



CLI, livre 3 : Guide de configuration de la ligne de commande VPN de la série Cisco Secure Firewall ASA, 9.19

Dernière modification : 2026-05-25

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 xiii

Objectifs du document xiii

Documentation associée xiii

Conventions de document xiii

Communications, services et renseignements supplémentaires xv

CHAPITRE 1

IPsec et ISAKMP 1

À propos de la tunnelisation, d'IPsec et d'ISAKMP 1

Présentation d'IPsec 2

Survol d'ISAKMP et d'IKE 2

À propos de la carte de chiffrement IKEv2 multi-homologues 4

Licences pour les VPN IPsec 7

Lignes directrices relatives aux VPN IPsec 7

Configurer ISAKMP 8

Configurer les politiques IKEv1 et IKEv2 8

Valeurs et mots-clés de la politique IKE 9

Activer IKE sur l'interface externe. 11

Activer ou désactiver le mode agressif IKEv1 12

Configurer une méthode d'ID pour les homologues ISAKMP IKEv1 et IKEv2 12

Notification INVALID_SELECTORS 13

Configurer la clé prépartagée IKEv2 en format hexadécimal 13

Activer ou désactiver l'envoi de la notification IKE 13

Configurer les options de fragmentation IKEv2 14

Authentification AAA avec autorisation 15

Activer IPsec sur NAT-T 16

Activer IPsec avec IKEv1 sur TCP 17

Configurer la correspondance de groupe de certificats pour IKEv1	18
Configurer IPsec	20
Définir les cartes de chiffrement	20
Exemple de cartes de chiffrement LAN à LAN	24
Définir les clés de l'infrastructure à clé publique (PKI)	28
Appliquer les cartes de chiffrement aux interfaces	29
Utiliser les listes de contrôle d'interface	29
Modifier la durée de vie des SA IPsec	32
Modifier le routage VPN	32
Créer des cartes de chiffrement statiques	33
Créer des cartes de chiffrement dynamiques	38
Configurer la redondance de site à site	41
Gestion des VPN IPsec	41
Affichage d'une configuration IPsec	41
Attendre la fin des sessions actives avant de redémarrer	42
Alerter les homologues avant la déconnexion	42
Effacer les associations de sécurité	43
Effacer les configurations de cartes de chiffrement	43

CHAPITRE 2
L2TP sur IPsec 45

À propos des VPN L2TP sur IPsec/IKEv1	45
Modes de transport et de tunnel IPsec	46
Exigences de licence pour L2TP sur IPsec	47
Conditions préalables à la configuration de L2TP sur IPsec	47
Lignes directrices et limites relatives à la licence	47
Configuration de L2TP sur Eclipse avec l'interface de ligne de commande	49
Créer des politiques IKE pour répondre aux propositions Windows 7	52
Exemple de configuration pour L2TP sur IPsec	53
Historique des fonctionnalités pour L2TP sur IPsec	54

CHAPITRE 3
Options de haute disponibilité 55

Options de haute disponibilité	55
VPN et mise en grappe sur le châssis Cisco Secure Firewall eXtensible Operating System (FXOS)	55
Équilibrage de la charge VPN	56

Basculement	56
Équilibrage de la charge VPN	57
À propos de l'équilibrage de charge VPN	57
Algorithme d'équilibrage de charge VPN	57
Configurations de groupes d'équilibrage de charge VPN	58
Élection du directeur d'équilibrage de charge VPN	58
Foire aux questions sur l'équilibrage de la charge VPN	59
Licences pour l'équilibrage de charge VPN	61
Conditions préalables à l'équilibrage de la charge VPN	61
Directives et limites pour l'équilibrage de charge VPN	62
Configuration de l'équilibrage de charge du VPN	63
Configurer les interfaces publique et privée pour l'équilibrage de charge VPN	64
Configurer les attributs du groupe d'équilibrage de charge VPN	65
Exemples de configuration pour l'équilibrage de charge VPN	68
Affichage des informations d'équilibrage de charge VPN	68
Historique des fonctionnalités pour l'équilibrage de charge VPN	69

CHAPITRE 4

Paramètres VPN généraux 71

Lignes directrices et limites relatives à la licence	71
Configurer IPsec pour contourner les ACL	72
Permettre le trafic intra-interface (hairpinning)	72
Considérations sur la NAT pour le trafic intra-interface	73
Définition du nombre maximal de sessions VPN IPsec ou SSL actives	74
Utiliser la mise à jour du client pour assurer des niveaux de révision acceptables du client IPsec	75
Mettre en œuvre une connexion entre une adresse IP attribuée par NAT et une adresse IP publique	77
Affichage des politiques de NAT du VPN	78
Configurer les limites de session VPN	78
Afficher l'allocation des ressources de licence	79
Afficher l'utilisation des ressources de licence	79
Limiter les sessions VPN	80
Utilisation d'un certificat d'identité lors de la négociation	80
Configurer le pool de cœurs de chiffrement	80
Configurer la tunnellation fractionnée dynamique	81
Configuration du tunnel VPN de gestion	82

