entre les terminaux H.323. Vous pouvez activer la configuration d'appel entre les terminaux H.323 lorsque le portier se trouve dans le réseau. Utilisez cette option pour ouvrir des trous d'épingle pour les appels basés sur les messages RegistrationRequest/RegistrationConfirm (RRQ/RCF). Comme ces messages RRQ/RCF sont envoyés vers et depuis le Gatekeeper, l'adresse IP du point d'extrémité appelant est inconnue et l'ASA ouvre un trou d'épingle via l'adresse IP/port source 0/0. Par défaut, cette option est activée.
- **timeout users time** : définit la limite de durée de l'appel H.323 (au format hh:mm:ss). Pour n'avoir aucun délai d'expiration, spécifiez 00:00:00. La plage est comprise entre 0:0:0 et 1193:0:0.
- **call-party-number** : applique l'envoi du numéro de partie d'appel lors de l'établissement de l'appel.
- **action h245-tunnel-block {drop-connection | log}** : applique le blocage de tunnel H.245. Précisez si vous souhaitez abandonner la connexion ou simplement la journaliser.
- **rtp-conformance [enforce-payloadtype]** : vérifie les paquets RTP circulant dans les passages pour vérifier la conformité du protocole. Le mot-clé facultatif enforce-payloadtype applique le type de charge utile pour qu'il soit audio ou vidéo en fonction de l'échange de signalisation.
- **state-checking {h225 | ras}** : active la validation de la vérification de l'état. Vous pouvez saisir la commande séparément pour activer la vérification de l'état pour H.225 et RAS.
- **early-message message\_type** : s'il faut autoriser le type spécifié de messages H.225 avant le message SETUP H.225. Vous pouvez autoriser le message **facility** à arriver tôt, 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, utilisez cette commande 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).

**Étape 6** Tout en étant toujours en mode de configuration des paramètres, vous pouvez configurer les groupes HSI.

a) Définissez un groupe HSI et passez en mode de configuration de groupe HSI : **hsi-group id**

Où *id* est l'identifiant de groupe HSI. La plage est comprise entre 0 et 2 147 483 647.

- b) Ajoutez un HSI au groupe de HSI en utilisant l'adresse IP : **hsi ip\_address**

Vous pouvez ajouter un maximum de cinq hôtes par groupe de HSI.

- c) Ajouter un terminal au groupe HSI : **endpoint ip\_address if\_name**

Où *ip\_address* est le terminal à ajouter et *if\_name* est l'interface par laquelle le terminal est connecté à l'ASA. Vous pouvez ajouter un maximum de dix terminaux par groupe de HSI.

---

### Exemple

L'exemple suivant montre comment configurer le filtrage de numéro de téléphone :

```
hostname(config)# regex caller 1 "5551234567"
hostname(config)# regex caller 2 "5552345678"
hostname(config)# regex caller 3 "5553456789"

hostname(config)# class-map type inspect h323 match-all h323_traffic
hostname(config-pmap-c)# match called-party regex caller1
hostname(config-pmap-c)# match calling-party regex caller2

hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# class h323_traffic
hostname(config-pmap-c)# drop
```

### 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 270.

## 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.

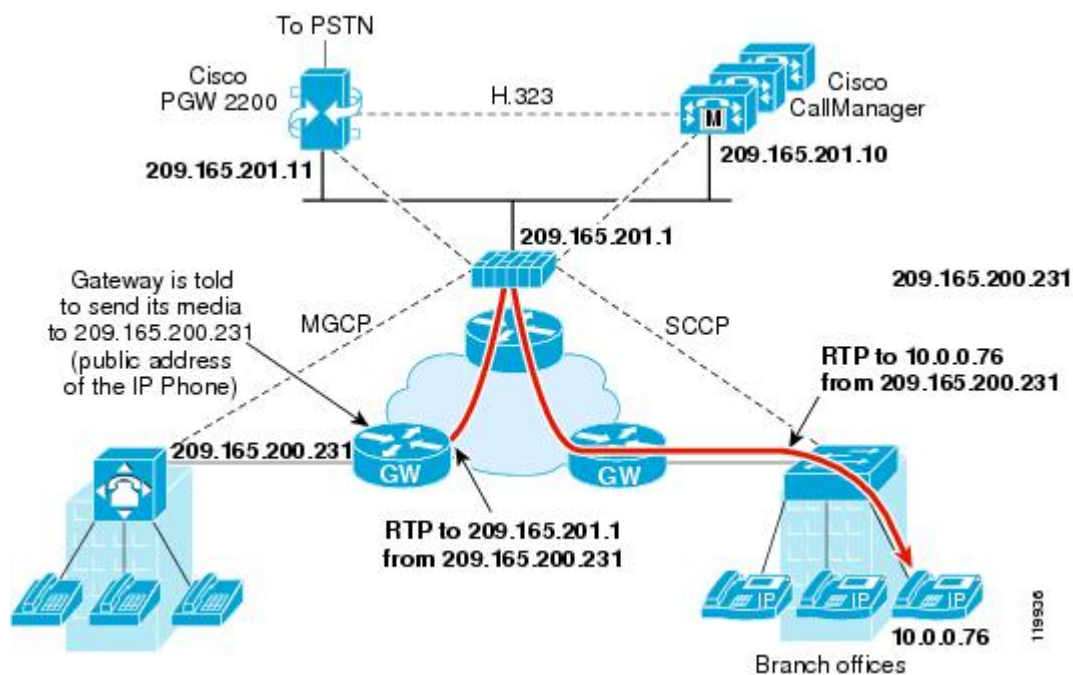
## Aperçu de l'inspection MGCP

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 41 : 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** Pour créer une liste des politiques d'inspection MGCP : **policy-map type inspect mgcp policy\_map\_name**  
Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.
- Étape 2** (Facultatif) Ajoutez une description à la liste des politiques : **description string**
- Étape 3** Entrez dans le mode de configuration des paramètres.

```
hostname(config-pmap) # parameters
hostname(config-pmap-p) #
```

- Étape 4** Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option.
- **call-agent ip\_address group\_id** : configure les groupes d'agents d'appel qui peuvent gérer une ou plusieurs passerelles. Les informations de groupe d'agents d'appel sont utilisées pour ouvrir des connexions pour les agents d'appel du groupe (hormis celui auquel une passerelle envoie une commande), afin que n'importe quel agent d'appel puisse envoyer la réponse. Les agents d'appel avec le même *group\_id* appartiennent au même groupe. Un agent d'appel peut appartenir à plusieurs groupes. L'option *group\_id* est un nombre compris entre 0 et 4 294 967 295. L'option *ip\_address* spécifie l'adresse IP de l'agent d'appel.
- Remarque**  
Les agents d'appel MGCP envoient des messages AUEP pour déterminer si les terminaux MGCP sont présents. Cela établit un flux dans l'ASA et permet aux terminaux MGCP de s'enregistrer auprès de l'agent d'appel.
- **gateway ip\_address group\_id** : identifie quel groupe d'agents d'appel gère une passerelle particulière. L'adresse IP de la passerelle est spécifiée avec l'option *ip\_address*. L'option *group\_id* est un nombre compris entre 0 et 4 294 967 295 qui doit correspondre à l'identifiant de groupe des agents d'appel qui gèrent la passerelle. Une passerelle ne peut appartenir qu'à un seul groupe.

- **command-queue** *command\_limit* : définit le nombre maximal de commandes autorisées dans la file d'attente de commande MGCP, de 1 à 2 147 483 647. Par défaut, c'est 200.

### Exemple

L'exemple suivant montre comment définir une liste MGCP :

```
hostname(config)# policy-map type inspect mgcp sample_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-agent 10.10.11.5 101
hostname(config-pmap-p)# call-agent 10.10.11.6 101
hostname(config-pmap-p)# call-agent 10.10.11.7 102
hostname(config-pmap-p)# call-agent 10.10.11.8 102
hostname(config-pmap-p)# gateway 10.10.10.115 101
hostname(config-pmap-p)# gateway 10.10.10.116 102
hostname(config-pmap-p)# gateway 10.10.10.117 102
hostname(config-pmap-p)# command-queue 150
```

### 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 270](#).

## 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 double NAT. 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 la multidiffusion RTSP 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.
- L'ASA ne peut pas effectuer la NAT sur les messages RTSP, car les adresses IP intégrées sont contenues dans les fichiers SDP dans le cadre des messages HTTP ou RTSP. Les paquets peuvent être fragmentés et l'ASA ne peut pas effectuer de NAT sur les paquets fragmentés.
- 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.

### 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

(Facultatif) Créez une carte de trafic d'inspection FTP en procédant comme suit.

Une carte de trafic regroupe plusieurs correspondances de trafic. Vous pouvez également identifier les commandes **match** 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 la carte de trafic vous permet de créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafic.

Pour spécifier le trafic qui ne doit pas correspondre à la carte de trafic, utilisez la commande **match not**. Par exemple, si la commande **match not** spécifie la chaîne « example.com », tout trafic qui inclut « example.com » ne correspond pas à la carte de classes.

Pour le trafic que vous identifiez dans cette carte de trafic, vous spécifiez les actions à appliquer dans la liste des politiques d'inspection.

Si vous souhaitez effectuer des actions différentes pour chaque commande **match**, vous devez identifier le trafic directement dans la liste des politiques.

- a) Créez la carte de trafic : **class-map type inspect rtsp [match-all | match-any] class\_map\_name**

Où *class\_map\_name* est le nom de la carte de trafic. Le mot-clé **match-all** est le mot-clé par défaut. Il spécifie que le trafic doit correspondre à tous les critères pour correspondre à la carte de trafic. Le mot-clé **match-any** spécifie que le trafic correspond à la carte de trafic s'il correspond à au moins un des critères. L'interface de ligne de commande passe en mode de configuration class-map, où vous pouvez saisir une ou plusieurs commandes **match**.

- b) (Facultatif) Ajoutez une description à la carte de trafic : **description string**

Où *string* est la description de la carte de trafic (jusqu'à 200 caractères).

- c) Précisez le trafic pour lequel vous souhaitez effectuer des actions à l'aide de l'une des commandes **match** suivantes. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

- **match [not] request-method method** : correspond à une méthode de demande RTSP. Les méthodes sont les suivantes : announce, describe, get\_parameter, options, pause, play, record, redirect, setup, set\_parameter, teardown.
- **match [not] url-filter regex {regex\_name | class class\_name}** : correspond à l'URL avec l'expression régulière ou à la liste d'expressions régulières spécifiée.

### Étape 2

Pour créer une liste des politiques d'inspection RTSP : **policy-map type inspect rtsp policy\_map\_name**

Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.

### Étape 3

(Facultatif) Ajoutez une description à la liste des politiques : **description string**

### Étape 4

Pour appliquer les actions au trafic correspondant, procédez comme suit.

- a) Précisez le trafic sur lequel vous souhaitez effectuer des actions en utilisant l'une des méthodes suivantes :
- Si vous avez créé une carte de trafic RTSP, spécifiez-la en entrant la commande suivante : **class class\_map\_name**

- Précisez le trafic directement dans la liste des politiques à l'aide de l'une des commandes **match** décrites pour les cartes de trafic RTSP. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.
- b) Précisez l'action que vous souhaitez effectuer sur le trafic correspondant en saisissant l'une des commandes suivantes :
- **drop-connection [log]** : abandon du paquet, fermeture de la connexion et éventuellement envoi d'un message de journal système. Cette option est disponible pour la mise en correspondance d'URL.
  - **log** : envoie un message de journal système.
  - **rate-limit message\_rate** : limite le débit de messages par seconde. Cette option est disponible pour la mise en correspondance de la méthode de demande.

Vous pouvez spécifier plusieurs commandes **class** ou **match** dans la carte de politiques. Pour en savoir plus sur l'ordre des commandes **class** et **match**, consultez [Comment plusieurs classes de trafic sont gérées, à la page 262](#).

## Étape 5

Pour configurer les paramètres qui influent sur le moteur d'inspection, procédez comme suit :

- a) Entrez en mode de configuration des paramètres :

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

- b) Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option :
- **reserve-port-protect** : restreint l'utilisation des ports de réservation lors de la négociation du support.
  - **url-length-limit bytes** : définit une limite de longueur d'URL autorisée dans le message, de 0 à 6 000 octets.

## Exemple

L'exemple suivant montre comment définir une liste des politiques d'inspection RTSP.

```
hostname(config)# regex badurl1 www.url1.com/rtsp.avi
hostname(config)# regex badurl2 www.url2.com/rtsp.rm
hostname(config)# regex badurl3 www.url3.com/rtsp.asp

hostname(config)# class-map type regex match-any badurl-list
hostname(config-cmap)# match regex badurl1
hostname(config-cmap)# match regex badurl2
hostname(config-cmap)# match regex badurl3

hostname(config)# policy-map type inspect rtsp rtsp-filter-map
hostname(config-pmap)# match url-filter regex class badurl-list
hostname(config-pmap-p)# drop-connection

hostname(config)# class-map rtsp-traffic-class
hostname(config-cmap)# match default-inspection-traffic
```

```
hostname(config)# policy-map rtsp-traffic-policy
hostname(config-pmap)# class rtsp-traffic-class
hostname(config-pmap-c)# inspect rtsp rtsp-filter-map

hostname(config)# service-policy rtsp-traffic-policy global
```

### 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 270.

## 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.

### Limitations 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 carte 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.

### 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 classe d'expression régulière.



## Procédure

**Étape 1** (Facultatif) Créez une carte de trafic d'inspection SIP en procédant comme suit.

Une carte de trafic regroupe plusieurs correspondances de trafic. Vous pouvez également identifier les commandes **match** 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 la carte de trafic vous permet de créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafic.

Pour spécifier le trafic qui ne doit pas correspondre à la carte de classe, utilisez la commande **match not**. Par exemple, si la commande **match not** spécifie la chaîne « example.com », tout trafic qui inclut « example.com » ne correspond pas à la carte de trafic.

Pour le trafic que vous identifiez dans cette carte de trafic, vous spécifiez les actions à prendre sur le trafic dans la liste des politiques d'inspection.

Si vous souhaitez effectuer différentes actions pour chaque commande **match**, vous devez identifier le trafic directement dans la liste des politiques.

a) Créez la carte de trafic : **class-map type inspect sip [match-all | match-any] class\_map\_name**

Où *class\_map\_name* est le nom de la carte de trafic. Le mot-clé **match-all** est le mot-clé par défaut. Il spécifie que le trafic doit correspondre à tous les critères pour correspondre à la carte de trafic. Le mot-clé **match-any** spécifie que le trafic correspond à la carte de trafic s'il correspond à au moins un énoncé **match**. L'interface de ligne de commande passe en mode de configuration class-map, où vous pouvez saisir une ou plusieurs commandes **match**.

b) (Facultatif) : Ajoutez une description à la carte de trafic : **description string**

Où *string* est la description de la carte de trafic (jusqu'à 200 caractères).

c) Précisez le trafic pour lequel vous souhaitez effectuer des actions à l'aide de l'une des commandes **match** suivantes. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

- **match [not] called-party regex {regex\_name | class class\_name}** : correspond à l'appelé, comme spécifié dans l'en-tête To, en fonction de l'expression régulière ou de la liste d'expressions régulières spécifiée.
- **match [not] calling-party regex {regex\_name | class class\_name}** : correspond à l'appelant, tel qu'il est indiqué dans l'en-tête From, en fonction de l'expression régulière ou de la liste d'expressions régulières spécifiée.
- **match [not] content length gt bytes** : correspond aux messages dont la longueur du contenu dans l'en-tête SIP est supérieure au nombre d'octets spécifié, entre 0 et 65 536.
- **match [not] content type {sdp | regex {regex\_name | class class\_name}}** : correspond au type de contenu SDP ou à l'expression régulière ou à la liste d'expressions régulières spécifiée.
- **match [not] im-subscriber regex {regex\_name | class class\_name}** : correspond à l'abonné SIP IM en fonction de l'expression régulière ou de la liste d'expressions régulières spécifiée.
- **match [not] message-path regex {regex\_name | class class\_name}** : correspond à l'en-tête Via SIP en fonction de l'expression régulière ou de la liste d'expressions régulières spécifiée.

- **match [not] request-method *method*** : correspond à une méthode de requête SIP : ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, unknown, update.
- **match [not] third-party-registration regex {*regex\_name* | class *class\_name*}** : correspond au demandeur d'un enregistrement tiers en fonction de l'expression régulière ou de la liste d'expressions régulières spécifiée.
- **match [not] uri {sip | tel} length gt *bytes*** : correspond à un URI des en-têtes SIP du type sélectionné (SIP ou TEL) dont la longueur est supérieure à la valeur spécifiée, entre 0 et 65 536 octets.

d) Saisissez **exit** pour quitter le mode de configuration class-map.

**Étape 2** Créez une liste des politiques d'inspection SIP : **policy-map type inspect sip *policy\_map\_name***

Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.

**Étape 3** (Facultatif) Ajoutez une description à la liste des politiques : **description *string***

**Étape 4** Pour appliquer les actions au trafic correspondant, procédez comme suit.

a) Précisez le trafic sur lequel vous souhaitez effectuer des actions en utilisant l'une des méthodes suivantes :

- Si vous avez créé une carte de trafic SIP, spécifiez-la en entrant la commande suivante : **class *class\_map\_name***
- Définissez le trafic directement dans la liste des politiques à l'aide de l'une des commandes **match** décrites pour les cartes de trafic SIP. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

b) Précisez l'action que vous souhaitez effectuer sur le trafic correspondant en saisissant l'une des commandes suivantes :

- **drop** : abandon de tous les paquets qui correspondent.
- **drop-connection** : abandon du paquet et fermeture de la connexion.
- **reset** : abandon du paquet, fermeture de la connexion et envoi d'une réinitialisation TCP au serveur ou au client.
- **log** : envoie un message de journal système. Vous pouvez utiliser cette option seule ou avec l'une des autres actions.
- **rate-limit *message\_rate*** : limite le débit des messages. La limitation de débit est disponible pour les correspondances de méthode de demande « invite » et « register » uniquement.

Vous pouvez spécifier plusieurs commandes **class** ou **match** dans la liste des politiques. Pour en savoir plus sur l'ordre des commandes **class** et **match**, consultez [Comment plusieurs classes de trafic sont gérées, à la page 262](#).

**Étape 5** Pour configurer les paramètres qui influent sur le moteur d'inspection, procédez comme suit :

a) Entrez en mode de configuration des paramètres :

```
hostname (config-pmap) # parameters
hostname (config-pmap-p) #
```

b) Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option :

- **im** : active la messagerie instantanée.
- **ip-address-privacy** : active la confidentialité des adresses IP, qui masque les adresses IP du serveur et des terminaux.
- **max-forwards-validation action {drop | drop-connection | reset | log} [log]** : vérifie la valeur de l'en-tête Max-Forwards, qui ne peut pas être zéro 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.
- **rtp-conformance [enforce-payloadtype]** : vérifie les paquets RTP circulant dans les passages pour vérifier la conformité du protocole. Le mot-clé facultatif **enforce-payloadtype** applique le type de charge utile pour qu'il soit audio ou vidéo en fonction de l'échange de signalisation.
- **software-version action {mask [log] | log}** : identifie la version du logiciel à l'aide des champs d'en-tête Server et User-Agent (terminal). Vous pouvez masquer la version du logiciel dans les messages SIP et éventuellement la consigner ou tout simplement la consigner.
- **state-checking action {drop | drop-connection | reset | log} [log]** : active la vérification des transitions d'état. 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.
- **strict-header-validation action {drop | drop-connection | reset | log} [log]** : active la vérification stricte des champs d'en-tête des messages SIP conformément à la RFC 3261. 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.
- **traffic-non-sip** : autorise le trafic non SIP sur le port de signalisation SIP bien connu.
- **trust-verification-server ip ip\_address** : identifie 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 entrer la commande jusqu'à quatre fois pour identifier quatre serveurs. 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.
- **trust-verification-server port number** : identifie le port des services de vérification de confiance. Le port par défaut est 2445. Utilisez donc cette commande uniquement si le serveur utilise un port différent. La plage de ports autorisée est de 1 026 à 32 768.
- **uri-non-sip action {mask [log] | log}** : identifie les URI non SIP présents dans les champs d'en-tête Alert-Info et Call-Info. Vous pouvez masquer les informations dans les messages SIP et éventuellement les consigner, ou tout simplement les consigner.