Affichage des sessions VPN actives	83
Affichage des sessions actives Secure Client (services client sécurisés) par type d'adresse IP	83
Affichage des sessions VPN de site à site actives par type d'adresse IP	84
À propos de l'application des politiques ISE :	84
Configurer les groupes de serveurs RADIUS pour l'application des politiques ISE	85
Exemples de configuration pour l'application de la politique ISE	88
Dépannage de l'application des politiques	89
Configurer les paramètres avancés SSL	89
Flux persistants tunnelisés IPsec	95
Configurer les flux de tunnel IPsec persistants à l'aide de l'interface de ligne de commande	97
Dépannage des flux persistants tunnelisés IPsec	97
La fonctionnalité des flux de tunnel IPsec persistants est-elle activée ?	97
Localisation des flux orphelins	98
Effacer les configurations WebVPN de l'ASA	98

CHAPITRE 5

Profils de connexion, stratégies de groupe et utilisateurs	99
Aperçu des profils de connexion, des stratégies de groupe et des utilisateurs	99
Profils de connexion	101
Paramètres de connexion du profil de connexion général	101
Paramètres de connexion de groupe de tunnels IPsec	102
Paramètres de connexion de profil de connexion pour les sessions VPN SSL	104
Configurer les profils de connexion	105
Profils de connexion	105
Configuration par défaut du profil de connexion IPsec d'accès à distance	105
Attributs généraux du groupe de tunnels IPsec	107
Configurer les profils de connexion d'accès à distance.	107
Préciser un nom et un type pour le profil de connexion d'accès à distance	107
Configurer les attributs généraux du profil de connexion d'accès à distance	108
Configurer de la double authentification	112
Configurer les attributs IPsec IKEv1 du profil de connexion d'accès à distance	114
Configurer les attributs PPP du profil de connexion à distance IPsec	116
Configurer les profils de connexion LAN-à-LAN	118
Configurer le profil de connexion LAN à LAN par défaut	118
Préciser un nom et un type pour un profil de connexion LAN à LAN	118

Configurer les attributs généraux du profil de connexion LAN-à-LAN	119
Configurer les attributs IPsec IKEv1 de site à site (LAN à LAN)	119
À propos des groupes de tunnels pour les clients IKEv2 basés sur les normes	122
Prise en charge des attributs IKEv2 basée sur les normes	122
Prise en charge DAP	123
Sélection de groupe de tunnels pour les clients d'accès à distance	123
Prise en charge de l'authentification pour les clients IKEv2 basés sur les normes	123
Authentification de plusieurs certificats	125
Configurer l'option query-identity pour la récupération de l'identité EAP	126
Configurer les paramètres de Microsoft Active Directory pour la gestion des mots de passe	128
Utiliser Active Directory pour forcer l'utilisateur à modifier le mot de passe lors de la prochaine connexion	128
Utiliser Active Directory pour préciser l'ancienneté maximale du mot de passe	129
Utiliser Active Directory pour appliquer la longueur minimale du mot de passe	129
Utiliser Active Directory pour appliquer la complexité du mot de passe	130
Configurer le profil de connexion pour la prise en charge des messages RADIUS/SDI pour Secure Client (services client sécurisés)	130
Configurer l'appareil de sécurité pour prendre en charge les messages RADIUS/SDI	131
Stratégies de groupe	132
Modifier la stratégie de groupe par défaut	133
Configurer les stratégies de groupe	136
Configurer une stratégie de groupe externe	136
Créer une stratégie de groupe interne	137
Configurer les attributs généraux de la stratégie de groupe interne	138
Nom de la stratégie de groupe	138
Configurer la bannière de message de stratégie de groupe	138
Préciser les ensembles d'adresses pour les connexions d'accès à distance	138
Attribuer un ensemble d'adresses IPv4 à une stratégie de groupe interne	139
Attribuer un ensemble d'adresses IPv6 à une stratégie de groupe interne	140
Préciser le protocole de tunnelisation pour la stratégie de groupe	141
Préciser un réseau VLAN pour l'accès à distance ou appliquer une règle de contrôle d'accès unifiée à la stratégie de groupe	141
Préciser les heures d'accès au VPN pour une stratégie de groupe	144
Préciser les connexions VPN simultanées pour une stratégie de groupe	145
Restreindre l'accès à un profil de connexion précis	146

Préciser le délai de connexion VPN maximal dans une stratégie de groupe	147
Préciser un délai d'inactivité de session VPN pour une stratégie de groupe	148
Configurer les serveurs WINS et DNS pour une stratégie de groupe	149
Définir la politique de tunnellation fractionnée	151
Préciser une liste de réseaux pour la tunnellation fractionnée	152
Configurer les attributs de domaine pour la tunnellation fractionnée	153
Configurer l'interception DHCP pour Windows XP et la tunnellation fractionnée	155
Configurer les paramètres du proxy de navigateur pour une utilisation avec les clients d'accès à distance	156
Configurer les attributs de sécurité pour les clients IPsec (IKEv1)	158
Configurer les attributs IPsec-UDP pour les clients IKEv1	161
Configurer les attributs pour les clients de matériel VPN	162
Configurer les attributs de stratégie de groupe pour les connexions Secure Client (services client sécurisés)	165
Configurer les attributs du serveur de sauvegarde	168
Configurer les paramètres du contrôle d'admission au réseau	169
Configurer les politiques de pare-feu des clients VPN	173
Configurer les politiques de pare-feu pour Secure Client (services client sécurisés)	174
Utiliser un serveur Zone Labs Integrity.	175
Définir le type de client de pare-feu sur Zone Labs	177
Définir les paramètres de pare-feu client	177
Configurer les règles d'accès client	179
Configurer les attributs d'utilisateur	181
Afficher la configuration du nom d'utilisateur	181
Configurer les attributs pour les utilisateurs individuels	182
Définir un mot de passe d'utilisateur et un niveau de privilège	182
Configurer les attributs d'utilisateur	183
Configurer les attributs d'utilisateur VPN	183
Bonnes pratiques pour la configuration et l'ajustement de l'ACL du filtre de VPN	190