---

## Exemples

L'exemple suivant montre comment désactiver la messagerie instantanée sur SIP :

```
hostname(config)# policy-map type inspect sip mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# no im

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect sip mymap

hostname(config)# service-policy global_policy global
```

L'exemple suivant montre comment identifier quatre serveurs de services de vérification de confiance.

```
hostname(config)# policy-map type inspect sip sample_sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.1
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.2
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.3
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.4
hostname(config-pmap-p)# trust-verification-server port 2445
```

### 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 270.

## 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, elle est mappée 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** Créez une liste des politiques d'inspection SCCP : **policy-map type inspect skinny policy\_map\_name**  
Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.
- Étape 2** (Facultatif) Ajoutez une description à la liste des politiques : **description string**
- Étape 3** (Facultatif) Abandonnez le trafic en fonction du champ d'ID de message de station dans les messages SCCP.
- Identifiez le trafic en fonction de la valeur de l'ID du message de la station en hexadécimal, de 0x0 à 0xffff. Vous pouvez spécifier un ID unique ou une plage d'ID à l'aide de la commande **match [not] message-id**. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.  
**match message-id {value | range start\_value end\_value}**  
**Exemple :**  

```
hostname(config-pmap)# match message-id 0x181
hostname(config-pmap)# match message-id range 0x200 0xffff
```
  - Précisez l'action à effectuer sur les paquets correspondants. Vous pouvez abandonner le paquet et éventuellement le journaliser : **drop [log]**
  - Répétez le processus jusqu'à ce que vous identifiiez tous les ID de message que vous souhaitez supprimer.
- Étape 4** Configurez les paramètres qui influent sur le moteur d'inspection.
- Entrez en mode de configuration des paramètres.  

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```
  - Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes ; utilisez la forme **no** de la commande pour désactiver l'option :
    - **enforce-registration** : applique l'enregistrement avant que les appels ne puissent être placés.

- **message-ID max** *hex\_value* : définit l’ID maximal de message de station SCCP autorisé. L’ID du message est en hexadécimal et le maximum par défaut est 0x181.
- **rtp-conformance** [**enforce-payloadtype**] : vérifie les paquets RTP circulant dans les passages pour vérifier la conformité du protocole. Le mot-clé facultatif **enforce-payloadtype** applique le type de charge utile pour qu’il soit audio ou vidéo en fonction de l’échange de signalisation.
- **sccp-prefix-len** {**max** | **min**} *length* : définit la valeur de longueur maximale ou minimale du préfixe SCCP autorisée. Entrez la commande deux fois pour définir une valeur minimale et maximale. Le minimum par défaut est 4, et il n’y a pas de maximum par défaut.
- **timeout** {**media** | **signaling**} *time* : définit les délais d’expiration pour les connexions du support et de la signalisation (au format hh:mm:ss). Pour n’avoir aucun délai d’expiration, spécifiez 0 pour le nombre. Le délai d’expiration de support par défaut est de 5 minutes et le délai d’expiration de signalisation par défaut est d’une heure.

### Exemple

L’exemple suivant montre comment définir une liste des politiques d’inspection SCCP.

```
hostname(config)# policy-map type inspect skinny skinny-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enforce-registration
hostname(config-pmap-p)# match message-id range 200 300
hostname(config-pmap-p)# drop log
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect skinny skinny-map
hostname(config)# service-policy global_policy global
```

### 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 270.

## 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 sténopés sont dupliqués. Cependant, l'ID de transaction n'est pas répliqué sur les nœuds. Dans le cas où un nœud tombe en panne après avoir reçu une demande STUN et qu'un autre nœud a reçu la réponse STUN, la réponse STUN sera abandonnée.



#### 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 270.

## 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).<br><br>Nous n'avons pas modifié de commandes.                                                                                                                                                  |
| 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.<br><br>Nous avons ajouté la commande de paramètre <b>trust-verification-server</b> .                                 |
| 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.<br><br>Nous n'avons pas modifié de commandes. |



| Nom de la caractéristique                                                                                                                      | Versions | Renseignements sur les fonctionnalités                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prise en charge de l'inspection SIP dans la mise en grappe d'ASA                                                                               | 9.4(1)   | <p>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.</p> <p>Nous avons introduit la commande suivante : <b>show cluster service-policy</b>.</p> |
| La prise en charge de l'inspection SIP pour le mandataire téléphonique et le mandataire UC-IME a été supprimée.                                | 9.4(1)   | <p>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.</p> <p>Nous avons supprimé les commandes suivantes : <b>phone-proxy</b>, <b>uc-ime</b>. Nous avons supprimé les mots-clés <b>phone-proxy</b> et <b>uc-time</b> de la commande <b>inspect sip</b>.</p>          |
| Prise en charge de l'inspection H.323 pour le message H.255 FACILITY entrant avant le message H.225 SETUP pour la compatibilité avec H.460.18. | 9.6(1)   | <p>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.</p> <p>Nous avons introduit la commande suivante : <b>early-message</b>.</p>                                                                                      |
| Inspection STUN (Session Traversal Utilities for NAT)                                                                                          | 9.6(2)   | <p>Vous pouvez désormais inspecter le trafic STUN pour les applications WebRTC, y compris Cisco Spark. L'inspection ouvre les trous d'épingle nécessaires au trafic de retour.</p> <p>Nous avons ajouté ou modifié les commandes suivantes : <b>inspect stun</b>, <b>show asp drop</b>, <b>show conn detail</b>, <b>show service-policy inspect stun</b>.</p>                                                |
| Prise en charge de TLSv1.2 dans le mandataire TLS et Cisco Unified Communications Manager 10.5.2.                                              | 9.7(1)   | <p>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 <b>client cipher-suite</b>.</p> <p>Nous avons modifié les commandes suivantes : <b>client cipher-suite</b>.</p>          |
| Le serveur mandataire TLS est obsolète pour l'inspection SCCP (Skinny).                                                                        | 9.13(1)  | <p>Le mot clé <b>tls-proxy</b> et la prise en charge de l'inspection chiffrée SCCP/Skinny sont désormais obsolètes. Le mot clé sera supprimé de la commande <b>inspect skinny</b> dans une version ultérieure.</p>                                                                                                                                                                                           |
| La prise en charge du proxy TLS a été supprimée pour l'inspection SCCP (Skinny).                                                               | 9.14(1)  | <p>Le mot-clé <b>tls-proxy</b> et la prise en charge de l'inspection chiffrée SCCP/Skinny ont été supprimés.</p>                                                                                                                                                                                                                                                                                             |

| Nom de la caractéristique                                                        | Versions | Renseignements sur les fonctionnalités                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| La liste des politiques d'inspection SIP par défaut abandonne le trafic non SIP. | 9.16(1)  | <p>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.</p> <p>Nous avons modifié la liste des politiques SIP par défaut pour inclure la commande <b>no traffic-non-sip</b>.</p> |



## 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 261.

- [Aperçu de l'inspection du réseau mobile](#), à la page 353
- [Licences pour l'inspection des protocoles de réseau mobile](#), à la page 360
- [Valeurs par défaut pour l'inspection GTP](#), à la page 361
- [Configurer l'inspection du réseau mobile](#), à la page 361
- [Surveillance de l'inspection du réseau mobile](#), à la page 394
- [Historique de l'inspection du réseau mobile](#), à la page 398

## 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.

## Aperçu de l'inspection GTP

Le protocole de tunnellation 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 tunnellation pour acheminer les paquets de données des utilisateurs.

Les réseaux des fournisseurs de services utilisent GTP pour tunneller 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. Utilisez la commande **logging timestamp**.

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 362.

## 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.

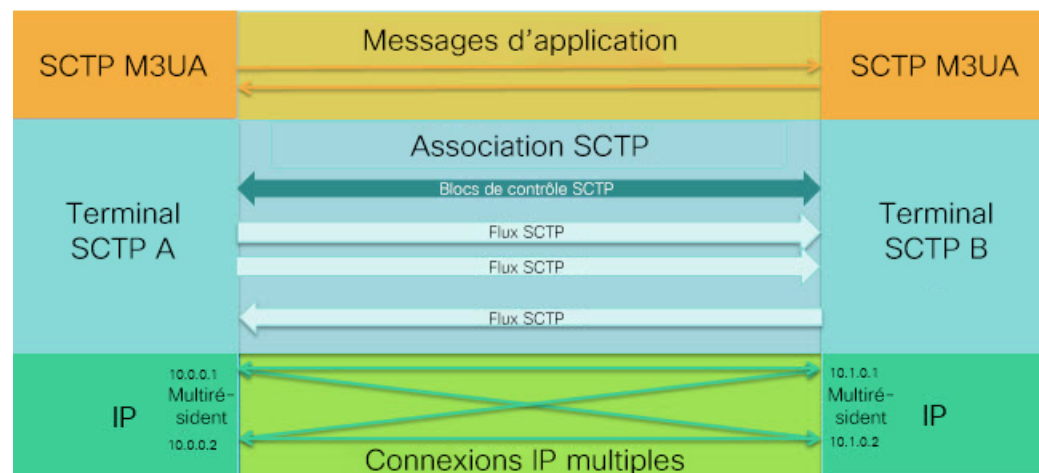
## Inspection et contrôle d'accès SCTP (Stream Control Transmission Protocol)

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 42 : 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.

Les sections suivantes décrivent plus en détail les services disponibles pour le trafic SCTP.

## 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.
- Balises 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 cartes de classes de trafic spécifiques \(tous les services\)](#), à la page 427.

## 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 12](#)
- [Ajoutez une ACE étendue pour la correspondance basée sur le port, à la page 36](#)

## 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 renverra 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 présente 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 une AVP personnalisée 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 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.

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 SGSN, 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 SGSN 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 SGSN 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
- Diameter

- M3UA

| Modèle                          | Exigence de licence                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| ASA virtuel, (tous les modèles) | Carrier (exploitant) licence (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 tunnellation 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 362.](#)
- Étape 2** (Facultatif) [Configurer une liste des politiques d'inspection SCTP, à la page 367.](#)
- Étape 3** (Facultatif) [Configurer une liste des politiques d'inspection Diameter, à la page 368.](#)
- 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 373.](#)
- 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 374](#)
- Étape 5** (Facultatif) [Configurer une liste des politiques d'inspection M3UA, à la page 385](#)
- Étape 6** [Configurer la politique de service d'inspection de réseau mobile, à la page 389.](#)
- Étape 7** (Facultatif) [Configurer l'inspection de comptabilité RADIUS, à la page 391.](#)
- 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** Créer une liste des politiques d'inspection GTP : **policy-map type inspect gtp *policy\_map\_name***
- Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.
- Étape 2** (Facultatif) Ajoutez une description à la liste des politiques : **description *string***
- Étape 3** Pour appliquer les actions au trafic correspondant, procédez comme suit.
- Précisez le trafic pour lequel vous souhaitez effectuer des actions à l'aide de l'une des commandes **match** suivantes. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.
    - match [not] apn regex {*regex\_name* | class *class\_name*}** : correspond au nom du point d'accès (APN) avec l'expression régulière ou la liste d'expressions régulières spécifiée.

- **match [not] message {v1 | v2} id {message\_id | range message\_id\_1 message\_id\_2}** : correspond à l'ID du message, qui peut être compris entre 1 et 255. Vous pouvez spécifier un ID unique ou une plage d'ID. Vous devez préciser si le message est destiné à GTPv0/1 (**v1**) ou GTPv2 (**v2**).
  - **match [not] message length min bytes max bytes** : correspond aux messages dans lesquels la longueur de la charge utile UDP (en-tête GTP plus le reste du message) est comprise entre les valeurs minimales et maximales, de 1 à 65 536.
  - **match [not] msisdn regex {regex\_name | class class\_name}** : 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.
  - **match [not] selection-mode mode\_value** : correspond à l'élément d'information du mode de sélection dans la demande de création d'un contexte PDP. 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.
  - **match [not] version {version\_id | range version\_id\_1 version\_id\_2}** : correspond à la version GTP, qui peut être comprise entre 0 et 255. Vous pouvez spécifier une version unique ou une plage de versions.
- b) Précisez l'action que vous souhaitez effectuer sur le trafic correspondant en saisissant l'une des commandes suivantes :
- **drop [log]** : abandonne tous les paquets qui correspondent. Ajoutez le mot-clé **log** pour envoyer également un message de journal système.
  - **rate-limit message\_rate** : limite le débit des messages. Cette option est disponible uniquement avec **message id**.

Vous pouvez spécifier plusieurs commandes **match** dans la liste des politiques. Pour en savoir plus sur l'ordre des commandes **match**, consultez [Comment plusieurs classes de trafic sont gérées, à la page 262](#).

#### Étape 4

Pour configurer les paramètres qui influent sur le moteur d'inspection, procédez comme suit :

- a) Entrez en mode de configuration des paramètres :

```
hostname(config-pmap) # parameters
hostname(config-pmap-p) #
```

- b) Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option :

- **anti-replay [window\_size]** : activez l'anti-replay en spécifiant une fenêtre glissante pour les messages GTP-U. La taille de la fenêtre coulissante est en nombre de messages et peut être de 128, 256, 512

ou 1024. Si vous ne spécifiez pas de taille, vous obtenez la valeur par défaut, 512. À mesure que des messages valides apparaissent, 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.

- **permit errors** : autorise 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.
- **request-queue max\_requests** : définit le nombre maximal de requêtes GTP qui seront mises en file d'attente en attente d'une réponse. Par défaut, c'est 200. Lorsque la limite est atteinte et qu'une nouvelle demande arrive, la demande qui est dans la file d'attente depuis le plus longtemps est supprimée. Les messages d'indication d'erreur, de version non prise en charge et d'accusé de réception de contexte SGSN ne sont pas considérés comme des demandes et n'entrent pas dans la file d'attente de demande pour attendre une réponse.
- **tunnel-limit max\_tunnels** : définit 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 que le nombre de tunnels spécifié par cette commande sera atteint.
- **timeout {endpoint | pdp-context | request | signaling | t3-response | tunnel} time** : définit le délai d'inactivité pour le service spécifié (au format hh:mm:ss). Pour n'avoir aucun délai d'expiration, spécifiez 0 pour le nombre. Saisissez la commande séparément pour chaque délai d'expiration.
  - **endpoint** : la période maximale d'inactivité avant le retrait d'un terminal GTP.
  - **pdp-context** : la période maximale d'inactivité avant la suppression du contexte PDP pour une session GTP. Dans GTPv2, il s'agit du contexte de support.
  - **request** : la 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.
  - **signaling** : la période maximale d'inactivité avant la suppression de la signalisation GTP.
  - **t3-response** : le temps d'attente maximal pour une réponse avant le retrait de la connexion.
  - **tunnel** : la période maximale d'inactivité du tunnel GTP avant son démontage.

## Étape 5

Tout en étant toujours en mode de configuration des paramètres, configurez la vérification GTP-U des paquets IP et l'anti-usurpation d'adresse.

**gtp-u-header-check [anti-spoofing [gtpv2-dhcp-bypass | gtpv2-dhcp-drop]]**

Sans mots clés, cette commande vérifie si la charge utile interne d'un paquet de données GTP est un paquet IP valide et abandonne le paquet s'il a un en-tête non IP.

Si vous incluez le mot-clé **anti-spoofing**, le système vérifie également si 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 abandonne le message GTP-U si les adresses IP ne correspondent pas. 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 6

Tout en étant toujours en mode de configuration des paramètres, configurez le filtrage de préfixe IMSI, si vous le souhaitez :

**mcc** *country\_code* **mnc** *network\_code*

**drop** **mcc** *country\_code* **mnc** *network\_code*

Vous pouvez entrer la commande autant de fois que nécessaire pour spécifier toutes les paires MCC/MNC ciblées, mais toutes les commandes dans la liste des politiques doivent être **mcc** ou **drop mcc**. Vous ne pouvez pas combiner ces commandes.

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 la commande :

- **mcc** command : le paquet est abandonné s'il ne correspond pas.
- **drop mcc** command : le paquet est abandonné s'il correspond.

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 7

Tout en étant toujours en mode de configuration des paramètres, activez la journalisation de l'emplacement, si vous le souhaitez.

**location-logging** [**cell-id**]

Journaliser 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).

Précisez le paramètre **cell-id** si vous souhaitez que les messages du journal incluent l'ID de cellule dans lequel 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).

## Étape 8

Tout en étant toujours en mode de configuration des paramètres, configurez le regroupement GSN ou PGW, si vous le souhaitez.

**permit-response to-object-group** *SGSN-SGW\_name* **from-object-group** *GSN-PGW\_pool*

Lorsque l'ASA effectue l'inspection GTP, l'ASA abandonne par défaut les réponses GTP des GSN ou PGW qui n'ont pas été spécifiées dans la demande GTP. Cette situation se produit lorsque vous utilisez l'équilibrage de charge entre un ensemble de GSN ou de PGW pour assurer l'efficacité et l'évolutivité de GPRS.

Pour configurer la mise en 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 spécifiez-le dans le paramètre **from-object-group**. De même, créez un groupe d'objets réseau pour le SGSN/SGW et sélectionnez-le dans le paramètre **to-object-group**. 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.

### Exemple :

Voici un exemple de mise en regroupement GSN/PGW. Un réseau entier de classe C est défini comme le pool GSN/PGW, mais vous pouvez identifier plusieurs adresses IP individuelles, une par commande **network-object**, au lieu d'identifier des réseaux entiers. L'exemple modifie ensuite une liste d'inspection GTP pour autoriser les réponses de l'ensemble au SGSN/SgW.

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.100.0 255.255.255.0
hostname(config)# object-group network sgsn32
hostname(config-network)# network-object host 192.168.50.100

hostname(config)# policy-map type inspect gtp gtp-policy
hostname(config-pmap)# parameters
hostname(config-pmap-p)# permit-response to-object-group sgsn32
from-object-group gsnpool32
```

### Exemple

L'exemple suivant montre comment limiter le nombre de tunnels dans le réseau :

```
hostname(config)# policy-map type inspect gtp gmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# tunnel-limit 3000

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect gtp gmap

hostname(config)# service-policy global_policy global
```

### 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 389.



## 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 carte de politique 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

Créer une liste des politiques d'inspection Sctp : **policy-map type inspect sctp policy\_map\_name**

Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration de liste des politiques.

#### Étape 2

(Facultatif) Ajoutez une description à la liste des politiques : **description string**

#### Étape 3

Abandonnez, limitez le débit ou journalisez le trafic en fonction du PPID dans les fragments de données Sctp.

a) Identifiez le trafic en fonction du PPID.

**match [not] ppid ppid\_1 [ppid\_2]**

Où *ppid\_1* est le numéro de PPID (0 à 4294967295) ou le nom (consulter l'aide de l'interface de ligne de commande pour les noms disponibles). Vous pouvez inclure un deuxième PPID (plus élevé), *ppid\_2*, pour spécifier une plage de PPID. Utilisez **match not ppid** pour identifier le trafic qui ne correspond pas au PPID ou à la plage.

Pour obtenir la liste actuelle des PPID Sctp, consultez

<http://www.iana.org/assignments/sctp-parameters/sctp-parameters.xhtml#sctp-parameters-25>

b) Précisez l'action à effectuer sur les paquets correspondants.

- **drop** : abandonne et journalise tous les paquets qui correspondent.
- **log** : envoie un message de journal système.
- **rate-limit rate** : limite le débit des messages. Le débit est en kilobits par seconde (kbps).

c) Répétez le processus jusqu'à ce que vous identifiiez tous les PPID que vous souhaitez gérer sélectivement.

### Exemple

L'exemple suivant crée une carte de politiques d'inspection qui supprimera les PPID non attribués (non attribués au moment où cet exemple a été écrit), les PPID de limite de débit 32 à 40 et enregistrera

le PPID de Diameter. La politique de service applique l'inspection à la classe `inspection_default`, qui correspond à tout le trafic SCTP.

```
policy-map type inspect sctp sctp-pmap
 match ppid 58 4294967295
 drop
 match ppid 26
 drop
 match ppid 49
 drop
 match ppid 32 40
 rate-limit 1000
 match ppid diameter
 log

policy-map global_policy
 class inspection_default
 inspect sctp sctp-pmap
 !
service-policy global_policy global
```

### 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 389.

## 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-parameters/aaa-parameters.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.

### 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 classe d'expression régulière.

### Procédure

**Étape 1** (Facultatif) Créez une carte de trafic d'inspection Diameter en procédant comme suit.

Une carte de trafic regroupe plusieurs correspondances de trafic. Vous pouvez également identifier les commandes **match** 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 la

carte de trafic vous permet de créer des critères de correspondance plus complexes et que vous pouvez réutiliser les cartes de trafic.

Pour spécifier le trafic qui ne doit pas correspondre à la carte de classe, utilisez la commande **match not**. Par exemple, si la commande **match not** spécifie la chaîne « example.com », tout trafic qui inclut « example.com » ne correspond pas à la carte de trafic.

Pour le trafic que vous identifiez dans cette carte de trafic, vous spécifiez les actions à prendre sur le trafic dans la liste des politiques d'inspection.

Si vous souhaitez effectuer des actions différentes pour chaque commande, **match**, vous devez identifier le trafic directement dans la liste des politiques.

- a) Créez la carte de trafic : **class-map type inspect diameter [match-all | match-any] class\_map\_name**

Où *class\_map\_name* est le nom de la carte de trafic. Le mot-clé **match-all** est le mot-clé par défaut et spécifie que le trafic doit correspondre à tous les critères pour correspondre à la carte de trafic. Le mot-clé **match-any** spécifie que le trafic correspond à la carte de trafic s'il correspond à au moins une instruction **match**. L'interface de ligne de commande passe en mode de configuration class-map, où vous pouvez saisir une ou plusieurs commandes **match**.

- b) (Facultatif) : Ajoutez une description à la carte de trafic : **description string**

Où *string* est la description de la carte de trafic (jusqu'à 200 caractères).

- c) Précisez le trafic sur lequel vous souhaitez effectuer des actions à l'aide de l'une des commandes **match** suivantes. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

- **match [not] application-id app\_id [app\_id\_2]** : correspond à l'identifiant de l'application, où *app\_id* est le nom ou le numéro de l'application Diameter (0 à 4294967295). 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. Utilisez l'aide de l'interface de ligne de commande pour obtenir la liste des noms d'application.

- **3gpp-rx-ts29214** (16777236)
- **3gpp-s6a** (16777251)
- **3gpp-s9** (16777267)
- **common-message** (0). Il s'agit du protocole Diameter de base.

- **match [not] command-code code [code\_2]** : correspond au code de commande, où *code* est le nom ou le numéro du code de commande Diameter (0 à 4294967295). 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, la commande suivante correspond au code de commande de demande/réponse d'échange de capacité :

```
match command-code cer-cea
```

- Faire correspondre la paire attribut-valeur (AVP).

Pour mettre en correspondance l'AVP par attribut uniquement :

**match [not] avp code [code\_2] [vendor-id id\_number]**

Pour faire correspondre un AVP en fonction de la valeur de l'attribut :

**match [not] avp code [vendor-id id\_number] value**

Lieu :

- **code** : nom ou numéro (1-4294967295) d'une paire attribut-valeur. Pour le premier code, vous pouvez spécifier le nom d'une AVP personnalisée ou d'une AVP enregistrée dans les RFC ou les spécifications techniques 3GPP et directement prise en charge dans le logiciel. Si vous souhaitez faire correspondre une plage d'AVP, spécifiez le deuxième code par numéro uniquement. Si vous souhaitez faire correspondre une AVP par sa valeur, vous ne pouvez pas spécifier de deuxième code. Consultez l'aide de l'interface de ligne de commande pour obtenir la liste des noms d'AVP.
- **vendor-id id\_number** : (facultatif) Le numéro d'ID du fournisseur doit également correspondre, de 0 à 4 294 967 295. Par exemple, l'ID du fournisseur 3GPP est 10415, l'IETF est 0.
- **value** : la partie valeur de l'AVP. Vous pouvez configurer cela uniquement si le type de données de l'AVP est pris en charge. Par exemple, vous pouvez spécifier une adresse IP pour une AVP qui a le type de données d'adresse. Voici la syntaxe spécifique de l'option de valeur pour les types de données pris en charge :

- Diameter Identity, Diameter URI, Octet String : utilisez des objets d'expression régulière ou de liste d'expressions régulières pour faire correspondre ces types de données.

{ **regex** *regex\_name* | **class** *regex\_class*}

- 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.

**date** *year month day* **time** *hh:mm:ss* **date** *year month day* **time** *hh:mm:ss*

Par exemple :

```
date 2015 feb 5 time 12:00:00 date 2015 mar 9 time 12:00:00
```

- Numérique : spécifiez une plage de chiffres :

**range** *number\_1 number\_2*

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) Saisissez **exit** pour quitter le mode de configuration de cartes de trafic.

## Étape 2

Créer une liste des politiques d'inspection : **policy-map type inspect diameter** *policy\_map\_name*

Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.

## Étape 3

(Facultatif) Ajoutez une description à la liste des politiques : **description** *chaîne*

## Étape 4

Pour appliquer les actions au trafic correspondant, procédez comme suit.

a) Précisez le trafic sur lequel vous souhaitez effectuer des actions en utilisant l'une des méthodes suivantes :

- Si vous avez créé une carte de trafic Diameter, spécifiez-la en entrant la commande suivante : **class** *class\_map\_name*
- Précisez le trafic directement dans la liste des politiques à l'aide de l'une des commandes **match** décrites pour les cartes de trafic Diameter.

b) Précisez l'action que vous souhaitez effectuer sur le trafic correspondant en saisissant l'une des commandes suivantes :

- **drop** : abandonner tous les paquets qui correspondent.
- **drop-connection** : abandonner le paquet et fermer la connexion.
- **log** : envoyer un message de journal système.

Vous pouvez spécifier plusieurs commandes **class** ou **match** dans la liste des politiques. Pour en savoir plus sur l'ordre des commandes **class** et **match**, consultez [Comment plusieurs classes de trafic sont gérées, à la page 262](#).

### Exemple :

```
hostname(config)# policy-map type inspect diameter diameter-map
hostname(config-pmap)# class diameter-class-map
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match command-code cer-cea
hostname(config-pmap-c)# log
```

## Étape 5

Pour configurer les paramètres qui influent sur le moteur d'inspection, procédez comme suit :

a) Entrez dans le mode de configuration des paramètres.

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme no de la commande pour désactiver l'option.

- **unsupported {application-id | command-code | avp} action log** : active la journalisation pour les éléments Diameter non pris en charge. Ces options précisent les ID d'application, les codes de commande et l'AVP qui ne sont pas directement pris en charge par le logiciel. La valeur par défaut

est d'autoriser les éléments sans les journaliser. Vous pouvez entrer la commande trois fois pour activer la journalisation pour tous les éléments.

- **strict-diameter {state | session}** : 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 la validation de la machine **state** ou la validation du message associé à **session**, ou les deux en saisissant la commande deux fois.

### Exemple :

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)# unsupported application-id action log
hostname(config-pmap-p)# unsupported command-code action log
hostname(config-pmap-p)# unsupported avp action log
hostname(config-pmap-p)# strict-diameter state
hostname(config-pmap-p)# strict-diameter session
```

### Exemple

L'exemple suivant montre comment enregistrer certaines applications et bloquer une adresse IP spécifique.

```
class-map type inspect diameter match-any log_app
 match application-id 3gpp-s6a
 match application-id 3gpp-s13

class-map type inspect diameter match-all block_ip
 match command-code cer-cea
 match avp host-ip-address 1.1.1.1

policy-map type inspect diameter diameter_map
 parameters
 unsupported application-id log
 class log_app
 log
 class block_ip
 drop-connection

policy-map global_policy
 class inspection_default
 inspect diameter diameter_map

service-policy global_policy global
```

### 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 389.

## 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 personnalisés 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 personnalisés uniquement si vous souhaitez les utiliser dans une carte de politique d'inspection Diameter ou une carte de classes pour la correspondance d'AVP.

### Procédure

Créez une AVP Diameter personnalisée.

**diameter avp** *name code value data-type type* [**vendor-id** *id\_number*] [**description** *text*]

Lieu :

- **name** : nom de l'AVP personnalisée que vous créez, jusqu'à 32 caractères. Vous ferez référence à ce nom dans la commande `match avp` d'une liste des politiques d'inspection Diameter ou d'une carte de trafic.
- **code value** : valeur du code AVP personnalisée, 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** : le type de données de l'AVP. Vous pouvez définir les types d'AVP suivants. Si la nouvelle AVP est d'un type différent, vous ne pouvez pas créer d'AVP personnalisée pour celle-ci.
  - **address** : pour les adresses IP.
  - **diameter-identity** : données d'identité de diamètre.
  - **diameter-uri** : Identificateur de ressource uniforme (URI) Diameter.
  - **float32** : nombre à virgule flottante 32 bits.
  - **float64** : nombre à virgule flottante 64 bits.
  - **int32** : nombre entier de 32 bits.
  - **int64** : nombre entier de 64 bits.
  - **octetstring** : chaîne d'octets.
  - **time** : valeur du temps.
  - **uint32** : entier non signé de 32 bits.
  - **uint64** : entier non signé 64 bits.
- **vendor-id id\_number**—(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** *texte* : (facultatif) Une description de l'AVP, jusqu'à 80 caractères. Placez la description entre guillemets si vous incluez des espaces.

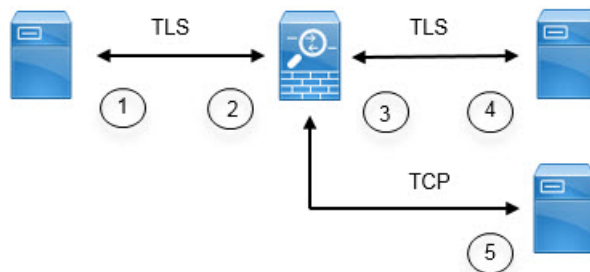
## Inspection des sessions Diameter chiffrées

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 43 : Inspection TLS Diameter**



|   |                                                                                                                                                                                                                                                   |   |                                                                                                                                                                                                                                                  |
|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Client TLS Diameter (MME) <ul style="list-style-type: none"> <li>• Certificat d'identité du client</li> <li>• Certificat d'autorité de certification utilisé pour signer le certificat d'identité du serveur proxy TLS ASA</li> </ul>             | 2 | Serveur proxy TLS ASA <ul style="list-style-type: none"> <li>• Certificat d'identité du serveur</li> <li>• Certificat d'autorité de certification utilisé pour signer le certificat d'identité du client TLS Diameter</li> </ul>                 |
| 3 | Client proxy TLS ASA <ul style="list-style-type: none"> <li>• Certificat d'identité du client (statique ou LDC)</li> <li>• Certificat d'autorité de certification utilisé pour signer le certificat d'identité du serveur TLS Diameter</li> </ul> | 4 | Serveur TLS Diameter (proxy complet) <ul style="list-style-type: none"> <li>• Certificat d'identité du serveur</li> <li>• Certificat d'autorité de certification utilisé pour signer le certificat d'identité du client proxy TLS ASA</li> </ul> |



|   |                                          |   |   |
|---|------------------------------------------|---|---|
| 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 différenciels 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 différenciels 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 différenciels 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 d'approbation de 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.

## 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) Créez le point de confiance pour le client Diameter.

Dans cet exemple, **enrollment terminal** indique que vous collerez le certificat dans l'interface de ligne de commande. Le point de confiance est appelé **diameter-clients**.

```
ciscoasa(config)# crypto ca trustpoint diameter-clients
ciscoasa(ca-trustpoint)# revocation-check none
ciscoasa(ca-trustpoint)# enrollment terminal
```

- b) Ajoutez le certificat.

```
ciscoasa(config)# crypto ca authenticate diameter-clients
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[certificate data omitted]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

### 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) Importez le certificat au format pkcs12.

Dans l'exemple suivant, **tls-proxy-server-tp** est le nom du point de confiance et **"123"** est la phrase secrète de déchiffrement. Utilisez votre propre nom de point de confiance et votre phrase d'accès.

```
ciscoasa (config)# crypto ca import tls-proxy-server-tp pkcs12 "123"

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[PKCS12 data omitted]

quit

INFO: Import PKCS12 operation completed successfully

ciscoasa (config)#
```

- b) Configurez le point de confiance.

```
ciscoasa(config)# crypto ca trustpoint tls-proxy-server-tp
ciscoasa(ca-trustpoint)# revocation-check none
```

## 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 d'approbation de serveur avec les clients Diameter, à la page 375](#)), 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

Importez le certificat d'autorité de certification utilisé pour signer le certificat du serveur Diameter dans un point de confiance ASA.

Cette étape permet à l'ASA de faire confiance au serveur Diameter.

- a) Créez le point de confiance pour le serveur Diameter.

Dans cet exemple, **enrollment terminal** indique que vous collerez le certificat dans l'interface de ligne de commande. Vous pouvez également utiliser l'URL d'inscription pour spécifier l'inscription automatique (SCEP) auprès de l'autorité de certification. Le point de confiance est appelé **diameter-server**.

```
ciscoasa(config)# crypto ca trustpoint diameter-server
ciscoasa(ca-trustpoint)# revocation-check none
ciscoasa(ca-trustpoint)# enrollment terminal
```

- b) Ajoutez le certificat.

```
ciscoasa(config)# crypto ca authenticate diameter-server
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVCqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[certificate data omitted]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qtkQ==
```

```
quit
```

```
INFO: Certificate has the following attributes:
Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
```

```
% Certificate successfully imported
```

## Étape 2

Importez le certificat et créez un point de confiance pour le certificat d'identité du client et la paire de clés du serveur proxy ASA.

Cette étape permet au serveur Diameter de faire confiance à l'ASA.

- a) Importez le certificat au format pkcs12.

Dans l'exemple suivant, **tls-proxy-client-tp** est le nom du point de confiance et **"123"** est la phrase secrète de déchiffrement. Utilisez votre propre nom de point de confiance et votre phrase d'accès.

```
ciscoasa (config)# crypto ca import tls-proxy-client-tp pkcs12 "123"
```

```
Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[PKCS12 data omitted]
```

```
quit
```

```
INFO: Import PKCS12 operation completed successfully
```

```
ciscoasa (config)#
```

- b) Configurez le point de confiance.

```
ciscoasa(config)# crypto ca trustpoint tls-proxy-client-tp
ciscoasa(ca-trustpoint)# revocation-check none
```

## Étape 3

Configurez le proxy TLS.

- a) Nommez le serveur proxy TLS et entrez le mode de configuration du serveur proxy TLS.

```
tls-proxy nom
```

- b) Identifiez le point de confiance utilisé lorsque l'ASA agit en tant que proxy par rapport aux clients Diameter.

```
server trust-point trustpoint_name
```

### Remarque

À des fins de test, ou si vous êtes certain de pouvoir faire confiance aux clients Diameter, vous pouvez ignorer cette étape et inclure la commande **no server authenticate-client** dans la configuration du proxy TLS.

- c) Identifiez le point de confiance utilisé lorsque l'ASA agit en tant que client proxy par rapport au serveur Diameter.

```
client trust-point name
```

- d) (Facultatif) Définissez les chiffrements que le client peut utiliser.

**client cipher-suite** *cipher-list*

Où *cipher-list* peut inclure une combinaison des éléments suivants :

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

Séparez plusieurs options par des espaces.

Si vous ne définissez pas les chiffrements que le proxy TLS peut utiliser, le proxy utilise la suite de chiffrement globale définie par la commande **ssl cipher**. 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 la commande **client cipher-suite** uniquement si vous souhaitez utiliser une suite différente de celle généralement disponible sur l'ASA.

Pour définir la version TLS minimale pour toutes les connexions client SSL sur l'ASA, consultez la commande **ssl client-version**. La valeur par défaut est TLS v1.0.

- e) (Facultatif) Définissez les chiffrements que le serveur peut utiliser.

**server cipher-suite** *cipher-list*

Où *cipher-list* peut inclure une combinaison des éléments suivants :

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

Séparez plusieurs options par des espaces.

Si vous ne définissez pas les chiffrements que le proxy TLS peut utiliser, le proxy utilise la suite de chiffrement globale définie par la commande **ssl cipher**. 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 la commande **server cipher-suite** uniquement si vous souhaitez utiliser une suite différente de celle généralement disponible sur l'ASA.

Pour définir la version TLS minimale pour toutes les connexions de serveur SSL sur l'ASA, consultez la commande **ssl server-version**. La valeur par défaut est TLS v1.0.

**Exemple :**

```
ciscoasa(config)# tls-proxy diameter-tls-static-proxy
ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp
```

```
ciscoasa(config-tlsp)# client trust-point tls-proxy-client-tp
```

### 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 389.

## 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 [Configurer la relation d'approbation de serveur avec les clients Diameter](#), à la page 375), 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 377, 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

Importez le certificat d'autorité de certification utilisé pour signer le certificat du serveur Diameter dans un point de confiance ASA.

Cette étape permet à l'ASA de faire confiance au serveur Diameter.

- Créez le point de confiance pour le serveur Diameter.

Dans cet exemple, **enrollment terminal** indique que vous collerez le certificat dans l'interface de ligne de commande. Vous pouvez également utiliser l'URL d'inscription pour spécifier l'inscription automatique (SCEP) auprès de l'autorité de certification. Le point de confiance est appelé **diameter-server**.

```
ciscoasa(config)# crypto ca trustpoint diameter-server
ciscoasa(ca-trustpoint)# revocation-check none
ciscoasa(ca-trustpoint)# enrollment terminal
```

- Ajoutez le certificat.

```
ciscoasa(config)# crypto ca authenticate diameter-server
```

```

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVCqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[certificate data omitted]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported

```

## Étape 2 Créez l'autorité de certification locale pour signer les certificats dynamiques locaux (LDC).

- a) Créez une paire de clés RSA pour le point de confiance.

Dans cet exemple, le nom de la paire de clés est `ldc-signer-key`.

```

ciscoasa(config)# crypto key generate rsa label ldc-signer-key
INFO: The name for the keys will be: ldc-signer-key
Keypair generation process
ciscoasa(config)#

```

- b) Créez le point de confiance de l'émetteur LDC.

Dans cet exemple, le nom du point de confiance est **ldc-server**, la paire de clés créée ci-dessus est utilisée, l'inscription autosignée est spécifiée (**enrollment self**, ce qui est obligatoire) et le nom commun de l'ASA est inclus comme nom d'objet. Vérifiez si l'application Diameter a des exigences spécifiques pour le nom du sujet.

La commande **proxy-ldc-issuer** définit le rôle de l'autorité de certification locale pour que le point de confiance puisse émettre des certificats dynamiques pour le proxy TLS.

```

ciscoasa(config)# crypto ca trustpoint ldc-server
ciscoasa(ca-trustpoint)# keypair ldc-signer-key
ciscoasa(ca-trustpoint)# subject-name CN=asa3
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# proxy-ldc-issuer
ciscoasa(ca-trustpoint)# exit

```

- c) Inscrivez le point de confiance.

```

ciscoasa(config)# crypto ca enroll ldc-server

```

## Étape 3 Configurez le proxy TLS.

- a) Nommez le proxy TLS et entrez le mode de configuration du proxy TLS.

**tls-proxy** *nom*

- b) Identifiez le point de confiance utilisé lorsque l'ASA agit en tant que serveur par rapport aux clients Diameter.

**server trust-point** *trustpoint\_name*

**Remarque**

À des fins de test, ou si vous êtes certain de pouvoir faire confiance aux clients Diameter, vous pouvez ignorer cette étape et inclure la commande **no server authenticate-client** dans la configuration du proxy TLS.

- c) Identifiez le point de confiance LDC utilisé lorsque l'ASA émet des certificats dynamiques et agit en tant que client par rapport au serveur Diameter.

**client ldc issuer** *name*

- d) Identifiez la paire de clés LDC. Précisez la même clé que celle définie dans le point de confiance LDC.

**client ldc key-pair** *name*

- e) (Facultatif) Définissez les chiffrements que le client peut utiliser.

**client cipher-suite** *cipher-list*

Où *cipher-list* peut inclure une combinaison des éléments suivants :

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

Séparez plusieurs options par des espaces.

Si vous ne définissez pas les chiffrements que le proxy TLS peut utiliser, le proxy utilise la suite de chiffrement globale définie par la commande **ssl cipher**. 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 la commande **client cipher-suite** uniquement si vous souhaitez utiliser une suite différente de celle généralement disponible sur l'ASA.

Pour définir la version TLS minimale pour toutes les connexions client SSL sur l'ASA, consultez la commande **ssl client-version**. La valeur par défaut est TLS v1.0.

- f) (Facultatif) Définissez les chiffrements que le serveur peut utiliser.

**server cipher-suite** *cipher-list*

Où *cipher-list* peut inclure une combinaison des éléments suivants :

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**



Séparez plusieurs options par des espaces.

Si vous ne définissez pas les chiffrements que le proxy TLS peut utiliser, le proxy utilise la suite de chiffrement globale définie par la commande **ssl cipher**. 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 la commande **server cipher-suite** uniquement si vous souhaitez utiliser une suite différente de celle généralement disponible sur l'ASA.

Pour définir la version TLS minimale pour toutes les connexions de serveur SSL sur l'ASA, consultez la commande **ssl server-version**. La valeur par défaut est TLS v1.0.

#### Exemple :

```
ciscoasa(config)# tls-proxy diameter-tls-ldc-proxy
ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp
ciscoasa(config-tlsp)# client ldc issuer ldc-server
ciscoasa(config-tlsp)# client ldc key-pair ldc-signer-key
```

#### Étape 4

Exportez le certificat de l'autorité de certification LDC et importez-le dans le serveur Diameter.

##### a) Exportez le certificat.

Dans l'exemple suivant, le point de confiance de LDC est ldc-server ; spécifiez votre propre nom de point de confiance LDC.