CHAPITRE 6

Adresses IP pour les VPN 191

Configurer une politique d'attribution d'adresses IP	191
Configurer les adresses IPv4	192
Configurer l'attribution des adresses IPv6	192

Afficher les méthodes d'attribution d'adresses	193
Configurer les ensembles d'adresses IP locales	193
Configurer les ensembles d'adresses IPv4 locales	194
Configurer les ensembles d'adresses IPv6 locaux	195
Configurer l'adressage AAA	195
Configurer l'adressage DHCP	196

CHAPITRE 7

VPN IPsec d'accès à distance 199

Présentation des VPN d'accès à distance IPsec	199
À propos des VPN Mobike et d'accès à distance	200
Exigences de licence pour le module AnyConnect VPN de Cisco Secure Client	201
Restrictions pour le VPN IPsec d'accès à distance	201
Configurer les VPN d'accès à distance IPsec	202
Configurer une interface	202
Configurer la politique ISAKMP et activer ISAKMP sur l'interface externe	203
Configurer un ensemble d'adresses	204
Ajouter un utilisateur	204
Créer un ensemble de transformation IKEv1 ou une proposition IKEv2	204
Définir un groupe de tunnels	206
Créer une carte de chiffrement dynamique	207
Créer une entrée de carte de chiffrement pour utiliser la carte de chiffrement dynamique	208
Configurer un VPN d'accès à distance IPsec IKEv2 en mode multicontexte	208
Authentification VPN à l'aide de clés prépartagées post-quantiques	209
Conditions préalables à l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN	209
Lignes directrices et limites relatives à l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN	209
Flux de travail pour l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN	210
Configurer les clés prépartagées post-quantiques et les clés prépartagées dans Windows Credential Manager	211
Configurer le profil VPN pour Secure Client avec des attributs de clé prépartagée post-quantique	212
Configurer l'authentification VPN sur ASA à l'aide de clés prépartagées post-quantiques	212
Exemples de configuration pour les VPN d'accès à distance IPsec	214
Exemples de configuration pour le VPN d'accès à distance IPsec IKEv2 basé sur les normes en mode multi-contexte	215

Exemples de configuration pour le VPN d'accès à distance Secure Client (services client sécurisés)	
IPSec IKEv2 en mode multicontexte	216
Historique des VPN d'accès à distance	217

CHAPITRE 8

VPN IPsec de LAN à LAN 219

Résumé de la configuration	219
Configurer le VPN de site à site en mode de contexte multiple	220
Interfaces de configuration	221
Configurer la politique ISAKMP et activer ISAKMP sur l'interface externe	222
Configurer les politiques ISAKMP pour les connexions IKEv1	222
Configurer les politiques ISAKMP pour les connexions IKEv2	224
Plusieurs échanges de clés pour IKEv2	224
Lignes directrices et limites relatives aux échanges de clés multiples, IKEv2	226
Vérifier les configurations d'échanges de clés multiples IKEv2	226
Créer un ensemble de transformation IKEv1	227
Créer une proposition IKEv2	228
Configurer une ACL	229
Définition d'un groupe de tunnels	230
Créer une carte de chiffrement et l'appliquer à une interface	231
Appliquer les cartes de chiffrement aux interfaces	234

CHAPITRE 9

Connexions du client VPN AnyConnect 235

À propos du client VPN Secure Client (services client sécurisés)	235
Exigences de licence pour Secure Client (services client sécurisés)	236
Configurer les connexions pour Secure Client (services client sécurisés)	237
Configurer l'ASA pour déployer le client via le Web	237
Activer l'installation permanente du client	239
Configurer DTLS	239
Inviter les utilisateurs distants	240
Activer le téléchargement du profil Secure Client (services client sécurisés)	241
Activer la mise à niveau différée Secure Client (services client sécurisés)	243
Activer la conservation DSCP	245
Activer les fonctionnalités Secure Client (services client sécurisés) supplémentaires	246
Activer le démarrage avant la connexion	246

Traduction des langues pour les messages utilisateur Secure Client (services client sécurisés)	247
Comprendre la traduction linguistique	247
Création de tableaux de traduction	247
Supprimer les tableaux de traduction	249
Configuration des fonctionnalités SSL avancées Secure Client (services client sécurisés)	250
Activer le renouvellement	251
Configurer	251
Activer les messages keepalive	253
Utiliser la compression	253
Ajuster la taille de la MTU	254
Mettre à jour les images Secure Client (services client sécurisés)	255
Activer l'accès VPN IPv6	255
SAML 2.0	256
Directives et limites relatives à SAML 2.0	258
Configurer un fournisseur d'identité (IdP) SAML 2.0	260
Configurer l'ASA en tant que fournisseur de services SAML 2.0	262
Configurer le navigateur du système d'exploitation par défaut pour l'authentification SAML	263
Configurer l'authentification par certificat et SAML	264
Exemple de SAML 2.0 et OneLogin	265
Dépannage de SAML 2.0	267
Surveiller les connexions Secure Client (services client sécurisés).	267
Déconnecter les sessions VPN AnyConnect	268
Historique des fonctionnalités pour les connexions Secure Client (services client sécurisés)	269