```
ciscoasa(config)# crypto ca export ldc-server identity-certificate
-----BEGIN CERTIFICATE-----
MIIDbDCCAlSgAwIBAgIQfWQvGFpj7hCCB49+ks4CjANBgkqhkiG9w0BAQUFADAT
MREwDwYDVQQDEwhIdW5ueUJlZTAeFw0xMzA2MjUwMTE5MzJaFw00ODA2MjUwMTI5
...[data omitted]...
1JZ48NoI64RqfGC/KHUsOQ==
-----END CERTIFICATE-----
```

##### b) Copiez les données de certificat et enregistrez-les dans un fichier.

Vous pouvez maintenant l'importer 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 389.

## Configurer le serveur proxy 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 d'approbation de serveur avec les clients Diameter, à la page 375](#).

## Procédure

### Étape 1

Configurez le serveur proxy TLS avec le déchargement TLS.

- a) Nommez le serveur proxy TLS et entrez le mode de configuration du serveur proxy TLS.

**tls-proxy** *nom*

- b) Identifiez le point de confiance utilisé lorsque l'ASA agit en tant que serveur par rapport aux clients Diameter.

**server trust-point** *trustpoint\_name*

#### Remarque

À des fins de test, ou si vous êtes certain de pouvoir faire confiance aux clients Diameter, vous pouvez ignorer cette étape et inclure la commande **no server authenticate-client** dans la configuration du proxy TLS.

- c) (Facultatif) Définissez les chiffrements que le serveur peut utiliser.

**server cipher-suite** *cipher-list*

Où *cipher-list* peut inclure une combinaison des éléments suivants :

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

Séparez plusieurs options par des espaces.

Si vous ne définissez pas les chiffrements que le proxy TLS peut utiliser, le proxy utilise la suite de chiffrement globale définie par la commande **ssl cipher**. 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 la commande **server cipher-suite** uniquement si vous souhaitez utiliser une suite différente de celle généralement disponible sur l'ASA.

Pour définir la version TLS minimale pour toutes les connexions de serveur SSL sur l'ASA, consultez la commande **ssl server-version**. La valeur par défaut est TLS v1.0.

- d) Précisez que la communication entre l'appareil de sécurité adaptable Cisco et le serveur Diameter doit se faire en texte clair. Dans cette relation, l'ASA agit en tant que client du serveur Diameter.

**client clear-text**

**Exemple :**

```
ciscoasa(config)# tls-proxy diameter-tls-offload-proxy
ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp
ciscoasa(config-tlsp)# client clear-text
```

**Étape 2**

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. Chaque règle doit :

- Effectuer une NAT d'identité statique pour l'adresse du serveur Diameter. C'est-à-dire que l'adresse IP dans l'objet doit être la même que l'adresse traduite dans la règle NAT.
- Traduire le port réel 3868, qui est le numéro de port TCP Diameter par défaut, en 5868, le numéro de port TLS Diameter par défaut.
- L'interface source doit être celle qui se connecte au serveur Diameter et l'interface de destination doit être celle qui se connecte au client Diameter.

L'exemple suivant traduit le trafic TCP sur le port 3868 entrant dans l'interface externe du serveur Diameter 10.29.29.29 vers le port 5868 sur l'interface interne.

```
ciscoasa(config)# object network diameter-client
ciscoasa(config-network-object)# host 10.29.29.29
ciscoasa(config-network-object)# nat (outside,inside) static 10.29.29.29
service tcp 3868 5868
```

**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 389.

## 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**

Créez une liste des politiques d'inspection M3UA : **policy-map type inspect m3ua** *policy\_map\_name*

Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration policy-map.

**Étape 2**

(Facultatif) Ajoutez une description à la liste des politiques : **description** *chaîne*

**Étape 3** Pour appliquer les actions au trafic correspondant, procédez comme suit.

- a) Précisez le trafic pour lequel vous souhaitez effectuer des actions à l'aide de l'une des commandes **match** suivantes. Si vous utilisez une commande **match not**, l'action est appliquée à tout trafic qui ne correspond pas au critère dans la commande **match not**.

- **match [not] message class class\_id [id message\_id]** : 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           |

- **match [not] opc code** : correspond au code de point d'origine dans le message de données, c'est-à-dire 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].
- **match [not] dpc code** : correspond au code de point de destination dans le message de données. Le code de point est au format *zone-région-sp*, comme expliqué pour **match opc**.
- **match [not] service-indicator number** : 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

b) Précisez l'action que vous souhaitez effectuer sur le trafic correspondant en saisissant l'une des commandes suivantes :

- **drop [log]** : abandonne tous les paquets qui correspondent. Vous pouvez également envoyer un message de journal système.
- **rate-limit message\_rate** : limite le débit des messages. Cette option est disponible uniquement avec **match message class**.

Vous pouvez spécifier plusieurs commandes **match** dans la liste des politiques. Pour en savoir plus sur l'ordre des commandes match, consultez [Comment plusieurs classes de trafic sont gérées, à la page 262](#).

#### Étape 4

Pour configurer les paramètres qui influent sur le moteur d'inspection, procédez comme suit :

a) Entrez en mode de configuration des paramètres :

```
hostname(config-pmap) # parameters
hostname(config-pmap-p) #
```

b) Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes; utilisez la forme **no** de la commande pour désactiver l'option :

- **message-tag-validation {dupu | error | notify}** : garantit que le contenu de certains champs est vérifié et validé pour le type de message spécifié. Les messages qui échouent à la validation sont abandonnés. La validation diffère en fonction du type de message.
  - 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.

- **ss7 variant** {ITU | ANSI | JAPAN | CHINA} : identifie la variante de SS7 utilisée dans votre réseau. 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.
- **strict-asp-state** : effectue une validation de l'état du processus du 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.
- **timeout endpoint time** : définit le délai d'inactivité pour supprimer les statistiques d'un point 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).
- **timeout session time** : définit le 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.

## Exemple

Voici un exemple de liste des politiques et de politique de service M3UA.

```
hostname(config)# policy-map type inspect m3ua m3ua-map
hostname(config-pmap)# match message class 2 id 6
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match message class 9
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match dpc 1-5-1
hostname(config-pmap-c)# drop log
hostname(config-pmap-c)# parameters
hostname(config-pmap-p)# ss7 variant ITU
hostname(config-pmap-p)# timeout endpoint 00:45:00

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect m3ua m3ua-map

hostname(config)# service-policy global_policy global
```

## 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 389.

## 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** Si nécessaire, créez une carte de trafic L3/L4 pour identifier le trafic pour lequel vous souhaitez appliquer l'inspection.

```
class-map name
 match parameter
```

**Exemple :**

```
hostname(config)# class-map mobile_class_map
hostname(config-cmap)# match access-list mobile
```

Dans la politique globale par défaut, la carte de trafic `inspection_default` est une carte de trafic spéciale qui comprend des ports par défaut pour tous les types d'inspection (**match default-inspection-traffic**). Si vous utilisez cette carte de trafic dans la politique par défaut ou pour une nouvelle politique de service, vous pouvez ignorer cette étape.

Pour en savoir plus sur la mise en correspondance des instructions, consultez [Créer une carte de trafic de couche 3/4 pour le trafic de transit, à la page 251](#).

- Étape 2** Ajoutez ou modifiez une liste des politiques qui définit les actions à entreprendre avec le trafic de la carte de trafic : **policy-map name**

**Exemple :**

```
hostname(config)# policy-map global_policy
```

Dans la configuration par défaut, la liste des politiques `global_policy` est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste `global_policy`, saisissez `global_policy` comme nom de politique.

- Étape 3** Déterminez la carte de trafic L3/L4 que vous utilisez pour l'inspection : **class name**

**Exemple :**

```
hostname(config-pmap)# class inspection_default
```

Pour modifier la politique par défaut ou pour utiliser la carte de trafic spéciale `inspection_default` dans une nouvelle politique, spécifiez **inspection\_default** pour le *nom*. Sinon, vous spécifiez la carte que vous avez créée précédemment au cours de cette procédure.

- Étape 4** Activez les inspections.

Dans les commandes suivantes, les listes des politiques d'inspection sont facultatives. Si vous avez créé l'une de ces listes pour personnaliser l'inspection, précisez leurs noms dans la commande appropriée. Pour Diameter, vous pouvez également spécifier un proxy TLS pour activer l'inspection des messages chiffrés.

- **inspect gtp** [*map\_name*] : pour activer l'inspection GTP.
- **inspect sctp** [*map\_name*] : pour activer l'inspection SCTP.
- **inspect diameter** [*map\_name*] [**tls-proxy** *proxy\_name*] : pour activer l'inspection Diameter.

#### 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.

- **inspect m3ua** [*map\_name*] : pour activer l'inspection M3UA.

#### Exemple :

```
hostname(config-class)# inspect gtp
hostname(config-class)# inspect sctp
hostname(config-class)# inspect diameter
hostname(config-class)# inspect m3ua
```

#### Remarque

Si vous modifiez la politique globale par défaut (ou toute politique en cours d'utilisation) pour utiliser une liste des politiques d'inspection différente, vous devez supprimer l'inspection avec la version **no inspect** de la commande, puis la rajouter avec le nouveau nom de liste des politiques d'inspection. Par exemple, pour modifier la liste des politiques pour GTP :

```
hostname(config-class)# no inspect gtp
hostname(config-class)# inspect gtp gtp-map
```

### Étape 5

Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée *global\_policy*), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

**service-policy** *polycymap\_name* {**global** | **interface** *interface\_name*}

#### Exemple :

```
hostname(config)# service-policy global_policy global
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces, et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.



## 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 391.  
**Étape 2** Configurer la politique de service d'inspection de comptabilité RADIUS, à la page 392.

## Configurer une liste des politiques d'inspection de comptabilité RADIUS

Vous devez créer une carte de politique d'inspection de comptabilité RADIUS pour configurer les attributs nécessaires à l'inspection.

### Procédure

- Étape 1** Créez une liste des politiques d'inspection de comptabilité RADIUS : **policy-map type inspect radius-accounting policy\_map\_name**
- Où *policy\_map\_name* est le nom de la liste des politiques. L'interface de ligne de commande passe en mode de configuration de liste des politiques.
- Étape 2** (Facultatif) Ajoutez une description à la liste des politiques : **description string**
- Étape 3** Entrez dans le mode de configuration des paramètres.

```
hostname(config-pmap) # parameters
hostname(config-pmap-p) #
```

- Étape 4** Définissez un ou plusieurs paramètres. Vous pouvez définir les options suivantes ; utilisez la forme **no** de la commande pour désactiver l'option.
- **send response** : demande à l'ASA d'envoyer des messages de démarrage et d'arrêt de la demande de comptabilité à l'expéditeur de ces messages (qui sont identifiés dans la commande **host** ).
  - **enable gprs** : met en œuvre la protection contre la surfacturation 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 number** : critères supplémentaires à utiliser lors de la création d'un tableau des comptes utilisateur lors de la réception des messages de démarrage de la demande de comptabilité. 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>.

- **host ip\_address [key secret]** : l'adresse IP du serveur RADIUS ou du 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. Vous pouvez répéter cette commande pour identifier plusieurs hôtes RADIUS et GGSN. L'ASA reçoit une copie des messages de comptabilité RADIUS de ces hôtes.
- **timeout users time** : définit le délai d'inactivité pour les utilisateurs (au format hh:mm:ss). Pour n'avoir aucun délai d'expiration, spécifiez 00:00:00. La valeur par défaut est de 1 heure.

### Exemple

```
policy-map type inspect radius-accounting radius-acct-pmap
 parameters
 send response
 enable gprs
 validate-attribute 31
 host 10.2.2.2 key 123456789
 host 10.1.1.1 key 12345
 class-map type management radius-class
 match port udp eq radius-acct
 policy-map global_policy
 class radius-class
 inspect radius-accounting radius-acct-pmap
```

## 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

Créez une carte de trafic de gestion L3/L4 pour identifier le trafic auquel vous souhaitez appliquer l'inspection et identifiez le trafic correspondant.

```
class-map type management name
match {port | access-list} parameter
```

#### Exemple :

```
hostname(config)# class-map type management radius-class-map
```

```
hostname(config-cmap)# match port udp eq radius-acct
```

Dans cet exemple, la correspondance concerne le port UDP de compte Radius, qui est 1646. Vous pouvez spécifier un port différent, une plage de ports (**match port udp range number1 number2**) ou utiliser **match access-list acl\_name** et utiliser une liste de contrôle d'accès.

**Étape 2** Ajoutez ou modifiez une liste des politiques qui définit les actions à entreprendre avec le trafic de la carte de trafic : **policy-map name**

**Exemple :**

```
hostname(config)# policy-map global_policy
```

Dans la configuration par défaut, la liste des politiques `global_policy` est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste `global_policy`, saisissez `global_policy` comme nom de politique.

**Étape 3** Déterminez la carte de trafic de gestion L3/L4 que vous utilisez pour l'inspection de comptabilité RADIUS : **class name**

**Exemple :**

```
hostname(config-pmap)# class radius-class-map
```

**Étape 4** Configurer l'inspection de comptabilité RADIUS : **inspect radius-accounting [radius-accounting\_policy\_map]**

Où `radius_accounting_policy_map` est la liste des politiques d'inspection de comptabilité RADIUS que vous avez créée dans [Configurer une liste des politiques d'inspection de comptabilité RADIUS](#), à la page 391.

**Exemple :**

```
hostname(config-class)# no inspect radius-accounting
hostname(config-class)# inspect radius-accounting radius-class-map
```

#### Remarque

Si vous modifiez une politique en cours d'utilisation pour utiliser une liste des politiques d'inspection différente, vous devez supprimer l'inspection de comptabilité RADIUS avec la commande **no inspect radius-accounting**, puis l'ajouter de nouveau avec le nouveau nom de liste des politiques d'inspection.

**Étape 5** Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée `global_policy`), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

**service-policy policymap\_name {global | interface interface\_name}**

**Exemple :**

```
hostname(config)# service-policy global_policy global
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une

interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

## 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.

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_pdpmb 31 total_deleted_pdpmb 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 ssenauth146

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 ssenauth146

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 ssenauth146

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 ssenauth146

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 ssenauth146

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.

- **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.

- **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.

- **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)   | <p>L'inspection GTP peut désormais gérer GTPv2. En outre, l'inspection GTP pour toutes les versions prend désormais en charge les adresses IPv6.</p> <p>Nous avons modifié la commande <b>match message id</b> à <b>match message {v1   v2} id message_id</b>. Nous avons remplacé la commande <b>timeout gsn</b> par <b>timeout endpoint</b>. Nous avons supprimé le mot-clé <b>gsn</b> de la commande <b>clear/show service-policy inspect gtp statistics</b> ; maintenant, saisissez simplement l'ID du terminal pour voir ou effacer ces statistiques. Les commandes <b>clear/show service-policy inspect gtp request</b> et <b>pdpmcb</b> comprennent maintenant un mot-clé <b>version</b>, afin que vous puissiez afficher les informations sur une version GTP spécifique.</p> |
| Inspection SCTP                                           | 9.5(2)   | <p>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).</p> <p>Nous avons ajouté ou modifié les commandes suivantes : <b>clear conn protocol sctp</b>, <b>inspect sctp</b>, <b>matchppid</b>, <b>policy-map type inspect sctp</b>, <b>show conn protocol sctp</b>, <b>show local-host connection sctp</b>, <b>show service-policy inspect sctp</b>.</p>                                                                                                                                                                                                                                              |
| Inspection Diameter                                       | 9.5(2)   | <p>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).</p> <p>Nous avons ajouté ou modifié les commandes suivantes : <b>class-map type inspect diameter</b>, <b>diameter</b>, <b>inspect diameter</b>, <b>match</b>, <b>application-id</b>, <b>match</b>, <b>avp</b>, <b>match</b>, <b>command-code</b>, <b>policy-map type inspect diameter</b>, <b>show conn detail</b>, <b>show diameter</b>, <b>show service-policy inspect diameter</b>, <b>unsupported</b>.</p>                                                                                                                                              |
| Améliorations de l'inspection Diameter                    | 9.6(1)   | <p>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.</p> <p>Nous avons ajouté ou modifié les commandes suivantes : <b>client clear-text</b>, <b>inspect diameter</b>, <b>strict-diameter</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |



| Nom de la caractéristique                                                                                                                                                                         | Versions | Renseignements sur les fonctionnalités                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Inspection avec état SCTP en mode grappe                                                                                                                                                          | 9.6(1)   | <p>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.</p> <p>Nous n'avons pas introduit ou modifié de commandes.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Inspection de l'adaptation de l'utilisateur MTP3 (M3UA)                                                                                                                                           | 9.6(2)   | <p>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.</p> <p>Nous avons ajouté ou modifié les commandes suivantes : <b>clear service-policy inspect m3ua {drops   endpoint [IP_address]}, inspect m3ua, match dpc, match opc, match service-indicator, policy-map type inspect m3ua, show asp table classify domain inspect-m3ua, show conn detail, show service-policy inspect m3ua {drops   endpoint [IP_address]}, ss7 variant, timeout endpoint.</b></p>                                                                                                                                                                                               |
| 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)   | <p>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 trous d'épingle 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.</p> <p>Nous avons modifié la sortie de commande suivante : <b>show sctp detail.</b></p>                                                                                                       |
| Améliorations de l'inspection M3UA.                                                                                                                                                               | 9.7(1)   | <p>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.</p> <p>Nous avons ajouté ou modifié les commandes suivantes : <b>clear service-policy inspect m3ua session [assocID id], match port sctp, message-tag-validation, show service-policy inspect m3ua drop, show service-policy inspect m3ua endpoint, show service-policy inspect m3ua session, show service-policy inspect m3ua table, strict-asp-state, timeout session.</b></p> |

| Nom de la caractéristique                                                                                                                                               | Versions | Renseignements sur les fonctionnalités                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prise en charge de la définition de la suite de chiffrement SSL du serveur proxy TLS                                                                                    | 9.8(1)   | <p>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 à l'aide de la commande <b>ssl cipher</b>.</p> <p>Nous avons introduit la commande suivante : <b>server cipher-suite</b></p>                                                                                                                                                                                            |
| Améliorations de l'inspection GTP pour le filtrage des MSISDN et du mode de sélection, l'anti-relecture et la protection contre l'usurpation d'adresse de l'utilisateur | 9.10(1)  | <p>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.</p> <p>Nous avons ajouté les commandes suivantes : <b>anti-replay</b>, <b>gtp-u-header-check</b>, <b>match msisdn</b>, <b>match selection-mode</b>.</p> |
| Prise en charge de GTPv1 version 10.12.                                                                                                                                 | 9.12(1)  | <p>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.</p> <p>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.</p> <p>Nous n'avons pas ajouté ni modifié de commandes.</p>                   |
| Journalisation de la localisation pour les stations mobiles (inspection GTP).                                                                                           | 9.13(1)  | <p>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.</p> <p>Nous avons ajouté la commande suivante : <b>location-logging</b>.</p>                                                                                                                                                      |
| Prise en charge de GTPv2 et GTPv1 version 15.                                                                                                                           | 9.13(1)  | <p>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.</p> <p>Nous n'avons pas ajouté ni modifié de commandes.</p>                                                                                                                                                                                                    |

| Nom de la caractéristique                                                         | Versions | Renseignements sur les fonctionnalités                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Possibilité de spécifier les préfixes IMSI à abandonner lors de l'inspection GTP. | 9.16(1)  | <p>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.</p> <p>Nous avons ajouté la commande suivante : <b>drop mcc</b>.</p> |
| Prise en charge de Secure Firewall 3100 pour la licence d'opérateur               | 9.18(1)  | <p>La licence d'opérateur permet l'inspection des protocoles Diameter, GTP/GPRS et SCTP.</p> <p>Commandes nouvelles ou modifiées : <b>feature carrier</b></p>                                                                                                                                                                                                                                                                                                                                  |





## PARTIE **V**

# Gestion des connexions et détection des menaces

- Paramètres de connexion, à la page 405
- Qualité de service, à la page 439
- Détection des menaces, à la page 453





## 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 405](#)
- [Configurer les paramètres de connexion, à la page 406](#)
- [Supervision des connexions, à la page 433](#)
- [Historique des paramètres de connexion, à la page 434](#)

## 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.
- **La détection des connexions inactives (DCD)** : Si vous avez des connexions persistantes qui sont valides mais souvent inactives, de sorte qu'elles se ferment parce qu'elles dépassent les paramètres de délai d'inactivité, vous pouvez activer la détection des connexions inactives pour identifier les connexions inactives mais valides et les maintenir actives (en réinitialisant leurs minuteurs 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 normalisateur 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

- 
- |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Étape 1</b> | <a href="#">Configurer les délais d'expiration globaux, à la page 407</a> . 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.                                                                                                                                                                                             |
| <b>Étape 2</b> | <a href="#">Protéger les serveurs contre une attaque DoS par inondation SYN (interception de TCP), à la page 410</a> . Utilisez cette procédure pour configurer l'interception TCP.                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Étape 3</b> | <a href="#">Personnaliser le traitement anormal des paquets TCP (listes TCP, normaliseur TCP), à la page 413</a> , si vous souhaitez modifier le comportement de normalisation TCP par défaut pour des classes de trafic spécifiques.                                                                                                                                                                                                                                                                                                                                                            |
| <b>Étape 4</b> | <a href="#">Contourner les vérifications de l'état de TCP pour le routage symétrique (TCP State Bypass), à la page 417</a> , si vous disposez de ce type d'environnement de routage.                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Étape 5</b> | <a href="#">Désactiver la gestion aléatoire de la séquence TCP, à la page 420</a> , si l'aléatorisation par défaut brouille les données pour certaines connexions.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Étape 6</b> | <a href="#">Délester les flux volumineux, à la page 422</a> , si vous devez améliorer les performances dans un centre de données exigeant en informatique.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Étape 7</b> | <a href="#">Configurer les paramètres de connexion pour des cartes de classes de trafic spécifiques (tous les services), à la page 427</a> . 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. |
| <b>Étape 8</b> | <a href="#">Configurer les options TCP, à la page 432</a> , 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

---

Utilisez la commande **timeout** pour définir les délais d'expiration globaux.

Toutes les valeurs de délai d'expiration sont au format *hh:mm:ss*, avec une durée maximale de 1193:0:0 dans la plupart des cas. Utilisez la commande **clear configure timeout** pour réinitialiser tous les délais d'expiration à leurs valeurs par défaut. Si vous souhaitez réinitialiser simplement un temporisateur à la valeur par défaut, entrez la commande **timeout** pour ce paramètre avec la valeur par défaut.

Utilisez **0** pour la valeur afin de désactiver un temporisateur.

Vous pouvez configurer les délais d'expiration globaux suivants.

- **timeout conn** *hh:mm:ss* : le délai d'inactivité après lequel une connexion se ferme, entre 0:5:0 et 1193:0:0. La valeur par défaut est 1 heure (1:0:0).
- **timeout half-closed** *hh:mm:ss* : 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. **conn** La durée minimale est de 30 secondes. La valeur par défaut est 10 minutes.
- **timeout udp** *hh:mm:ss* : 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.
- **timeout icmp** *hh:mm:ss* : le délai d'inactivité pour ICMP, entre 0:0:2 et 1193:0:0. La valeur par défaut est de 2 secondes (0:0:2).
- **timeout icmp-error** *hh:mm:ss* : le délai d'inactivité avant que l'ASA ne supprime une connexion ICMP après avoir reçu un paquet de réponse d'écho ICMP, entre 0:0:0 et 0:1:0 ou la valeur **timeout 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.
- **timeout sunrpc** *hh:mm:ss* : 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.
- **timeout H323** *hh:mm:ss* : le temps d'inactivité après lequel les connexions multimédias H.245 (TCP) et H.323 (UDP) sont fermées, entre 0:0:0 et 1193:0:0. La valeur par défaut est 5 minutes (0:5:0). 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).
- **timeout h225** *hh:mm:ss* : le temps d'inactivité avant la fermeture d'une connexion de signalisation H.225. Le délai d'expiration par défaut pour H.225 est de 1 heure (1:0:0). Pour fermer une connexion immédiatement après la libération de tous les appels, un délai d'expiration de 1 seconde (0:0:1) est recommandé.
- **timeout mgcp** *hh:mm:ss* : le temps d'inactivité après lequel une connexion de support MGCP est supprimée, entre 0:0:0 et 1193:0:0. La valeur par défaut est 5 minutes (0:5:0).
- **timeout mgcp-pat** *hh:mm:ss* : intervalle absolu après lequel une traduction MGCP PAT est supprimée, entre 0:0:0 et 1193:0:0. La valeur par défaut est 5 minutes (0:5:0). La durée minimale est de 30 secondes.
- **timeout sctp** *hh:mm:ss* : durée 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)
- **timeout sip** *hh:mm:ss* : durée d'inactivité jusqu'à la fermeture d'une connexion de port de signalisation SIP, entre 0:5:0 et 1193:0:0. La valeur par défaut est de 30 minutes (0:30:0).

- **timeout sip\_media** *hh:mm:ss* : le temps d'inactivité avant la fermeture d'une connexion de port média SIP. Cette durée doit être d'au moins 1 minute. La valeur par défaut est 2 minutes. Le temporisateur de médias SIP est utilisée pour les paquets de médias SIP RTP/RTCP avec SIP UDP, plutôt que le délai d'inactivité d'UDP.
- **timeout sip-provisional-media** *hh:mm:ss* : la valeur du délai d'expiration pour les connexions média provisoires SIP, entre 0:1:0 et 0:30:0. La valeur par défaut est 2 minutes.
- **timeout sip-invite** *hh:mm:ss* : le temps d'inactivité après lequel les passages pour les réponses PROVISOIRES et les traductions de médias seront fermés, entre 0:1:0 et 00:30:0. La valeur par défaut est de 3 minutes. (0:3:0).
- **timeout sip-disconnect** *hh:mm:ss* : le temps d'inactivité après lequel une session SIP est supprimée si le 200 OK n'est pas reçu pour un message CANCEL ou BYE, entre 0:0:1 et 00:10:0. La valeur par défaut est 2 minutes. (0:2:0)
- **timeout uauth** *hh:mm:ss* {**absolute** | **inactivity**} — La durée avant l'expiration du cache d'authentification et d'autorisation et l'utilisateur doit réauthentifier la connexion suivante, entre 0:0:0 et 1193:0:0. La valeur par défaut est 5 minutes (0:5:0). Le temporisateur par défaut est **absolute**; vous pouvez définir le délai d'expiration après une période d'inactivité en saisissant le mot-clé **inactivity**. La durée uauth doit être plus courte que la durée xlate. Réglez à 0 pour désactiver la mise en cache. N'utilisez pas 0 si le protocole FTP passif est utilisé pour la connexion ou si la commande virtual http est utilisée pour l'authentification Web.
- **timeout xlate** *hh:mm:ss* : le temps d'inactivité jusqu'à ce qu'un emplacement de traduction soit libéré. Cette durée doit être d'au moins 1 minute. La valeur par défaut est de 3 heures.
- **timeout pat-xlate** *hh:mm:ss* : 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.
- **timeout tcp-proxy-reassembly** *hh:mm:ss* : 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).
- **timeout floating-conn** *hh:mm:ss* : lorsqu'il existe plusieurs routes 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 permettre d'utiliser de meilleures routes, définissez le délai d'expiration à une valeur comprise entre 0:0:30 et 1193:0:0.
- **timeout conn-holddown** *hh:mm:ss* : 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 du temporisateur 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.
- **timeout igp stale-route** *hh:mm:ss* : durée pendant laquelle une route périmée est conservée 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.

## 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 proxy pour le serveur et génère une réponse SYN-ACK à la requête SYN du client à l'aide de la méthode de témoin 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

Créez une carte de trafic L3/L4 pour identifier les serveurs que vous protégez. Utilisez une correspondance de liste d'accès.

```
class-map name
match parameter
```

**Exemple :**

```
hostname(config)# access-list servers extended permit tcp any host 10.1.1.5 eq http
hostname(config)# access-list servers extended permit tcp any host 10.1.1.6 eq http
hostname(config)# class-map protected-servers
hostname(config-cmap)# match access-list servers
```

**Étape 2**

Ajoutez ou modifiez une liste des politiques qui définit les actions à entreprendre avec le trafic de la carte de trafic et identifiez cette dernière.

```
policy-map name
class name
```

**Exemple :**

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class protected-servers
```

Dans la configuration par défaut, la liste des politiques `global_policy` est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste `global_policy`, saisissez `global_policy` comme nom de politique. Pour la carte de trafic, spécifiez la classe que vous avez créée précédemment au cours de cette procédure.

**Étape 3**

Définissez les limites de connexion embryonnaires.

- **set connection embryonic-conn-max** *n* : le nombre maximal de connexions TCP embryonnaires simultanées autorisées, de 0 à 2 000 000. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions.
- **set connection per-client-embryonic-max** *n* : le nombre maximal de connexions TCP embryonnaires simultanées autorisées par client, entre 0 et 2 000 000. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions.
- **set connection syn-cookie-mss** *n* : 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'est significatif que si vous configurez **set connection embryonic-conn-max** ou **per-client-embryonic-max**.

**Exemple :**

```
hostname(config-pmap-c)# set connection embryonic-conn-max 1000
hostname(config-pmap-c)# set connection per-client-embryonic-max 50
```

**Étape 4**

Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée `global_policy`), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

```
service-policy policymap_name {global | interface interface_name}
```

**Exemple :**

```
hostname(config)# service-policy global_policy global
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

**Étape 5** Configurez les statistiques de détection des menaces pour les attaques interceptées par TCP Intercept.

**threat-detection statistics tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks\_per\_sec*] [**average-rate** *attacks\_per\_sec*]

Lieu :

- **rate-interval** *minutes* 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. Pendant cet intervalle, le système échantillonne le nombre d'attaques 30 fois.
- **burst-rate** *attacks\_per\_sec* définit le seuil pour la génération de messages syslog, entre 25 et 2147483647. La valeur par défaut est de 400 par seconde. Lorsque le débit en rafale est dépassé, le périphérique génère le message syslog 733104.
- **average-rate** *attacks\_per\_sec* 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.

**Exemple :**

```
hostname(config)# threat-detection statistics tcp-intercept
```

**Étape 6** Surveillez les résultats à l'aide des commandes suivantes :

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**] : affichez les 10 principaux serveurs protégés par l'attaque. Le mot-clé **all** affiche les données historiques 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.
- **clear threat-detection statistics tcp-intercept** : efface les statistiques d'interception TCP.

**Exemple :**

```
hostname(config)# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack Time)>

1 10.1.1.5:80 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2 10.1.1.6:80 inside 10 10 6080 10.0.0.200 (0 secs ago)
```

## 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.

La configuration par défaut comprend les paramètres suivants :

```
no check-retransmission
no checksum-verification
exceed-mss allow
queue-limit 0 timeout 4
reserved-bits allow
syn-data allow
synack-data drop
invalid-ack drop
seq-past-window drop
tcp-options range 6 7 clear
tcp-options range 9 18 clear
tcp-options range 20 255 clear
tcp-options md5 allow
tcp-options mss allow
tcp-options selective-ack allow
tcp-options timestamp allow
tcp-options window-scale allow
ttl-evasion-protection
urgent-flag clear
window-variation allow-connection
```

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

- 
- |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Étape 1</b> | Créez une liste TCP pour préciser les critères de normalisation TCP que vous souhaitez rechercher : <b>tcp-map</b><br><i>tcp-map-name</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Étape 2</b> | Configurez les critères de liste TCP en saisissant une ou plusieurs des commandes suivantes. Les valeurs par défaut sont utilisées pour toutes les commandes que vous n'entrez pas. Utilisez la forme <b>no</b> de la commande pour désactiver le paramètre. <ul style="list-style-type: none"><li>• <b>check-retransmission</b> : empêche la retransmission TCP incohérente. Cette commande est désactivée par défaut.</li><li>• <b>checksum-verification</b> : vérifie la somme de contrôle TCP, en abandonnant les paquets qui échouent la vérification. Cette commande est désactivée par défaut.</li><li>• <b>exceed-mss {allow   drop}</b> : autorisez ou abandonnez les paquets dont la longueur des données dépasse la taille maximale de segment TCP. La valeur par défaut est d'autoriser les paquets.</li><li>• <b>invalid-ack {allow   abandon}</b> : autorisez ou abandonnez les paquets avec un ACK non valide. La valeur par défaut est d'abandonner le paquet, à l'exception des connexions WAAS, où ils sont autorisés. Vous pourriez voir des ACK non valides dans les instances suivantes :</li></ul> |

- 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 le même que le 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.
- **queue-limit** *pkt\_num* [**timeout seconds**] : définit le nombre maximal de paquets hors ordre qui peuvent être mis en mémoire tampon et mis en ordre pour une connexion TCP, entre 1 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 (la commande **inspect**), et TCP check-retransmission (commande TCP map **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 commande **queue-limit** à 1 ou plus, le nombre de paquets hors ordre 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**. 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.

L'argument **timeout seconds** définit 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 l'argument *pkt\_num* est défini à 0 ; vous devez définir la limite à 1 ou au-dessus pour que le mot-clé **timeout** prenne effet.

- **reserved-bits** {**allow** | **clear** | **drop**} : set the action for reserved bits in the TCP header. Vous pouvez **autoriser** le paquet (sans modifier les bits), **effacer** les bits et autoriser le paquet, ou **abandonner** le paquet.
- **seq-past-window** {**allow** | **abandon**} : définir l'action pour les paquets qui ont des numéros de séquence de fenêtre dépassée, 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. Vous pouvez **autoriser** les paquets uniquement si la commande **queue-limit** est définie à 0 (désactivée). La valeur par défaut est d'abandonner les paquets.
- **synack-data** {**allow** | **abandon**} : autorisez ou abandonnez les paquets TCP SYNACK qui contiennent des données. La valeur par défaut est d'abandonner le paquet.
- **syn-data** {**allow** | **abandon**} : autorisez ou abandonnez les paquets SYN avec des données. La valeur par défaut est d'autoriser le paquet.
- **tcp-options** {**md5** | **mss** | **selective-ack** | **timestamp** | **window-scale** | **range lower upper**} *action* : définissez l'action pour les paquets avec options TCP. Ces options sont nommées : **md5**, **mss**, **selective-ack** (mécanisme de réception sélectif), **timestamp**, et **window-scale** (mécanisme d'évolutivité des fenêtres). Pour d'autres options, vous les spécifiez par numéro sur le mot-clé **range**, où les limites de plage sont 6-7, 9-18 et 20-255. Pour cibler une seule option par numéro, saisissez le même nombre pour la plage inférieure et supérieure. Vous pouvez saisir la commande plusieurs fois dans une liste pour définir votre politique complète. 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. Voici les actions possibles :



- **allow [multiple]** : autorisez les paquets qui contiennent une seule option de ce type. Il s'agit du réglage par défaut pour toutes les options nommées. Si vous souhaitez autoriser les paquets même s'ils contiennent plusieurs instances de l'option, ajoutez le mot-clé **multiple**. (Le mot-clé **multiple** n'est pas disponible avec **range**.)
- **maximum limit** : pour **mss** uniquement. Définissez la taille de segment maximale à la limite indiquée, de 68 à 65 535. Le MSS TCP par défaut est défini dans la commande **sysopt connection tcpmss**.
- **clear** : supprimez les options de ce type de l'en-tête et autorisez le paquet. Il s'agit du réglage par défaut pour toutes les options numérotées. Notez que l'effacement de l'option d'horodatage désactive PAWS et RTT.
- **drop** : abandon des paquets qui contiennent cette option. Cette action est disponible pour **md5** et **range** uniquement.
- **ttl-evasion-protection** : 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. La protection contre le contournement TTL est activée par défaut, de sorte que vous n'aurez qu'à saisir la forme **no** de cette commande.  
  
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.
- **urgent-flag {allow | clear}** : définit l'action pour les paquets portant l'indicateur URG. Vous pouvez **autoriser** le paquet ou **effacer** l'indicateur et autoriser le paquet. La valeur par défaut est d'effacer l'indicateur.  
  
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.
- **window-variation {allow | drop}** : autorise ou abandonne une connexion dont la taille de fenêtre a été modifiée de manière inattendue. La valeur par défaut est d'autoriser la connexion.  
  
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. Lorsque cette condition est détectée, la connexion peut être abandonnée.

### Étape 3

Appliquez la liste TCP à une classe de trafic à l'aide d'une politique de service.

- a) Définissez la classe de trafic avec une carte de classe L3/L4 et ajoutez la carte à une carte de politiques.

```
class-map name
match parameter
policy-map name
class name
```

**Exemple :**

```
hostname(config)# class-map normalization
hostname(config-cmap)# match any
hostname(config)# policy-map global_policy
hostname(config-pmap)# class normalization
```

Dans la configuration par défaut, la liste des politiques `global_policy` est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste `global_policy`, saisissez `global_policy` comme nom de politique. Pour en savoir plus sur la mise en correspondance des instructions pour les cartes de trafic, consultez [Créer une carte de trafic de couche 3/4 pour le trafic de transit](#), à la page 251.

- b) Appliquez la liste TCP : **set connection advanced-options** *tcp-map-name*

**Exemple :**

```
hostname(config-pmap-c)# set connection advanced-options tcp_map1
```

- c) Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée `global_policy`), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

**service-policy** *polycymap\_name* {**global** | **interface** *interface\_name*}

**Exemple :**

```
hostname(config)# service-policy global_policy global
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

## Exemples

Par exemple, pour autoriser les paquets d'indicateurs et de décalages urgents pour tout le trafic envoyé à la plage de ports TCP entre le port de données FTP bien connu et le port Telnet, entrez les commandes suivantes :

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config-tcp-map)# class-map urg-class
hostname(config-cmap)# match port tcp range ftp-data telnet
hostname(config-cmap)# policy-map pmap
hostname(config-pmap)# class urg-class
hostname(config-pmap-c)# set connection advanced-options tmap
hostname(config-pmap-c)# service-policy pmap global
```

## Contourner les vérifications de l'état de TCP pour le routage symétrique (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.

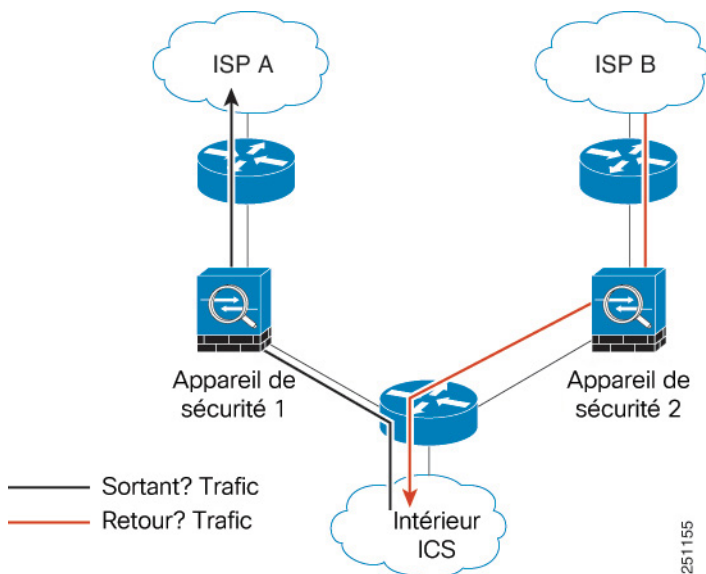
### Le problème du routage asymétrique

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 44 : 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 la 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.
- Basculement avec état

### Lignes directrices de NAT de contournement d'état TCP

Comme la session de traduction est établie séparément pour chaque ASA, 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 utilisant la commande **set connection timeout idle** pour la carte de trafic de contournement de l'état TCP. Les connexions TCP normales expirent par défaut après 60 minutes.

### Procédure

- |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Étape 1</b> | <p>Créez une carte de trafic L3/L4 pour identifier les hôtes qui nécessitent un contournement de l'état TCP. Utilisez une correspondance de liste d'accès pour identifier les hôtes source et de destination.</p> <pre>class-map name<br/>match parameter</pre> <p><b>Exemple :</b></p> <pre>hostname(config)# access-list bypass extended permit tcp host 10.1.1.1 host 10.2.2.2<br/>hostname(config)# class-map bypass-class<br/>hostname(config-cmap)# match access-list bypass</pre>                                                                                                                                                                                                                                  |
| <b>Étape 2</b> | <p>Ajoutez ou modifiez une liste des politiques qui définit les actions à entreprendre avec le trafic de la carte de trafic et identifiez cette dernière.</p> <pre>policy-map name<br/>class name</pre> <p><b>Exemple :</b></p> <pre>hostname(config)# policy-map global_policy<br/>hostname(config-pmap)# class bypass-class</pre> <p>Dans la configuration par défaut, la liste des politiques <code>global_policy</code> est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste <code>global_policy</code>, saisissez <code>global_policy</code> comme nom de politique. Pour la carte de trafic, spécifiez la classe que vous avez créée précédemment au cours de cette procédure.</p> |
| <b>Étape 3</b> | <p>Activer le contournement de l'état TCP sur la carte : <b>set connection advanced-options tcp-state-bypass</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Étape 4</b> | <p>Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée <code>global_policy</code>), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**service-policy** *polycymap\_name* {**global** | **interface** *interface\_name*}

### Exemple :

```
hostname(config)# service-policy global_policy global
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

### Exemple

Voici un exemple de configuration pour le contournement de l'état TCP :

```
hostname(config)# access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.224 any

hostname(config)# class-map tcp_bypass
hostname(config-cmap)# description "TCP traffic that bypasses stateful firewall"
hostname(config-cmap)# match access-list tcp_bypass

hostname(config-cmap)# policy-map tcp_bypass_policy
hostname(config-pmap)# class tcp_bypass
hostname(config-pmap-c)# set connection advanced-options tcp-state-bypass

hostname(config-pmap-c)# service-policy tcp_bypass_policy interface outside
```

## 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**

Créez une carte de trafic L3/L4 pour identifier le trafic dont les numéros de séquence TCP ne doivent pas être rendus aléatoires. 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.

```
class-map name
match parameter
```

**Exemple :**

```
hostname(config)# access-list preserve-sq-no extended permit tcp any host 10.2.2.2
hostname(config)# class-map no-tcp-random
hostname(config-cmap)# match access-list preserve-sq-no
```

**Étape 2**

Ajoutez ou modifiez une liste des politiques qui définit les actions à entreprendre avec le trafic de la carte de trafic et identifiez cette dernière.

```
policy-map name
class name
```

**Exemple :**

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class no-tcp-random
```

Dans la configuration par défaut, la liste des politiques `global_policy` est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste `global_policy`, saisissez `global_policy` comme nom de politique. Pour la carte de trafic, spécifiez la classe que vous avez créée précédemment au cours de cette procédure.

**Étape 3**

Désactivez la randomisation du numéro de séquence TCP sur la classe :

**set connection random-sequence-number disable**

Si vous décidez de le réactiver ultérieurement, remplacez « disable » par **enable**.

**Étape 4**

Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée `global_policy`), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

```
service-policy policymap_name {global | interface interface_name}
```

**Exemple :**

```
hostname(config)# service-policy global_policy global
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

## 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
- 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 à ASA 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.