CHAPITRE 10

Secure Client (services client sécurisés) Analyse de l'hôte	271
Préalables pour la posture HostScan/Secure Firewall	271
Licences pour HostScan	271
Progiciel HostScan	272
Installer ou mettre à niveau HostScan/Secure Firewall Posture	272
Activer ou désactiver HostScan	273
Afficher la version de HostScan/Secure Firewall Posture activée sur l'ASA	274
Désinstaller HostScan/Secure Firewall Posture	274
Attribuer des modules de fonctionnalité Secure Client (services client sécurisés) aux stratégies de groupe	275

Documentation associée à HostScan/Secure Firewall Posture 276

CHAPITRE 11

Virtual Tunnel Interface 279

À propos des Virtual Tunnel Interfaces (Interfaces de tunnel virtuel) 279

Lignes directrices pour les interfaces Virtual Tunnel Interfaces 280

Créer un tunnel VTI 283

Ajouter une proposition IPsec (ensembles de transformations) 284

Ajouter un profil IPsec 285

Ajouter une interface VTI 287

Ajouter une interface VTI dynamique 290

Historique des fonctionnalités de Virtual Tunnel Interface 292

CHAPITRE 12

Configurer un serveur AAA externe pour le VPN 295

À propos des serveurs AAA externes 295

Comprendre l'application des politiques aux attributs d'autorisation 295

Lignes directrices relatives à l'utilisation de serveurs AAA externes 296

Configurer l'authentification de plusieurs certificats 296

Configurer plusieurs noms d'utilisateur de certificat 297

Configurer l'autorisation avec LDAP pour le VPN 298

Définir la configuration LDAP ASA 299

Attributs Cisco pris en charge pour l'autorisation LDAP 300

Types d'URL pris en charge dans les listes de contrôle d'accès 310

Lignes directrices relatives à l'utilisation des paires Cisco-AV 310

Syntaxe des attributs AV Pair Cisco 311

Exemples d'ACL à l'aide de paires Cisco-AV 312

Exemples d'autorisation d'accès à distance Active Directory/LDAP 313

Appliquer la politique aux attributs basés sur l'utilisateur 313

Appliquer l'affectation d'adresse IP statique pour les tunnels Secure Client (services client sécurisés)
315

Appliquer l'autorisation ou le refus d'accès entrant 317

Appliquer les règles d'heures de connexion et d'heure du jour 319



À propos de ce guide

Les rubriques suivantes expliquent comment utiliser ce guide.

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

Objectifs du document

L'objectif de ce guide est de vous aider à configurer VPN sur le 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.

Ce guide s'applique à la série ASA. 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, tels que les mots de passe, sont délimités par des crochets en chevron.
!, #	Un point d'exclamation (!) ou un dièse (#) au début d'une ligne de code indique une ligne de commentaire.

Alertes adressées aux lecteurs

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



Remarque

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



Astuces

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



Mise en garde

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

**Économiseur de temps**

Indique que l'action décrite permet de gagner du temps. Vous pouvez gagner du temps en exécutant l'action décrite dans le paragraphe.

**Avertissement**

signifie que le lecteur doit être averti. Dans cette situation, vous pourriez effectuer une opération risquant d'entraîner des blessures corporelles.

Communications, services et renseignements supplémentaires

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

Outil de recherche de bogues

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

IPsec et ISAKMP

- À propos de la tunnelisation, d'IPsec et d'ISAKMP, à la page 1
- Licences pour les VPN IPsec, à la page 7
- Lignes directrices relatives aux VPN IPsec, à la page 7
- Configurer ISAKMP, à la page 8
- Configurer IPsec, à la page 20
- Gestion des VPN IPsec, à la page 41

À propos de la tunnelisation, d'IPsec et d'ISAKMP

Ce sujet décrit les normes IPsec (Internet Protocol Security) et ISAKMP (Internet Security Association and Key Management Protocol) utilisées pour créer des réseaux privés virtuels (VPN).

La tunnellation permet d'utiliser un réseau TCP/IP public, comme Internet, pour créer des connexions sécurisées entre des utilisateurs distants et un réseau privé d'entreprise. Chaque connexion sécurisée s'appelle un tunnel.

L'ASA utilise les normes de tunnellation ISAKMP et IPsec pour créer et gérer les tunnels. ISAKMP et IPsec accomplissent les tâches suivantes :

- Négocier les paramètres du tunnel.
- Établir des tunnels.
- Authentifier les utilisateurs et les données.
- Gérer les clés de sécurité.
- Chiffrer et déchiffrer les données.
- Gérer le transfert de données dans le tunnel.
- Gérer le transfert de données entrant et sortant en tant que point terminal de tunnel ou routeur.

L'ASA fonctionne comme un point terminal de tunnel bidirectionnel. Il peut recevoir des paquets simples du réseau privé, les encapsuler, créer un tunnel et les envoyer à l'autre extrémité du tunnel où ils sont désencapsulés et envoyés à leur destination finale. Il peut également recevoir des paquets encapsulés du réseau public, les désencapsuler et les envoyer à leur destination finale sur le réseau privé.