#### **flow-offload enable**

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.

En mode contexte multiple, l'activation ou la désactivation du déchargement de flux l'active ou le désactive pour tous les contextes. Vous ne pouvez pas avoir différents paramètres par contexte.

#### Exemple :

```
ciscoasa(config)# flow-offload enable
```

WARNING: This command will take effect after the running-config is saved and the system has been rebooted.

```
ciscoasa(config)# write memory
ciscoasa(config)# reload
```

## Étape 2

Créez la règle de politique de service qui identifie le trafic admissible au déchargement.

- a) Créez une carte de trafic L3/L4 pour identifier le trafic admissible au déchargement de flux. La mise en correspondance par liste d'accès ou par port constitue généralement les options les plus courantes.

```
class-map name
match parameter
```

### Exemple :

```
hostname(config)# access-list offload permit tcp 10.1.1.0 255.255.255.224 any
hostname(config)# class-map flow_offload
hostname(config-cmap)# match access-list offload
```

- b) Ajoutez ou modifiez une liste des politiques qui définit les actions à entreprendre avec le trafic de la carte de trafic et identifiez cette dernière.

```
policy-map name
class name
```

### Exemple :

```
hostname(config)# policy-map offload_policy
hostname(config-pmap)# class flow_offload
```

Dans la configuration par défaut, la liste des politiques `global_policy` est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste `global_policy`, saisissez `global_policy` comme nom de politique. Pour la carte de trafic, spécifiez la classe que vous avez créée précédemment au cours de cette procédure.

- c) Activer le déchargement de flux sur la carte : **set connection advanced-options flow-offload**
- d) Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée `global_policy`), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

```
service-policy policymap_name {global | interface interface_name}
```

### Exemple :

```
hostname(config)# service-policy offload_policy interface outside
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

### Exemple

L'exemple suivant carte tout le trafic TCP du sous-réseau 10.1.1.0 255.255.255.224 comme admissible au déchargement et associe la politique à l'interface externe.

```
hostname(config)# access-list offload permit tcp 10.1.1.0 255.255.255.224 any
hostname(config)# class-map flow_offload
hostname(config-cmap)# match access-list offload
hostname(config)# policy-map offload_policy
hostname(config-pmap)# class flow_offload
hostname(config-pmap-c)# set connection advanced-options flow-offload
hostname(config)# service-policy offload_policy interface outside
```

## 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 désactivée.
- 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

- 
- |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Étape 1</b> | Activez le déchargement de flux IPsec.<br><b>flow-offload-ipsec</b>                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Étape 2</b> | Activez l'optimisation de sortie pour optimiser le chemin d'accès aux données afin d'améliorer les performances pour les flux de tunnel unique.<br><b>flow-offload-ipsec egress-optimization</b><br><br>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. L'optimisation de sortie n'est pas activée par défaut. |
- 

## Configurer les paramètres de connexion pour des cartes de 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'aléatorisation 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.

La commande **set connection** (pour les limites de connexion et l'aléatorisation de séquence) et les commandes **set connection timeout** sont décrites ici séparément pour chaque paramètre. Cependant, vous pouvez saisir les commandes sur une seule ligne et si vous les saisissez séparément, elles s'affichent dans la configuration comme une seule commande.

**Procédure****Étape 1**

Créez une carte de trafic L3/L4 pour identifier le trafic pour lequel vous souhaitez personnaliser les paramètres de connexion.

```
class-map name
match parameter
```

**Exemple :**

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
```

Pour en savoir plus sur la mise en correspondance des instructions, consultez [Créer une carte de trafic de couche 3/4 pour le trafic de transit, à la page 251](#).

**Étape 2** Ajoutez ou modifiez une liste des politiques qui définit les actions à entreprendre avec le trafic de la carte de trafic et identifiez cette dernière.

```
policy-map name
class name
```

**Exemple :**

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class CONNS
```

Dans la configuration par défaut, la liste des politiques `global_policy` est affectée globalement à toutes les interfaces. Si vous souhaitez modifier la liste `global_policy`, saisissez `global_policy` comme nom de politique. Pour la carte de trafic, spécifiez la classe que vous avez créée précédemment au cours de cette procédure.

**Étape 3** Définir les limites de connexion et la répartition aléatoire du numéro de séquence TCP. (Interception TCP.)

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.

- **set connection conn-max *n***—(TCP, UDP, SCTP.) Le nombre maximal de connexions simultanées autorisées, entre 0 et 2 000 000, pour l'ensemble de la classe. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions. Pour les connexions TCP, cela s'applique uniquement aux connexions établies.
  - Si deux serveurs sont configurés pour autoriser les connexions simultanées, la limite de connexion est appliquée à chaque serveur configuré séparément.
  - Étant donné que la limite est appliquée à une classe, un hôte attaquant peut utiliser toutes les connexions et n'en laisser aucune pour les autres hôtes qui correspondent à la classe.
- **set connection per-client-max *n***—(TCP, UDP, SCTP.) Le nombre maximal de connexions simultanées autorisées par client, entre 0 et 2 000 000. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions. Cette option restreint le nombre maximal de connexions simultanées autorisées pour chaque hôte correspondant à la classe. Pour les connexions TCP, cela inclut les connexions établies, à moitié ouvertes et à moitié fermées.
- **set connection embryonic-conn-max *n***—Le nombre maximal de connexions TCP embryonnaires simultanées autorisées, entre 0 et 2 000 000. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions. 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.
- **set connection per-client-embryonic-max *n***—Le nombre maximal de connexions TCP embryonnaires simultanées autorisées par client, entre 0 et 2 000 000. La valeur par défaut est 0, ce qui permet un nombre illimité de connexions.
- **set connection syn-cookie-mss *n*** : 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'est significatif que si vous configurez **set connection embryonic-conn-max** ou **per-client-embryonic-max**.

- **set connection random-sequence-number {enable | disable}** : activer ou désactiver la randomisation des numéros de séquence TCP. La répartition aléatoire est activée par défaut.

**Exemple :**

```
hostname(config-pmap-c)# set connection conn-max 256 random-sequence-number disable
```

**Étape 4**

Définissez les délais d'expiration de connexion et la détection de connexion inactive (DCD).

Les valeurs par défaut décrites ci-dessous supposent que vous n'avez pas modifié les valeurs globales par défaut pour ces comportements à l'aide de la commande **timeout** ; les valeurs globales par défaut remplacent celles décrites ici. Saisissez **0** pour désactiver le temporisateur, afin qu'une connexion n'expire jamais.

- **set connection timeout embryonic hh:mm:ss** : la période de délai d'expiration jusqu'à ce qu'une connexion TCP embryonnaire (semi-ouverte) soit fermée, entre 0:0:5 et 1 193:00:00. La valeur par défaut est 0:0:30.

- **set connection timeout idle hh:mm:ss[reset]** : la période de délai d'inactivité après laquelle une connexion établie de n'importe quel protocole se ferme, entre 0:0:1 et 1 193:0:0. La valeur par défaut est 1:0:0. Pour le trafic TCP, le mot-clé **reset** envoie une réinitialisation aux terminaux TCP lorsque la connexion expire.

Le délai d'inactivité **udp** par défaut est de 2 minutes. Le délai d'inactivité **icmp** par défaut est de 2 secondes. Le délai d'inactivité **esp** et **ha** par défaut est de 30 secondes. Pour tous les autres protocoles, le délai d'inactivité par défaut est de 2 minutes.

- **set connection timeout half-closed hh:mm:ss**—Le délai d'inactivité jusqu'à la fermeture d'une connexion à moitié fermée, entre 0:5:0 (pour la version 9.1(1) et les versions antérieures) ou 0:0:30 (pour la version 9.1(2) et versions ultérieures) 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.

- **set connection timeout dcd [retry-interval [max\_retries]]**—Activez la détection des connexions inactives (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. 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.

L'intervalle de réessai définit la durée au format *hh:mm:ss* à attendre après chaque sonde DCD non réactive avant d'envoyer une autre sonde, entre 0:0:1 et 24:0:0. La valeur par défaut est 0:0:15. *max-retries* définit le nombre de tentatives consécutives échouées pour DCD avant de déclarer la connexion comme inactive. La valeur minimale est 1 et la valeur maximale est 255. La valeur par défaut est égale à 5.

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.

**Exemple :**

```
hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0
half-closed 0:20:0 dcd
```



**Étape 5** Décrémentez le temps de vie (TTL) sur les paquets qui correspondent à la classe : **set connection decrement-ttl**

Cette commande, ainsi que la commande **icmp unreachable**, est nécessaire pour permettre un traceroute via l'ASA qui affiche l'ASA comme l'un des sauts.

**Exemple :**

```
hostname(config)# class-map global-policy
hostname(config-cmap)# match any
hostname(config-cmap)# exit
hostname(config)# policy-map global_policy
hostname(config-pmap)# class global-policy
hostname(config-pmap-c)# set connection decrement-ttl
hostname(config-pmap-c)# exit
hostname(config)# icmp unreachable rate-limit 50 burst-size 6
```

**Étape 6** Définir des options avancées.

Les options avancées sont des configurations à usage spécial qui ne sont pas nécessaires dans des circonstances normales. Vous les configurez avec la commande **set connection advanced-options**

- **set connection advanced-options tcp\_map\_name** : personnaliser le comportement du normalisateur TCP en appliquant une liste TCP. Pour de plus amples renseignements, voir [Personnaliser le traitement anormal des paquets TCP \(listes TCP, normaliseur TCP\)](#), à la page 413.
- **set connection advanced-options tcp-state-bypass** : mettre en œuvre le contournement de l'état TCP. Pour de plus amples renseignements, voir [Contourner les vérifications de l'état de TCP pour le routage symétrique \(TCP State Bypass\)](#), à la page 417.
- **set connection advanced-options sctp-state-bypass** : mettre en œuvre le contournement de l'état SCTP pour désactiver l'inspection dynamique SCTP. Pour en savoir plus, consultez [Inspection dynamique SCTP](#), à la page 355.
- **set connection advanced-options flow-offload** : (ASA sur le Châssis Firepower 4100/9300, FXOS 1.1.3 ou version ultérieure, uniquement.) Implémentation du 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 entrer la commande **flow-offload enable**, qui ne fait pas partie de la politique de service.

**Exemple :**

```
hostname(config-pmap-c)# set connection advanced-options tcp_map1
```

**Étape 7** Si vous modifiez une politique de service existante (comme la politique globale par défaut appelée `global_policy`), vous pouvez ignorer cette étape. Sinon, activez la liste des politiques sur une ou plusieurs interfaces.

**service-policy** *polycymap\_name* {**global** | **interface** *interface\_name*}

**Exemple :**

```
hostname(config)# service-policy global_policy global
```

Le mot clé **global** applique la liste des politiques à toutes les interfaces et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une

interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

### Exemple

L'exemple suivant définit les limites de connexion et les délais d'expiration pour tout le trafic :

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
hostname(config-cmap)# policy-map CONNS
hostname(config-pmap)# class CONNS
hostname(config-pmap-c)# set connection conn-max 1000 embryonic-conn-max 3000
hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0
half-closed 0:20:0 dcd
hostname(config-pmap-c)# service-policy CONNS interface outside
```

Vous pouvez entrer des commandes **set connection** avec plusieurs paramètres ou saisir chaque paramètre en tant que commande distincte. L'ASA combine les commandes en une seule ligne dans la configuration en cours d'exécution. Par exemple, si vous avez saisi les deux commandes suivantes en mode de configuration de classe :

```
hostname(config-pmap-c)# set connection conn-max 600
hostname(config-pmap-c)# set connection embryonic-conn-max 50
```

La sortie de la commande **show running-config policy-map** afficherait le résultat des deux commandes en une seule commande combinée :

```
set connection conn-max 600 embryonic-conn-max 50
```

## 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

(CLI). Configurez le comportement de réinitialisation TCP.

```
service { resetinbound [interface [interface_name] | resetoutbound [interface [interface_name]
| resetoutside }] [...]
```

- **resetinbound**. Envoie des réinitialisations TCP pour toutes les sessions TCP entrantes qui tentent de transiter par l'ASA et qui 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 touché. Lorsque cette option n'est

pas activée, l'ASA rejette silencieusement les paquets refusés. Si vous ne spécifiez pas d'interface, ce paramètre s'applique à toutes les interfaces.

- **resetoutbound.** Envoie des réinitialisations TCP pour toutes les sessions TCP sortantes qui tentent de transiter par l'ASA et qui sont refusées par l'ASA en fonction des listes d'accès ou des paramètres AAA. 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 touché. Lorsque cette option n'est pas activée, l'ASA rejette silencieusement les paquets refusés. Par défaut, cette option est activée. Vous pourriez souhaiter désactiver les réinitialisations sortantes pour réduire la charge du processeur pendant les tempêtes de trafic, par exemple.
- **resetoutside.** Active les réinitialisations pour les paquets TCP qui se terminent au niveau de 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 refusés.

Nous vous recommandons d'utiliser cette option avec la PAT de l'interface. Cette option 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.

**Étape 2** Définissez TCP MSS pour vous assurer que la taille maximale de segment TCP pour le trafic de transit ne dépasse pas la valeur que vous avez définie et que la taille maximale n'est pas inférieure à une taille spécifiée.

**sysopt connection tcpmss** [ **minimum** ] *bytes*

Sans **minimum** mot-clé. Définissez la taille maximale du segment TCP 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.

**minimum.** Remplace la taille maximale du segment pour qu'elle ne soit pas inférieure aux octets spécifiés, entre 48 et 65 535 octets. Cette fonctionnalité est désactivée par défaut (définie sur 0).

**Étape 3** Définir le délai d'attente de connexion TCP.

**sysopt connection timewait**

Utilisez cette commande pour forcer 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 pourriez vouloir utiliser cette fonctionnalité si la séquence de terminaison TCP par défaut d'une application hôte terminal est une fermeture simultanée.

**Étape 4** Définissez le nombre maximal de segments TCP non traités.

**sysopt connection tcp-max-unprocessed-seg** *segments*

Définissez 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.

## Supervision des connexions

Vous pouvez utiliser les commandes suivantes pour surveiller les connexions :

- **show conn [detail]**

Affiches des renseignements sur la connexion. Des 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 : <b>set connection advanced-options tcp-state-bypass</b> . |

| Nom de la caractéristique                                                               | Versions de plateforme | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Délai d'expiration de connexion pour tous les protocoles                                | 8.2(2)                 | <p>Le délai d'inactivité a été modifié pour s'appliquer à tous les protocoles, pas seulement au TCP.</p> <p>La commande suivante a été modifiée : <b>set connection timeout</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Délai d'expiration pour les connexions utilisant une route statique de sauvegarde       | 8.2(5)/8.4(2)          | <p>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.</p> <p>Nous avons modifié la commande suivante : <b>timeout floating-conn.</b></p> |
| Délai d'expiration configurable pour PAT xlate                                          | 8.4(3)                 | <p>Lorsqu'une xlate PAT 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.</p> <p>Nous avons introduit la commande suivante : <b>timeout pat-xlate.</b></p> <p><i>Cette fonctionnalité n'est pas disponible dans les versions 8.5(1) ou 8.6(1).</i></p>                             |
| Augmentation des limites de connexion maximales pour les règles de politique de service | 9.0(1)                 | <p>Le nombre maximal de connexions pour les règles de politique de service a été augmenté de 65 535 à 2 000 000.</p> <p>Nous avons modifié les commandes suivantes : <b>set connection conn-max, set connection embryonic-conn-max, set connection per-client-embryonic-max, set connection per-client-max.</b></p>                                                                                                                                                                                                                                                                                              |
| Réduction de la valeur minimale du délai d'expiration à moitié fermé à 30 secondes      | 9.1(2)                 | <p>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.</p> <p>Nous avons modifié les commandes suivantes : <b>set connection timeout half-closed, timeout half-closed.</b></p>                                                                                                                                                                                                                                                                   |
| Délai d'expiration de la connexion pour la convergence des routes.                      | 9.4(3)<br>9.6(2)       | <p>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.</p> <p>Nous avons ajouté la commande suivante : <b>timeout conn-holddown.</b></p>                        |

| Nom de la caractéristique                                                                          | Versions de plateforme | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Délai d'inactivité SCTP et contournement de l'état SCTP                                            | 9.5(2)                 | <p>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.</p> <p>Nous avons ajouté ou modifié les commandes suivantes : <b>timeout sctp</b>, <b>set connection advanced-options sctp-state-bypass</b>.</p>                                                                                                                                                                             |
| Décharge de flux pour l'ASA sur le Firepower 9300                                                  | 9.5(2.1)               | <p>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.</p> <p>Cette fonctionnalité nécessite FXOS 1.1.3.</p> <p>Nous avons ajouté ou modifié les commandes suivantes : <b>clear flow-offload</b>, <b>flow-offload enable</b>, <b>set-connection advanced-options flow-offload</b>, <b>show conn detail</b>, <b>show flow-offload</b>.</p> |
| Prise en charge du déchargement de flux pour l'ASA sur le Firepower 4100.                          | 9.6(1)                 | <p>Vous pouvez identifier les flux qui doivent être déchargés de l'ASA et commutés directement dans la carte réseau pour le Firepower 4100.</p> <p>Cette fonctionnalité requiert FXOS 1.1.4.</p> <p>Il n'y a aucune nouvelle commande ni écran ASDM pour cette fonctionnalité.</p>                                                                                                                                                                                                                                                      |
| Prise en charge du déchargement de flux pour les connexions de multidiffusion en mode transparent. | 9.6(2)                 | <p>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.</p> <p>Il n'y a aucune nouvelle commande ni écran ASDM pour cette fonctionnalité.</p>                                                                                                                       |

| Nom de la caractéristique                                                                                                                 | Versions de plateforme | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modifications dans la gestion des options TCP.                                                                                            | 9.6(2)                 | <p>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.</p> <p>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.</p> <p>Nous avons modifié la commande suivante : <b>timeout igp stale-route</b>.</p> |
| Délai d'expiration de route obsolète pour les protocoles de passerelle intérieure                                                         | 9.7(1)                 | <p>Vous pouvez maintenant configurer le délai d'expiration pour supprimer des routes obsolètes pour les protocoles de passerelle intérieure tels que OSPF.</p> <p>Nous avons ajouté la commande suivante : <b>timeout igp stale-route</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Délai d'expiration global pour les erreurs ICMP                                                                                           | 9.8(1)                 | <p>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.</p> <p>Nous avons ajouté la commande suivante : <b>timeout icmp-error</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Délai d'inactivité par défaut pour le contournement d'état TCP                                                                            | 9.10(1)                | <p>Le délai d'inactivité par défaut pour les connexions de contournement d'état TCP est désormais de 2 minutes au lieu de 1 heure.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 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)                | <p>Si vous activez la détection des connexions inactives (DCD), vous pouvez utiliser la commande <b>show conn detail</b> 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 <b>show conn</b> vous indique la fréquence à laquelle les points terminaux ont été sondés. En outre, DCD est désormais pris en charge dans une grappe.</p> <p>Commandes nouvelles ou modifiées : <b>show conn</b> (sortie uniquement).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Nom de la caractéristique                                                   | Versions de plateforme | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configurer la taille maximale de segment (MSS) pour les connexions amorces. | 9.16(1)                | <p>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.</p> <p>Commandes nouvelles ou modifiées : <b>set connection syn-cookie-mss</b>.</p>                                                              |
| Décharge de flux IPsec.                                                     | 9.18(1)                | <p>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.</p> <p>Nous avons ajouté les commandes suivantes : <b>clear flow-offload-ipsec</b>, <b>flow-offload-ipsec</b>, <b>show flow-offload-ipsec</b></p> |





## 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 439](#)
- [Lignes directrices relatives à la QoS, à la page 441](#)
- [Configurer QoS, à la page 442](#)
- [Surveiller la QoS, à la page 448](#)
- [Exemples de configuration pour la mise en file d'attente prioritaire et la régulation, à la page 449](#)
- [Historique QoS, à la page 451](#)

## 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 440](#) 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 440](#).

## 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. Au 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 de 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 444](#)), 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 relatives à la QoS

### Lignes directrices relatives au mode contextuel

Pris en charge en mode contexte unique uniquement Ne prend pas en charge le mode contexte multiple.

### Lignes directrices 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.

### Lignes directrices pour IPv6

Ne prend pas en charge IPv6.