Présentation d'IPsec

L'ASA utilise IPsec pour les connexions VPN de site à site et offre la possibilité d'utiliser IPsec pour les connexions VPN client à réseau local. Dans la terminologie IPsec, un *homologue* est un client d'accès à distance ou une autre passerelle sécurisée. Pour les deux types de connexion, l'ASA prend officiellement en charge uniquement les homologues Cisco. Comme nous respectons les normes de l'industrie VPN, les ASA peuvent fonctionner avec des homologues d'autres fournisseurs ; toutefois, nous ne les prenons pas en charge.

Lors de l'établissement du tunnel, les deux homologues négocient des associations de sécurité (SA) qui régissent l'authentification, le chiffrement, l'encapsulation et la gestion des clés. Ces négociations comportent deux phases : la première pour établir le tunnel (l'IKE SA) et la seconde pour régir le trafic dans le tunnel (l'IPsec SA).

Un VPN de LAN à LAN connecte des réseaux dans différents emplacements géographiques. Dans les connexions IPsec de site à site, l'ASA peut fonctionner comme initiateur ou répondeur. Dans les connexions client IPsec à réseau local, l'ASA fonctionne uniquement comme répondeur. Les initiateurs proposent des SA ; les répondeurs acceptent, rejettent ou font des contre-propositions, tout cela conformément aux paramètres SA configurés. Pour établir une connexion, les deux entités doivent convenir des SA.

Comprendre les tunnels IPsec

Les tunnels IPsec sont des ensembles de SA que l'ASA établit entre les homologues. Les SA précisent les protocoles et les algorithmes à appliquer aux données sensibles et précisent également le matériel de clé que les homologues utilisent. Les SA IPsec contrôlent la transmission réelle du trafic utilisateur. Les SA sont unidirectionnelles, mais sont généralement établies en paires (entrantes et sortantes).

Les homologues négocient les paramètres à utiliser pour chaque SA. Chaque SA comprend les éléments suivants :

- Ensembles de transformation IKEv1 ou propositions IKEv2
- cartes de chiffrement
- ACL
- Groupes de tunnels
- Politiques de préfragmentation

Survol d'ISAKMP et d'IKE

ISAKMP est le protocole de négociation qui permet à deux hôtes de s'accorder sur la façon de créer une association de sécurité IPsec (SA). Il fournit un cadre commun pour convenir du format des attributs SA. Cette association de sécurité comprend la négociation avec l'homologue au sujet de la SA, ainsi que la modification ou la suppression de la SA. ISAKMP sépare la négociation en deux étapes : la phase 1 et la phase 2. La phase 1 crée le premier tunnel, qui protège les messages de négociation ISAKMP ultérieurs. La phase 2 crée le tunnel qui protège les données.

IKE utilise ISAKMP pour configurer la SA pour l'utilisation d'IPsec. IKE crée les clés cryptographiques utilisées pour authentifier les homologues.

L'ASA prend en charge IKEv1 pour les connexions de l'ancien client VPN Cisco et IKEv2 pour le client VPN AnyConnect.

Pour définir les termes des négociations ISAKMP, vous créez une politique IKE, qui comprend les éléments suivants :

- Le type d'authentification requis pour l'homologue IKEv1, soit signature RSA à l'aide de certificats, soit clé prépartagée (PSK).
- Une méthode de chiffrement pour protéger les données et garantir la confidentialité.
- Une méthode HMAC (hachage de codes d'authentification de message) pour s'assurer de l'identité de l'expéditeur et pour s'assurer que le message n'a pas été modifié pendant le transfert.
- Un groupe Diffie-Hellman pour déterminer la force de l'algorithme de détermination de la clé de chiffrement. L'ASA utilise cet algorithme pour dériver les clés de chiffrement et de hachage.
- Pour IKEv2, une fonction pseudo-aléatoire (PRF) distincte est utilisée comme algorithme pour dériver les éléments de clé et effectuer les opérations de hachage nécessaires au chiffrement du tunnel IKEv2, entre autres.
- Une limite de temps pendant laquelle l'ASA utilise une clé de chiffrement avant de la remplacer.

Avec les politiques IKEv1, vous définissez une valeur pour chaque paramètre. Pour IKEv2, vous pouvez configurer plusieurs algorithmes de chiffrement et d'authentification, et plusieurs algorithmes d'intégrité pour une seule politique. L'ASA classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue selon cet ordre. Cet ordonnancement vous permet d'envoyer potentiellement une seule proposition pour transmettre toutes les transformations autorisées, au lieu d'envoyer chaque combinaison autorisée comme avec IKEv1.

L'ASA ne prend pas en charge les associations de sécurité multiples (SA) IKEv2. L'ASA accepte actuellement le trafic IPsec entrant uniquement sur la première SA trouvée. Si du trafic IPsec est reçu sur une autre SA, il est abandonné avec le motif `vpn-overlap-conflict`. Plusieurs SA IPsec peuvent résulter de tunnels dupliqués entre deux homologues, ou d'une tunnellation dissymétrique.

Comprendre les ensembles de transformations IKEv1 et les propositions IKEv2

Un ensemble de transformation IKEv1 ou une proposition IKEv2 est une combinaison de protocoles de sécurité et d'algorithmes qui définissent la façon dont l'ASA protège les données. Pendant les négociations d'une SA IPsec, les homologues doivent identifier un ensemble de transformation ou une proposition identique aux deux extrémités. L'ASA applique ensuite l'ensemble de transformation ou la proposition correspondante afin de créer une SA qui protège les flux de données de l'ACL associée à cette carte de chiffrement.

Avec les ensembles de transformation IKEv1, vous définissez une valeur pour chaque paramètre. Pour les propositions IKEv2, vous pouvez configurer plusieurs types de chiffrement et d'authentification ainsi que plusieurs algorithmes d'intégrité pour une seule proposition. L'ASA classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue selon cet ordre. Cela vous permet d'envoyer potentiellement une seule proposition pour transmettre toutes les combinaisons autorisées au lieu d'avoir besoin d'envoyer chaque combinaison autorisée individuellement, comme avec IKEv1.

L'ASA supprime le tunnel si vous modifiez la définition de l'ensemble de transformation ou de la proposition utilisée pour créer sa SA. Consultez la section [Effacer les associations de sécurité, à la page 43](#) pour obtenir de plus amples renseignements.



Remarque

Si vous effacez ou supprimez le seul élément d'un ensemble de transformation ou d'une proposition, l'ASA supprime automatiquement les références de carte de chiffrement qui y sont associées.

À propos de la carte de chiffrement IKEv2 multi-homologues

À partir de la version 9.14(1), ASA IKEv2 prend en charge la carte de chiffrement multi-homologues : lorsqu'un homologue d'un tunnel tombe en panne, IKEv2 tente d'établir le tunnel avec l'homologue suivant dans la liste. Vous pouvez configurer une carte de chiffrement avec un maximum de 10 adresses homologues. Cette prise en charge des homologues multiples par IKEv2 est particulièrement utile lorsque vous migrez depuis IKEv1 avec des cartes de chiffrement multi-homologues.

IKEv2 prend en charge uniquement les cartes de chiffrement bidirectionnelles. Par conséquent, les homologues multiples sont également configurés sur des cartes de chiffrement bidirectionnelles, et celles-ci servent aussi à accepter la demande des homologues qui initient le tunnel.

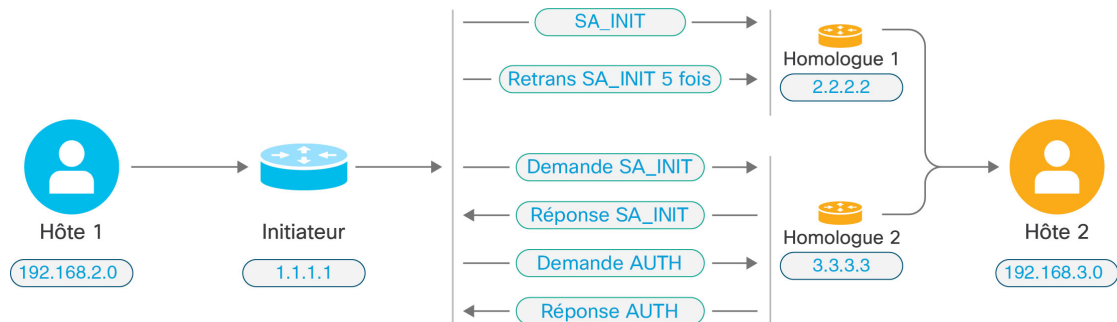
Comportement de l'initiateur IKEv2

IKEv2 initie une session avec un homologue, par exemple Peer1. Si Peer1 est inaccessible après 5 retransmissions SA_INIT, une retransmission finale est envoyée. Cette activité prend environ 2 minutes.

Lorsque Peer1 tombe en panne, le message SA_INIT est envoyé à Peer2. Si Peer2 est également inaccessible, l'établissement de la session est lancé avec Peer3 après 2 minutes.

Une fois que tous les homologues de la liste d'homologues de la carte de chiffrement ont été essayés, IKEv2 relance la session à partir de Peer1 jusqu'à ce qu'une SA soit établie avec l'un des homologues. La figure suivante illustre ce comportement.

Illustration 1 : Flux de processus de l'initiateur



Remarque

Un trafic continu est nécessaire pour initier l'IKE SA afin que chaque tentative échouée fasse passer à l'homologue suivant et qu'un homologue accessible finisse par établir la SA. En cas d'interruption du trafic, un déclenchement manuel est nécessaire pour initier l'IKE SA avec l'homologue suivant.

Comportement du répondeur IKEv2

Si le périphérique répondeur de l'IKE SA est configuré avec plusieurs homologues dans la carte de chiffrement, chaque fois qu'une IKE SA est tentée, l'adresse de l'initiateur de l'IKE SA est validée par rapport à celle de l'homologue actif courant dans la carte crypto.

Par exemple, si l'homologue actif courant dans la carte de chiffrement, utilisée comme répondeur, est le premier homologue, l'IKE SA est initiée à partir de l'adresse IP de Peer1. De même, si l'homologue actif

actuel dans la carte de chiffrement, utilisée comme répondeur, est le deuxième homologue, l'IKE SA est initiée à partir de l'adresse IP de Peer2.



Remarque Le parcours des homologues n'est pas pris en charge du côté répondeur dans une topologie IKEv2 multi-homologues.