### Lignes directrices 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 **class-default**.
- 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

- 
- |                |                                                                                                                   |
|----------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Étape 1</b> | Déterminer les limites de la file d'attente et de l'anneau TX pour une file d'attente prioritaire, à la page 442. |
| <b>Étape 2</b> | Configurer la file d'attente prioritaire pour une interface, à la page 444.                                       |
| <b>Étape 3</b> | Configurer une règle de service pour la mise en file d'attente prioritaire et la régulation, à la page 445.       |
- 

## 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 444](#).

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 | _____                                      | Mbit/s | x | 125                                 | = | _____              |   |                                                 |
|   | Bande passante sortante (Mbit/s ou kbit/s) |        |   |                                     |   | Nombre d'octets/ms |   |                                                 |
|   |                                            | kbit/s | x | 0,125                               | = | _____              |   |                                                 |
|   |                                            |        |   |                                     |   | Nombre d'octets/ms |   |                                                 |
| 2 | _____                                      |        | ÷ | _____                               | x | _____              | = | _____                                           |
|   | Nombre d'octets/ms de l'étape 1            |        |   | Taille moyenne des paquets (octets) |   | 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, une connexion 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 calcul des limites de l'anneau TX

|   |                                            |        |   |                                      |   |                    |   |                                           |
|---|--------------------------------------------|--------|---|--------------------------------------|---|--------------------|---|-------------------------------------------|
| 1 | _____                                      | Mbit/s | x | 125                                  | = | _____              |   |                                           |
|   | Bande passante sortante (Mbit/s ou kbit/s) |        |   |                                      |   | Nombre d'octets/ms |   |                                           |
|   |                                            | kbit/s | x | 0,125                                | = | _____              |   |                                           |
|   |                                            |        |   |                                      |   | Nombre d'octets/ms |   |                                           |
| 2 | _____                                      |        | ÷ | _____                                | x | _____              | = | _____                                     |
|   | Nombre d'octets/ms de l'étape 1            |        |   | Taille maximale des paquets (octets) |   | 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** Créez la file d'attente prioritaire pour l'interface.

**priority-queue** *interface\_name*

**Exemple :**

```
hostname(config)# priority-queue inside
```

L'argument *interface\_name* spécifie le nom de l'interface physique sur laquelle vous souhaitez activer la file d'attente prioritaire.

**Étape 2** Modifiez la taille des files d'attente prioritaires.

**queue-limit** *number\_of\_packets*

La limite de file d'attente par défaut est de 1 024 paquets. 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 se remplisse, vous pouvez utiliser la commande **queue-limit** pour augmenter la taille du tampon de file d'attente.

La limite supérieure de la plage de valeurs pour la commande **queue-limit** est déterminée dynamiquement au moment de l'exécution. Pour afficher cette limite, saisissez **file d'attente-limit ?** dans la ligne de commande. 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** 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.

**Exemple :**

```
hostname(config-priority-queue)# queue-limit 260
```

**Étape 3** Précisez la profondeur des files d'attente prioritaires.

**tx-ring-limit** *number\_of\_packets*

La limite de sonnerie tx-ring par défaut est de 511 paquets. Cette commande 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. Ce paramètre garantit que l'anneau de transmission matériel impose une quantité limitée de latence supplémentaire pour un paquet de priorité élevée.

La limite supérieure de la plage de valeurs pour la commande **tx-ring-limit** est déterminée dynamiquement au moment de l'exécution. Pour afficher cette limite, saisissez **tx-ring-limit ?** dans la ligne de commande.

Les facteurs clés sont la mémoire nécessaire pour prendre en charge les files d'attente et la mémoire disponible sur le périphérique.

La valeur **tx-ring-limit** 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.

#### Exemple :

```
hostname(config-priority-queue)# tx-ring-limit 3
```

#### Exemples

L'exemple suivant établit une file d'attente prioritaire sur l'interface « outside » (l'interface GigabitEthernet0/1), avec les valeurs queue-limit et tx-ring-limit par défaut :

```
hostname(config)# priority-queue outside
```

L'exemple suivant établit une file d'attente prioritaire sur l'interface « outside » (l'interface GigabitEthernet0/1), définit queue-limit à 260 paquets et définit tx-ring-limit à 3 :

```
hostname(config)# priority-queue outside
hostname(config-priority-queue)# queue-limit 260
hostname(config-priority-queue)# tx-ring-limit 3
```

## 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 441](#) 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** Créez une carte de trafic L3/L4 pour identifier le trafic pour lequel vous souhaitez effectuer une mise en file d'attente prioritaire.

```
class-map name
match parameter
```

### Exemple :

```
hostname(config)# class-map priority_traffic
hostname(config-cmap)# match access-list priority
```

Consultez [Créer une carte de trafic de couche 3/4 pour le trafic de transit, à la page 251](#) pour de plus amples renseignements.

- Étape 2** Créez une carte de trafic L3/L4 pour identifier le trafic pour lequel vous souhaitez effectuer une régulation prioritaire.

```
class-map name
match parameter
```

### Exemple :

```
hostname(config)# class-map policing_traffic
hostname(config-cmap)# match access-list policing
```

### 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** Ajouter ou modifier une liste des politiques : **policy-map name**

### Exemple :

```
hostname(config)# policy-map QoS_policy
```

- Étape 4** Identifiez la carte de trafic que vous avez créée pour le trafic prioritaire et configurez la mise en file d'attente prioritaire pour la classe.

```
class priority_map_name
priority
```

### Exemple :

```
hostname(config-pmap)# class priority_class
hostname(config-pmap-c)# priority
```



**Étape 5** Déterminez la carte de trafic que vous avez créée pour le trafic régulé : **class** *nom*

**Exemple :**

```
hostname(config-pmap) # class policing_class
```

**Étape 6** Configurez la régulation pour la classe.

**police** {**output** | **input**} **conform-rate** [**conform-burst**] [**conform-action** [**drop** | **transmit**]] [**exceed-action** [**drop** | **transmit**]]

Les options sont les suivantes :

- **output** : active la régulation du trafic circulant dans le sens de sortie.
- **input** : active la régulation du trafic circulant dans le sens d'entrée.
- **conform-rate** : définit la 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-burst** : (facultatif) Spécifie le 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. Si vous omettez la variable, la taille de rafale est calculée comme suit : 1/32 du débit conforme en octets. Par exemple, la taille de rafale pour un débit de 5 Mbit/s serait de 156 250.
- **conform-action** : (Facultatif) Définit l'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** : (facultatif) Définit l'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.

**Exemple :**

```
hostname(config-pmap-c) # police output 56000 10500
```

**Étape 7** Activez la liste des politiques sur une ou plusieurs interfaces.

**service-policy** *polycymap\_name* {**global** | **interface** *interface\_name*}

**Exemple :**

```
hostname(config) # service-policy QoS_policy interface inside
```

L'option **global** applique la liste des politiques à toutes les interfaces, et **interface** applique la politique à une interface. Une seule politique globale est autorisée. Vous pouvez remplacer la politique globale sur une interface en appliquant une politique de service à cette interface. Vous ne pouvez appliquer qu'une seule liste de politiques à chaque interface.

# Surveiller la QoS

Les rubriques suivantes expliquent comment surveiller la QoS.

## 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: TGI-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.

## Exemples de configuration pour la mise en file d'attente prioritaire et la régulation

Les sections suivantes fournissent des exemples de configuration de la mise en file d'attente et du contrôle prioritaires.

### Exemples de cartes de trafic pour le trafic VPN

Dans l'exemple suivant, la commande **class-map** classe tout le trafic TCP non tunnelisé à l'aide d'une liste de contrôle d'accès nommée tcp\_traffic :

```
hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic
```

Dans l'exemple suivant, d'autres critères de correspondance plus spécifiques sont utilisés pour classer le trafic vers des groupes de tunnels spécifiques liés à la sécurité. Ces critères de correspondance spécifiques précisent

qu'une correspondance sur un groupe de tunnels (dans ce cas, Tunnel-Group-1, défini précédemment) est requise comme première caractéristique de correspondance pour classer le trafic pour un tunnel spécifique et qu'elle permet une ligne de correspondance supplémentaire pour classer le trafic (point de code de services différenciés IP, transfert accéléré).

```
hostname(config)# class-map TGl-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef
```

Dans l'exemple suivant, la commande **class-map** classe le trafic tunnelisé et non tunnelisé en fonction du type de trafic :

```
hostname(config)# access-list tunneled extended permit ip 10.10.34.0 255.255.255.0
192.168.10.0 255.255.255.0
hostname(config)# access-list non-tunneled extended permit tcp any any
hostname(config)# tunnel-group tunnel-grp1 type IPsec_L2L

hostname(config)# class-map browse
hostname(config-cmap)# description "This class-map matches all non-tunneled tcp traffic."
hostname(config-cmap)# match access-list non-tunneled

hostname(config-cmap)# class-map TGl-voice
hostname(config-cmap)# description "This class-map matches all dscp ef traffic for
tunnel-grp 1."
hostname(config-cmap)# match dscp ef
hostname(config-cmap)# match tunnel-group tunnel-grp1

hostname(config-cmap)# class-map TGl-BestEffort
hostname(config-cmap)# description "This class-map matches all best-effort traffic for
tunnel-grp1."
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address
```

L'exemple suivant montre une façon de réguler le trafic dans un tunnel, à condition que le trafic classé ne soit pas spécifié comme un tunnel, mais passe *par* le tunnel. Dans cet exemple, 192.168.10.10 est l'adresse de la machine hôte du côté privé du tunnel distant, et l'ACL est nommée « host-over-l2l ». En créant une carte de trafic (nommée « host-specific »), vous pouvez ensuite réguler la classe « host-specific » avant que la connexion LAN à LAN ne régule le tunnel. Dans cet exemple, le trafic « host-specific » est limité en débit avant le tunnel, puis le tunnel est limité en débit :

```
hostname(config)# access-list host-over-l2l extended permit ip any host 192.168.10.10
hostname(config)# class-map host-specific
hostname(config-cmap)# match access-list host-over-l2l
```

## Exemple de priorité et de régulation

L'exemple suivant s'appuie sur la configuration développée dans la section précédente. Comme dans l'exemple précédent, il existe deux cartes de trafic nommées : tcp\_traffic et TGl-voice.

```
hostname(config)# class-map TGl-best-effort
hostname(config-cmap)# match tunnel-group Tunnel-Group-1
hostname(config-cmap)# match flow ip destination-address
```

L'ajout d'une troisième carte de trafic fournit une base pour définir une politique QoS tunnelisée et non tunnelisée, comme suit, qui crée une politique QoS simple pour le trafic tunnelisé et non tunnelisé, en affectant les paquets de la carte TG1-voice à la file d'attente à faible latence et en définissant des limites de débit sur les flux de trafic tcp\_traffic et TG1-best-effort.

Dans cet exemple, le débit maximal pour le trafic de la classe tcp\_traffic est de 56 000 bits/seconde et une taille de rafale maximale de 10 500 octets par seconde. Pour la carte TC1-BestEffort, le débit maximal est de 200 000 bits/seconde, avec une rafale maximale de 37 500 octets/seconde. Le trafic dans la classe TC1-voice n'a pas de vitesse maximale ni de débit de rafale maximal régulés, car il appartient à une classe prioritaire.

```
hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic

hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grpl
hostname(config-cmap)# match dscp ef

hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# match tunnel-group tunnel-grpl
hostname(config-cmap)# match flow ip destination-address

hostname(config)# policy-map qos
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# police output 56000 10500

hostname(config-pmap-c)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# class TG1-best-effort
hostname(config-pmap-c)# police output 200000 37500

hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)# police output 1000000 37500

hostname(config-pmap-c)# service-policy qos global
```

## Historique QoS

| Nom de la caractéristique                                        | Versions de plateforme | Description                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mise en file et régulation prioritaires                          | 7.0(1)                 | Nous avons lancé la mise en file d'attente et le contrôle prioritaires QoS.<br><br>Nous avons introduit les commandes suivantes : <b>priority-queue</b> , <b>queue-limit</b> , <b>tx-ring-limit</b> , <b>priority</b> , <b>police</b> , <b>show priority-queue statistics</b> , <b>show service-policy police</b> , <b>show service-policy priority</b> , <b>show running-config priority-queue</b> , <b>clear configure priority-queue</b> . |
| 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.<br><br>Nous avons introduit les commandes suivantes : <b>shape</b> , <b>show service-policy shape</b> .                                                                                                                                                                                                                                                    |

| Nom de la caractéristique                                                                             | Versions de plateforme | Description                                                                                                                               |
|-------------------------------------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 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 de priorité 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 453](#)
- [Lignes directrices pour la détection des menaces, à la page 456](#)
- [Paramètres par défaut pour la détection des menaces, à la page 456](#)
- [Configurer la détection des menaces, à la page 457](#)
- [Surveillance de la détection des menaces, à la page 461](#)
- [Exemples pour la détection des menaces, à la page 467](#)
- [Historique de la détection des menaces, à la page 468](#)

## 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 454](#).
- Statistiques de détection avancée des menaces : effectue le suivi de 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 454](#).

- 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 455](#).

## 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 :

- Dénier 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. Elle 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 des applications
- 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 attaque de 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**.

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                                                                                                     | 80 abandons/s au cours des 3 600 dernières secondes. | 320 abandons/s au cours de la dernière période de 120 secondes. |
| • Limite de connexion dépassée                                                                                                 |                                                      |                                                                 |
| • Paquets ICMP suspects détectés                                                                                               |                                                      |                                                                 |
| 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 de la dernière période de 20 secondes.    |
|                                                                                                                                                                  | 320 abandons/s au cours des 3 600 dernières secondes.   | 640 abandons/s au cours des 120 dernières secondes.               |
| <ul style="list-style-type: none"> <li>• Échec des vérifications de base du pare-feu</li> <li>• Paquets ayant échoué à l'inspection de l'application.</li> </ul> | 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 457.](#)

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 458.](#)

**Étape 3** [Configurer l'analyse de détection des menaces, à la page 460.](#)

## 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** Activez les statistiques de détection des menaces de base (si vous les avez désactivées précédemment).

**threat-detection basic-threat**

**Exemple :**

```
hostname(config)# threat-detection basic-threat
```

La détection des menaces de base est activée par défaut. Utilisez **no threat-detection basic-threat** pour la désactiver.

**Étape 2** (Facultatif) Modifiez les paramètres par défaut pour un ou plusieurs types d'événement.

**threat-detection rate {acl-drop | bad-packet-drop | conn-limit-drop | dos-drop | fw-drop | icmp-drop | inspect-drop | interface-drop | scanning-threat | syn-attack} rate-interval rate\_interval average-rate av\_rate burst-rate burst\_rate**

Pour obtenir une description de chaque type d'événement, consultez [Statistiques de base sur la détection des menaces, page 8-1](#).

Lorsque vous utilisez cette commande avec le mot-clé **scanning-threat**, elle est également utilisée dans la détection des menaces d'analyse. Si vous ne configurez pas la détection des menaces de base, vous pouvez toujours utiliser cette commande avec le mot-clé **scanning-threat** pour configurer les limites de débit pour la détection des menaces d'analyse.

Vous pouvez configurer jusqu'à trois intervalles de débit différents pour chaque type d'événement.

**Exemple :**

```
hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate 100
```

## Configurer les statistiques de détection avancée des menaces

Vous pouvez configurer l'ASA pour collecter des statistiques détaillées. Par défaut, les statistiques pour les ACL sont activées. Pour activer d'autres statistiques, procédez comme suit.

## Procédure

**Étape 1** (Facultatif) Activez *toutes* les statistiques.

**statistiques de détection des menaces**

Pour activer uniquement certaines statistiques, saisissez cette commande pour chaque type de statistique (montré plus loin dans cette procédure), et ne saisissez pas également la commande sans option. Vous pouvez saisir **statistiques de détection des menaces** (sans option), puis personnaliser certaines statistiques en entrant

la commande avec des options spécifiques aux statistiques (par exemple, **statistiques de détection des menaces host number-of-rate 2**). Si vous saisissez **statistiques de détection des menaces** (sans aucune option), puis saisissez une commande pour des statistiques spécifiques, mais sans option spécifique à la statistique, cette commande n'a aucun effet, car elle est déjà activée.

Si vous saisissez la forme **no** de cette commande, elle supprime toutes les commandes **statistiques de détection des menaces**, y compris la commande **statistiques de détection des menaces access-list**, qui est activée par défaut.

#### Exemple :

```
hostname(config)# threat-detection statistics
```

### Étape 2

(Facultatif) Activez les statistiques pour les ACL (si elles ont été désactivées précédemment).

#### statistiques de détection des menaces access-list

Les statistiques pour les listes de contrôle d'accès sont activées par défaut. Les statistiques d'ACL ne sont affichées qu'à l'aide de la commande **show threat-detection top access-list**.

#### Exemple :

```
hostname(config)# threat-detection statistics access-list
```

### Étape 3

(Facultatif) Configurez les statistiques pour les hôtes (mot clé **host**), les ports TCP et UDP (mot clé **port**) ou les protocoles IP non TCP/UDP (mot clé **protocol**).

#### statistiques de détection des menaces {host | port | protocol} [number-of-rate {1 | 2 | 3}]

Le mot-clé **number-of-rate** définit le nombre d'intervalles de débit gérés pour les statistiques. Le nombre d'intervalles de débit par défaut est **1**, ce qui réduit l'utilisation de la mémoire. Pour afficher davantage d'intervalles de débit, définissez la valeur à **2** ou **3**. Par exemple, si vous définissez la valeur à **3**, vous affichez les données des dernières 1 heure, 8 heures et 24 heures. Si vous définissez ce mot-clé à **1** (par défaut), seules les statistiques d'intervalle de débit les plus courts sont conservées. Si vous définissez la valeur à **2**, les deux intervalles les plus courts sont conservés.

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.

#### Exemple :

```
hostname(config)# threat-detection statistics host number-of-rate 2
```

```
hostname(config)# threat-detection statistics port number-of-rate 2
```

```
hostname(config)# threat-detection statistics protocol number-of-rate 3
```

### Étape 4

(Facultatif) Configurez les statistiques pour les attaques interceptées par TCP Intercept.

#### statistiques de détection des menaces tcp-intercept [rate-interval minutes] [burst-rate attacks\_per\_sec] [average-rate attacks\_per\_sec]

Lieu :

- **rate-interval** 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. Pendant cet intervalle, le système échantillonne le nombre d'attaques 30 fois.

- **burst-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-rate** : définit le seuil de débit moyen pour la génération des 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.

Pour activer l'interception TCP, consultez [Protéger les serveurs contre une attaque DoS par inondation SYN \(interception de TCP\)](#), à la page 410.

#### Remarque

Cette commande est disponible en mode de contexte multiple, contrairement aux autres commandes de détection des menaces.

#### Exemple :

```
hostname(config)# threat-detection statistics tcp-intercept rate-interval 60
burst-rate 800 average-rate 600
```

## 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** Activer la détection des menaces par analyse.

**threat-detection scanning-threat** [shun [except {ip-address ip\_address mask | object-group network\_object\_group\_id}]]

Par défaut, le message de journal système 733101 est généré lorsqu'un hôte est identifié comme agresseur. Entrez cette commande plusieurs fois pour identifier plusieurs adresses IP ou groupes d'objets réseau à exempter du bannissement.

#### Exemple :

```
hostname(config)# threat-detection scanning-threat shun except
ip-address 10.1.1.0 255.255.255.0
```

**Étape 2** (Facultatif) Définissez la durée du contournement pour les hôtes attaquants.

**threat-detection scanning-threat shun duration** seconds

**Exemple :**

```
hostname(config)# threat-detection scanning-threat shun duration 2000
```

**Étape 3**

(Facultatif) Modifiez la limite d'événements par défaut lorsque l'ASA identifie un hôte comme agresseur ou comme cible.

**threat-detection rate scanning-threat rate-interval** *rate\_interval* **average-rate** *av\_rate* **burst-rate** *burst\_rate*

Si vous avez déjà configuré cette commande dans le cadre de la configuration de base de détection des menaces, ces paramètres sont partagés avec la fonctionnalité de détection des menaces par analyse; vous ne pouvez pas configurer des débits distincts pour la détection des menaces de base et la détection des menaces par analyse. Si vous ne définissez pas les débits à l'aide de cette commande, les valeurs par défaut sont utilisées pour la fonctionnalité de détection des menaces par analyse et la fonctionnalité de détection des menaces de base. Vous pouvez configurer jusqu'à trois intervalles de débit différents en entrant des commandes distinctes.

**Exemple :**

```
hostname(config)# threat-detection rate scanning-threat rate-interval 1200
average-rate 10 burst-rate 20
```

```
hostname(config)# threat-detection rate scanning-threat rate-interval 2400
average-rate 10 burst-rate 20
```

## 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 base de la détection des menaces

Pour afficher les statistiques de base sur la détection des menaces, utilisez la commande suivante :

**show threat-detection rate** [**min-display-rate** *min\_display\_rate*] [**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**]

L'argument **min-display-rate** *min\_display\_rate* limite l'affichage aux statistiques qui dépassent le taux d'affichage minimal en événements par seconde. Vous pouvez définir le *min\_display\_rate* entre 0 et 2147483647.

Les autres arguments vous permettent de limiter l'affichage à des catégories spécifiques. Pour une description de chaque type d'événement, consultez [Statistiques de détection des menaces de base, à la page 454](#).

Le résultat affiche le débit moyen en événements/s sur deux périodes fixes : les 10 dernières minutes et la dernière heure. Il affiche également : le débit de rafale actuel en événements/s sur le dernier intervalle de rafale terminé, qui est 1/30 de l'intervalle de débit moyen ou 10 secondes, selon le plus élevé des deux; le nombre de fois que les débits ont été dépassés (déclenchés); et le nombre total d'événements au fil des périodes.

L'ASA stocke le nombre à la fin de chaque période de rafale, pour un total de 30 intervalles de rafale terminés. L'intervalle de rafale inachevée qui se produit actuellement n'est pas inclus dans le débit moyen. Par exemple, si l'intervalle de débit moyen est de 20 minutes, l'intervalle de rafale est de 20 secondes. Si le dernier intervalle

de rafale a été compris entre 3:00:00 et 3:00:20 et que vous utilisez la commande **afficher** à 3:00:25, les 5 dernières secondes ne sont pas incluses dans la sortie.

La seule exception à cette règle est si le nombre d'événements dans l'intervalle de rafale inachevé dépasse déjà le nombre d'événements dans l'intervalle de rafale le plus ancien (n° 1 sur 30) lors du calcul du nombre total d'événements. Dans ce cas, l'ASA calcule le nombre total d'événements comme les 29 derniers intervalles complets, plus les événements jusqu'à présent dans l'intervalle de rafale inachevé. Cette exception vous permet de surveiller une augmentation importante des événements en temps réel.

Vous pouvez effacer les statistiques à l'aide de la commande **clear threat-detection rate**.

Voici un exemple de sortie de la commande **show threat-detection rate** :

```
hostname# show threat-detection rate
```

|                   | Average (eps) | Current (eps) | Trigger | Total events |
|-------------------|---------------|---------------|---------|--------------|
| 10-min ACL drop:  | 0             | 0             | 0       | 16           |
| 1-hour ACL drop:  | 0             | 0             | 0       | 112          |
| 1-hour SYN attck: | 5             | 0             | 2       | 21438        |
| 10-min Scanning:  | 0             | 0             | 29      | 193          |
| 1-hour Scanning:  | 106           | 0             | 10      | 384776       |
| 1-hour Bad pkts:  | 76            | 0             | 2       | 274690       |
| 10-min Firewall:  | 0             | 0             | 3       | 22           |
| 1-hour Firewall:  | 76            | 0             | 2       | 274844       |
| 10-min DoS attck: | 0             | 0             | 0       | 6            |
| 1-hour DoS attck: | 0             | 0             | 0       | 42           |
| 10-min Interface: | 0             | 0             | 0       | 204          |
| 1-hour Interface: | 88            | 0             | 0       | 318225       |

## Surveillance des statistiques de détection avancée des menaces

Pour surveiller les statistiques de détection avancée des menaces, utilisez les commandes affichées dans le tableau suivant. La sortie d'affichage affiche les éléments suivants :

- Le débit moyen en événements/s sur des périodes fixes.
- Le débit de rafale actuel en événements/s sur le dernier intervalle de rafale terminé, qui est de 1/30 de l'intervalle de débit moyen ou de 10 secondes, selon le plus élevé des deux.
- Le nombre de fois que les débits ont été dépassés (pour les statistiques de trafic abandonnées uniquement).
- Le nombre total d'événements sur les périodes de temps fixes.

L'ASA stocke le nombre à la fin de chaque période de rafale, pour un total de 30 intervalles de rafale terminés. L'intervalle de rafale inachevée qui se produit actuellement n'est pas inclus dans le débit moyen. Par exemple, si l'intervalle de débit moyen est de 20 minutes, l'intervalle de rafale est de 20 secondes. Si le dernier intervalle de rafale a été compris entre 3:00:00 et 3:00:20 et que vous utilisez la commande **afficher** à 3:00:25, les 5 dernières secondes ne sont pas incluses dans la sortie.

La seule exception à cette règle est si le nombre d'événements dans l'intervalle de rafale inachevé dépasse déjà le nombre d'événements dans l'intervalle de rafale le plus ancien (n° 1 sur 30) lors du calcul du nombre total d'événements. Dans ce cas, l'ASA calcule le nombre total d'événements comme les 29 derniers intervalles complets, plus les événements jusqu'à présent dans l'intervalle de rafale inachevé. Cette exception vous permet de surveiller une augmentation importante des événements en temps réel.



| Commande                                                                                                                                                                                                                                                                     | Objectif                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show threat-detection statistics</b> [ <b>min-display-rate</b> <i>min_display_rate</i> ] <b>top</b> [[ <b>access-list</b>   <b>host</b>   <b>port-protocol</b> ] [ <b>rate-1</b>   <b>rate-2</b>   <b>rate-3</b> ]   <b>tcp-intercept</b> [ <b>all</b> ] <b>detail</b> ]] | <p>Affiche les 10 principales statistiques. Si vous ne saisissez aucune option, les 10 principales statistiques sont affichées pour toutes les catégories.</p> <p>L'argument <b>min-display-rate</b> <i>min_display_rate</i> limite l'affichage aux statistiques qui dépassent le taux d'affichage minimal en événements par seconde. Vous pouvez définir le <i>min_display_rate</i> entre 0 et 2147483647.</p> <p>Les lignes suivantes expliquent les mots-clés facultatifs.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>show threat-detection statistics</b> [ <b>min-display-rate</b> <i>min_display_rate</i> ] <b>top access-list</b> [ <b>rate-1</b>   <b>rate-2</b>   <b>rate-3</b> ]                                                                                                         | <p>Pour afficher les 10 principaux ACE correspondant aux paquets, y compris les ACE d'autorisation et de refus, utilisez le mot-clé <b>access-list</b>. Le trafic autorisé et refusé ne sont pas distincts dans cet affichage. Si vous activez la détection des menaces de base à l'aide de la commande <b>threat-detection basic-threat</b>, vous pouvez suivre les refus d'ACL à l'aide de la commande <b>show threat-detection rate acl-drop</b>.</p> <p>Le mot-clé <b>rate-1</b> affiche les statistiques pour les plus petits intervalles de débit fixe disponibles dans l'affichage ; <b>rate-2</b> affiche l'intervalle de débit suivant le plus important ; et <b>rate-3</b>, si vous avez défini trois intervalles, affiche le plus grand intervalle de débit. Par exemple, l'affichage présente les statistiques de la dernière heure, des 8 dernières heures et des 24 dernières heures. Si vous définissez le mot-clé <b>rate-1</b>, l'ASA affiche uniquement l'intervalle de temps d'1 heure.</p> |
| <b>show threat-detection statistics</b> [ <b>min-display-rate</b> <i>min_display_rate</i> ] <b>top host</b> [ <b>rate-1</b>   <b>rate-2</b>   <b>rate-3</b> ]                                                                                                                | <p>Pour afficher uniquement les statistiques d'hôte, utilisez le mot-clé <b>host</b>.</p> <p><b>Remarque</b> : 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.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>show threat-detection statistics</b> [ <b>min-display-rate</b> <i>min_display_rate</i> ] <b>top port-protocol</b> [ <b>rate-1</b>   <b>rate-2</b>   <b>rate-3</b> ]                                                                                                       | <p>Pour afficher les statistiques sur les ports et les protocoles, utilisez le mot-clé <b>port-protocol</b>. Le mot-clé <b>port-protocol</b> 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.</p>                                                                                                                                                                                                                                                                                                                                  |
| <b>show threat-detection statistics</b> [ <b>min-display-rate</b> <i>min_display_rate</i> ] <b>top tcp-intercept</b> [ <b>all</b> ] <b>detail</b> ]]                                                                                                                         | <p>Pour afficher les statistiques d'interception TCP, utilisez le mot-clé <b>tcp-intercept</b>. L'affichage inclut les 10 principaux serveurs protégés sous attaque. Le mot-clé <b>all</b> affiche les données historiques de tous les serveurs suivis. Le mot-clé <b>detail</b> affiche 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.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>show threat-detection statistics</b> [ <b>min-display-rate</b> <i>min_display_rate</i> ] <b>host</b> [ <i>ip_address</i> [ <i>mask</i> ]]                                                                                                                                 | <p>Affiche les statistiques pour tous les hôtes ou pour un hôte ou un sous-réseau spécifique.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>show threat-detection statistics</b> [ <b>min-display-rate</b> <i>min_display_rate</i> ] <b>port</b> [ <i>start_port</i> [- <i>end_port</i> ]]                                                                                                                            | <p>Affiche les statistiques pour tous les ports ou pour un port ou une plage de ports spécifique.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Commande                                                                                                                                                 | Objectif                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show threat-detection statistics</b> [ <b>min-display-rate</b> <i>min_display_rate</i> ] <b>protocol</b> [ <i>protocol_number</i>   <i>protocol</i> ] | <p>Affiche les statistiques pour tous les protocoles IP ou pour un protocole spécifique.</p> <p>L'argument <i>protocol_number</i> est un entier compris entre 0 et 255. L'argument du <i>protocole</i> peut être l'un des suivants : <b>ah</b>, <b>eigrp</b>, <b>esp</b>, <b>gre</b>, <b>icmp</b>, <b>icmp6</b>, <b>igmp</b>, <b>igrp</b>, <b>ip</b>, <b>ipinip</b>, <b>ipsec</b>, <b>nos</b>, <b>ospf</b>, <b>pcp</b>, <b>pim</b>, <b>pptp</b>, <b>snp</b>, <b>tcp</b>, <b>udp</b>.</p> |

## Évaluation des statistiques de détection des menaces de l'hôte

Voici un exemple de résultat de la commande **show threat-detection statistics host** :

```
hostname# show threat-detection statistics host

 Average (eps) Current (eps) Trigger Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
 1-hour Sent byte: 2938 0 0 10580308
 8-hour Sent byte: 367 0 0 10580308
 24-hour Sent byte: 122 0 0 10580308
 1-hour Sent pkts: 28 0 0 104043
 8-hour Sent pkts: 3 0 0 104043
 24-hour Sent pkts: 1 0 0 104043
 20-min Sent drop: 9 0 1 10851
 1-hour Sent drop: 3 0 1 10851
 1-hour Recv byte: 2697 0 0 9712670
 8-hour Recv byte: 337 0 0 9712670
 24-hour Recv byte: 112 0 0 9712670
 1-hour Recv pkts: 29 0 0 104846
 8-hour Recv pkts: 3 0 0 104846
 24-hour Recv pkts: 1 0 0 104846
 20-min Recv drop: 42 0 3 50567
 1-hour Recv drop: 14 0 1 50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
 1-hour Sent byte: 0 0 0 614
 8-hour Sent byte: 0 0 0 614
 24-hour Sent byte: 0 0 0 614
 1-hour Sent pkts: 0 0 0 6
 8-hour Sent pkts: 0 0 0 6
 24-hour Sent pkts: 0 0 0 6
 20-min Sent drop: 0 0 0 4
 1-hour Sent drop: 0 0 0 4
 1-hour Recv byte: 0 0 0 706
 8-hour Recv byte: 0 0 0 706
 24-hour Recv byte: 0 0 0 706
 1-hour Recv pkts: 0 0 0 7
```

Le tableau suivant explique la sortie.

**Tableau 17 : show threat-detection statistics host**

| Champ       | Description                                                                      |
|-------------|----------------------------------------------------------------------------------|
| Hébergement | Adresse IP de l'hôte                                                             |
| tot-ses     | Le nombre total de sessions pour cet hôte depuis son ajout à la base de données. |

| Champ         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| act-ses       | Le nombre total de sessions actives dans lesquelles l'hôte est actuellement impliqué.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| fw-drop       | Le nombre d'abandons de pare-feu. Les abandons de pare-feu sont un taux combiné qui inclut tous les abandons de paquets liés au pare-feu suivis dans la détection des menaces de base, y compris les refus d'ACL, les paquets incorrects, les limites de connexion dépassées, les paquets d'attaques DoS, les paquets ICMP suspects, les paquets d'attaques TCP SYN et les paquets d'attaques par session UDP sans données de retour. 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| insp-drop     | Le nombre de paquets abandonnés en raison d'un échec de l'inspection de l'application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| null-ses      | Le nombre de sessions nulles, qui sont des sessions TCP SYN qui ne se sont pas terminées dans le délai d'expiration de 3 secondes, et les sessions UDP qui n'ont fait l'objet d'aucune donnée envoyée par son serveur 3 secondes après le début de la session.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| bad-acc       | Le nombre de tentatives d'accès incorrectes aux ports d'hôte fermés. Lorsqu'il est déterminé qu'un port se trouve dans une session nulle (voir la description du champ null-ses), l'état du port de l'hôte est défini à HOST_PORT_CLOSE. Tout client qui accède au port de l'hôte est immédiatement classé comme un mauvais accès sans qu'il soit nécessaire d'attendre un délai d'expiration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Moyenne (eps) | <p>Le débit moyen en événements/s sur chaque période.</p> <p>L'ASA stocke le nombre à la fin de chaque période de rafale, pour un total de 30 intervalles de rafale terminés. L'intervalle de rafale inachevée qui se produit actuellement n'est pas inclus dans le débit moyen. Par exemple, si l'intervalle de débit moyen est de 20 minutes, l'intervalle de rafale est de 20 secondes. Si le dernier intervalle de rafale a été compris entre 3:00:00 et 3:00:20 et que vous utilisez la commande <b>afficher</b> à 3:00:25, les 5 dernières secondes ne sont pas incluses dans la sortie.</p> <p>La seule exception à cette règle est si le nombre d'événements dans l'intervalle de rafale inachevé dépasse déjà le nombre d'événements dans l'intervalle de rafale le plus ancien (n° 1 sur 30) lors du calcul du nombre total d'événements. Dans ce cas, l'ASA calcule le nombre total d'événements comme les 29 derniers intervalles complets, plus les événements jusqu'à présent dans l'intervalle de rafale inachevé. Cette exception vous permet de surveiller une augmentation importante des événements en temps réel.</p> |
| Actuel (eps)  | Le débit de rafale actuel en événements/s sur le dernier intervalle de rafale terminé, qui est de 1/30 de l'intervalle de débit moyen ou de 10 secondes, selon le plus élevé des deux. Pour l'exemple spécifié dans la description de la moyenne (eps), le taux actuel est le taux de 3:19:30 à 3:20:00                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| initiales     | Le nombre de fois que les limites de débit de paquets abandonnés ont été dépassées. Pour le trafic valide identifié dans les lignes des octets et des paquets envoyés et reçus, cette valeur est toujours 0, car il n'y a aucune limite de débit à déclencher pour le trafic valide.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Champ                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nombre total d'événements              | Le nombre total d'événements sur chaque intervalle de débit. L'intervalle de rafale inachevée qui se produit actuellement n'est pas inclus dans le nombre total d'événements. La seule exception à cette règle est si le nombre d'événements dans l'intervalle de rafale inachevé dépasse déjà le nombre d'événements dans l'intervalle de rafale le plus ancien (n° 1 sur 30) lors du calcul du nombre total d'événements. Dans ce cas, l'ASA calcule le nombre total d'événements comme les 29 derniers intervalles complets, plus les événements jusqu'à présent dans l'intervalle de rafale inachevé. Cette exception vous permet de surveiller une augmentation importante des événements en temps réel. |
| 20 min, 1 heure, 8 heures et 24 heures | Statistiques pour ces intervalles de débit fixe. Pour chaque intervalle : <ul style="list-style-type: none"> <li>• Octets envoyés : le nombre d'octets envoyés par l'hôte.</li> <li>• Paquets envoyés : le nombre de paquets envoyés par l'hôte.</li> <li>• Envoyés abandonnés : le nombre de paquets envoyés par l'hôte qui ont été abandonnés en raison d'une attaque par analyse.</li> <li>• Octets reçus : le nombre d'octets reçus par l'hôte.</li> <li>• Paquets reçus : le nombre de paquets reçus par l'hôte.</li> <li>• Réception de l'abandon : le nombre de paquets reçus par l'hôte qui ont été abandonnés en raison d'une attaque par analyse.</li> </ul>                                        |

## Surveillance de la détection des menaces, des hôtes contournés, des agresseurs et des cibles

Pour surveiller et gérer les hôtes et les attaquants bloqués, ainsi que les cibles pour la détection des menaces d'analyse, utilisez les commandes suivantes. Ces commandes sont destinées uniquement à la détection des menaces d'analyse et ne s'appliquent pas à d'autres services.

- **show threat-detection shun**

Affiche les hôtes actuellement bloqués. Par exemple :

```
hostname# show threat-detection shun

Shunned Host List:
(outside) src-ip=10.0.0.13 255.255.255.255
(inside) src-ip=10.0.0.13 255.255.255.255
```

- **clear threat-detection shun [ip\_address [mask]]**

Libère un hôte de la liste de blocage. Si vous ne spécifiez pas d'adresse IP, tous les hôtes sont effacés de la liste de blocage.

Par exemple, pour libérer l'hôte à l'adresse 10.1.1.6, entrez la commande suivante :

```
hostname# clear threat-detection shun 10.1.1.6
```

- **show threat-detection scanning-threat [attacker | target]**

Affiche les hôtes que l'ASA considère comme des attaquants (y compris les hôtes dans la liste de blocage) et affiche les hôtes qui sont la cible d'une attaque. Si vous ne saisissez pas d'option, les attaquants et les hôtes cibles sont affichés. Par exemple :

```
hostname# show threat-detection scanning-threat
Latest Target Host & Subnet List:
 192.168.1.0 (121)
 192.168.1.249 (121)
Latest Attacker Host & Subnet List:
 192.168.10.234 (outside)
 192.168.10.0 (outside)
 192.168.10.2 (outside)
 192.168.10.3 (outside)
 192.168.10.4 (outside)
 192.168.10.5 (outside)
 192.168.10.6 (outside)
 192.168.10.7 (outside)
 192.168.10.8 (outside)
 192.168.10.9 (outside)
```

## Exemples pour la détection des menaces

L'exemple suivant configure les statistiques de détection des menaces de base et modifie les paramètres de taux d'attaque DoS. Toutes les statistiques de détection avancée des menaces sont activées, avec le nombre d'intervalles de taux des statistiques d'hôte réduit à 2. L'intervalle de débit d'interception TCP est également personnalisé. La détection des menaces d'analyse est activée avec le blocage automatique pour toutes les adresses, à l'exception de 10.1.1.0/24. Les intervalles de taux de menace d'analyse sont personnalisés.

```
threat-detection basic-threat
threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate 100
threat-detection statistics
threat-detection statistics host number-of-rate 2
threat-detection statistics tcp-intercept rate-interval 60 burst-rate 800 average-rate 600
threat-detection scanning-threat shun except ip-address 10.1.1.0 255.255.255.0
threat-detection rate scanning-threat rate-interval 1200 average-rate 10 burst-rate 20
threat-detection rate scanning-threat rate-interval 2400 average-rate 10 burst-rate 20
```

# 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)                 | <p>Statistiques de détection de base et avancée des menaces, la détection des menaces d'analyse a été introduite.</p> <p>Les commandes suivantes ont été introduites : <b>threat-detection basic-threat, threat-detection rate, show threat-detection rate, clear threat-detection rate, threat-detection statistics, show threat-detection statistics, threat-detection scanning-threat, threat-detection rate scanning-threat, show threat-detection scanning-threat, show threat-detection shun, clear threat-detection shun.</b></p> |
| Durée du bannissement                                                                       | 8.0(4)/8.1(2)          | <p>Vous pouvez maintenant définir la durée du blocage,</p> <p>La commande suivante a été introduite : <b>threat-detection scanning-threat shun duration.</b></p>                                                                                                                                                                                                                                                                                                                                                                         |
| Statistiques TCP Intercept                                                                  | 8.0(4)/8.1(2)          | <p>Les statistiques TCP Intercept ont été introduites.</p> <p>Les commandes suivantes ont été modifiées ou introduites : <b>threat-detection statistics tcp-intercept, show threat-detection statistics top tcp-intercept, clear threat-detection statistics.</b></p>                                                                                                                                                                                                                                                                    |
| Personnaliser les intervalles de débit des statistiques d'hôte                              | 8.1(2)                 | <p>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.</p> <p>La commande suivante a été modifiée : <b>threat-detection statistics host number-of-rates.</b></p>                                                                                                                                                                                                                                               |
| L'intervalle de débit de rafale a été modifié à 1/30 du débit moyen.                        | 8.2(1)                 | <p>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.</p>                                                                                                                                                                                                                                                                                                                 |
| Personnaliser les intervalles de débit des statistiques de port et de protocole             | 8.3(1)                 | <p>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.</p> <p>Les commandes suivantes ont été modifiées : <b>threat-detection statistics port number-of-rates, threat-detection statistics protocol number-of-rates.</b></p>                                                                                                                                                                                   |
| Amélioration de l'utilisation de la mémoire                                                 | 8.3(1)                 | <p>L'utilisation de la mémoire pour la détection des menaces a été améliorée.</p> <p>La commande suivante a été introduite : <b>show threat-detection memory.</b></p>                                                                                                                                                                                                                                                                                                                                                                    |

## À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.

## À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.



## À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.

## À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.

## 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.