Réinitialisation de l'index d'homologue lors des modifications de la carte de chiffrement

Toute modification de la carte de chiffrement réinitialise l'index d'homologue à zéro, et l'initiation du tunnel recommence à partir du premier homologue de la liste. Le tableau suivant présente la transition de l'index multi-homologues dans des conditions particulières :

Tableau 1 : Transition de l'index multi-homologues avant la SA

Conditions antérieures à SA	Index d'homologue déplacé Oui/Non/Réinitialiser
Homologue inaccessible	Oui
Incompatibilité de proposition de phase 1	Oui
Incompatibilité de proposition de phase 2	Oui
Accusé de réception DPD non reçu	Oui
Incompatibilité des sélecteurs de trafic pendant la phase d'authentification	Oui
Échec de l'authentification	Oui
Échec du renouvellement en raison d'un homologue inaccessible	Réinitialiser

Tableau 2 : Transition de l'index multi-homologues après la SA

Conditions après SA	Index d'homologue déplacé Oui/Non/Réinitialiser
Échec du renouvellement en raison d'une incompatibilité de proposition	Réinitialiser
Incompatibilité des sélecteurs de trafic lors du renouvellement	Réinitialiser
Modification de la carte de chiffrement	Réinitialiser
Basculement HA	Non
Effacer le chiffrement IKEv2 SA	Réinitialiser
Effacer ipsec sa	Réinitialiser

Conditions après SA	Index d'homologue déplacé Oui/Non/Réinitialiser
Délai d'expiration IKEv2 SA	Réinitialiser

Lignes directrices relatives à IKEv2 multi-homologues

Protocoles IKEv1 et IKEv2

Si une carte de chiffrement est configurée avec les deux versions IKE et plusieurs homologues, une tentative de SA est effectuée sur chaque homologue avec les deux versions avant de passer au suivant.

Par exemple, si une carte de chiffrement est configurée avec deux homologues, soit P1 et P2, le tunnel est initié vers P1 avec IKEv2, puis vers P1 avec IKEv1, puis vers P2 avec IKEv2, et ainsi de suite.

Haute disponibilité

Une carte de chiffrement avec plusieurs homologues initie des tunnels vers le périphérique répondeur qui se trouve en haute disponibilité. Elle passe au périphérique répondeur suivant lorsque le premier périphérique n'est pas accessible.

Un périphérique initiateur amorce des tunnels vers le périphérique répondeur. Si le périphérique actif tombe en panne, le périphérique en veille tente d'établir le tunnel à partir de l'adresse IP de Peer1, indépendamment du fait que la carte de chiffrement soit passée à l'adresse IP de Peer2 sur le périphérique actif.

Grappe centralisée

Une carte de chiffrement avec plusieurs homologues peut lancer des tunnels vers le périphérique répondeur qui se trouve dans un déploiement de grappe centralisée. Si le premier périphérique est inaccessible, il tente de passer au périphérique du répondeur suivant.

Un périphérique initiateur amorce des tunnels vers le périphérique répondeur. Chaque nœud de la grappe passe à Peer2 si Peer1 n'est pas accessible.

Grappe distribuée

La mise en grappe distribuée n'est pas prise en charge lorsqu'une carte de chiffrement IKEv2 multi-homologues est configurée.

Mode contexte multiple

En mode contexte multiple, le comportement multi-homologues est propre à chaque contexte.

Commandes de débogage

Si l'établissement du tunnel échoue, activez ces commandes pour analyser davantage le problème.

- `debug crypto ikev2 platform 255`
- `debug crypto ikev2 protocol 255`
- `debug crypto ike-common 255`

L'exemple suivant montre un journal de débogage propre à IKEv2 multi-homologues, qui affiche la transition des homologues.

```
Sep 13 10:08:58 [IKE COMMON DEBUG]Failed to initiate ikev2 SA with peer 192.168.2.2,  
initiate to next peer 192.168.2.3 configured in the multiple peer list of the crypto map.
```

Licences pour les VPN IPsec



Remarque Cette fonctionnalité n'est pas disponible sur les modèles sans chiffrement de charge utile.

Le VPN d'accès à distance IPsec utilisant IKEv2 nécessite une licence AnyConnect Plus ou Apex, disponible séparément. Le VPN d'accès à distance IPsec utilisant IKEv1 et le VPN de site à site IPsec utilisant IKEv1 ou IKEv2 utilise la licence Autre VPN fournie avec la licence Essentials. Consultez [les licences pour fonctionnalités de la gamme Cisco ASA](#) pour connaître les valeurs maximales par modèle.

Lignes directrices relatives aux VPN IPsec

Directives relatives au mode contextuel

Pris en charge en mode contexte unique ou multiple. Une licence AnyConnect Apex est requise pour le VPN d'accès à distance en mode multi-contexte. Bien que l'ASA ne reconnaisse pas spécifiquement une licence AnyConnect Apex, elle applique les caractéristiques d'une licence Apex, telles que AnyConnect Premium sous licence jusqu'à la limite de la plateforme, Secure Client (services client sécurisés) pour la mobilité, Secure Client (services client sécurisés) pour le téléphone VPN Cisco et l'évaluation avancée des points terminaux.

Directives sur le mode pare-feu

Pris en charge uniquement en mode de pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.

Directives en matière de basculement

- Les sessions VPN IPsec sont répliquées uniquement dans les configurations de basculement actif/veille.
- Lorsqu'un basculement se produit, le numéro de séquence ESP augmente de 25 millions pour empêcher un faux positif anti-rejeu.

Directives supplémentaires

Lorsque vous configurez IKE, le système réserve automatiquement les ports RADIUS UDP 1645 et 1646. Cette réservation est indiquée dans le journal système 713903, où les numéros de port sont affichés comme 27910 et 28166. Cette réservation garantit que les ports ne sont pas utilisés pour les traductions PAT.

Configurer ISAKMP

Configurer les politiques IKEv1 et IKEv2

IKEv1 et IKEv2 prennent chacune en charge un maximum de 20 politiques IKE, chacune avec un ensemble de valeurs différent. Attribuez une priorité unique à chaque politique que vous créez. Plus le numéro de priorité est faible, plus la priorité est élevée.

Lorsque la négociation IKE commence, l'homologue qui initie la négociation envoie toutes ses politiques à l'homologue distant, et l'homologue distant recherche une correspondance. L'homologue distant vérifie toutes les politiques de l'homologue par rapport à chacune de ses politiques configurées dans l'ordre de priorité (priorité la plus élevée en premier) jusqu'à ce qu'il trouve une correspondance.

Une correspondance existe lorsque les deux politiques des deux homologues contiennent les mêmes valeurs de chiffrement, de hachage, d'authentification et de paramètres Diffie-Hellman. Pour IKEv1, la politique d'homologue distante doit également spécifier une durée de vie inférieure ou égale à la durée de vie de la politique envoyée par l'initiateur. Si les durées de vie ne sont pas identiques, l'ASA utilise la durée de vie la plus courte. Pour IKEv2, la durée de vie n'est pas négociée mais gérée localement par chaque homologue, ce qui permet de la configurer indépendamment. S'il n'existe aucune correspondance acceptable, IKE refuse la négociation et la SA n'est pas établie.

Il existe un compromis implicite entre la sécurité et les performances lorsque vous choisissez une valeur spécifique pour chaque paramètre. Le niveau de sécurité fourni par les valeurs par défaut est adéquat pour les exigences de sécurité de la plupart des entreprises. Si vous interopérez avec un homologue qui ne prend en charge qu'une seule des valeurs d'un paramètre, votre choix se limite à cette valeur.

Vous devez inclure la priorité dans chacune des commandes ISAKMP. Le numéro de priorité identifie de manière unique la politique et détermine la priorité de la politique dans les négociations IKE.

Procédure

Étape 1 Pour créer une politique IKE, entrez la commande **crypto ikev1 | ikev2 policy** à partir du mode de configuration globale en mode contexte unique ou multiple. L'invite affiche le mode de configuration de politique IKE.

Exemple :

```
hostname(config)# crypto ikev1 policy 1
```

Remarque

Les nouvelles configurations ASA n'ont pas de politique IKEv1 ou IKEv2 par défaut.

Étape 2 Spécifiez l'algorithme de chiffrement. La valeur par défaut est AES-128.

encryption [aes | aes-192 | aes-256]

Exemple :

```
hostname(config-ikev1-policy)#  
encryption aes
```

Étape 3 Précisez l'algorithme de hachage. La valeur par défaut est SHA-1.

hash[sha]

Exemple :

```
hostname(config-ikev1-policy) #  
hash sha
```

Étape 4

Spécifiez la méthode d'authentification. La valeur par défaut est les clés prépartagées.

authentication[pre-shared]rsa-sig

Exemple :

```
hostname(config-ikev1-policy) # authentication rsa-sig
```

Étape 5

Précisez l'identifiant de groupe Diffie-Hellman. La valeur par défaut est Group 14.

group [14]

Exemple :

```
hostname(config-ikev1-policy) #  
group 14
```

Étape 6

Précisez la durée de vie de la SA. La valeur par défaut est 86 400 secondes (24 heures).

lifetime seconds

Exemple :

Cet exemple définit une durée de vie de 4 heures (14 400 secondes) :

```
hostname(config-ikev1-policy) # lifetime 14400
```

Étape 7

Précisez les paramètres supplémentaires à l'aide des mots-clés de politique IKEv1 et IKEv2 et leurs valeurs fournies dans [Valeurs et mots-clés de la politique IKE](#), à la page 9. Si vous ne spécifiez pas de valeur pour un paramètre de politique donné, la valeur par défaut s'applique.

Valeurs et mots-clés de la politique IKE

	Mot-clé	Signification	Description
authentication	rsa-sig	Un certificat numérique avec des clés générées par l'algorithme de signatures RSA	Spécifie la méthode d'authentification utilisée par l'ASA pour établir l'identité de chaque homologue IPsec.
	pre-share (pré-partage)(par défaut)	Clés prépartagées	Les clés prépartagées n'évoluent pas facilement avec un réseau en croissance, mais sont plus faciles à configurer dans un petit réseau.
encryption	AES(par défaut)	AES avec une clé de 128 bits	Spécifie l'algorithme de chiffrement symétrique qui protège les données transmises entre deux homologues IPsec. La valeur par défaut est une clé de 128 bits.

	Mot-clé	Signification	Description
hash	sha (par défaut)	SHA-1 (variante HMAC)	Spécifie l'algorithme de hachage utilisé pour assurer l'intégrité des données. Il garantit qu'un paquet provient bien de la source indiquée et qu'il n'a pas été modifié en cours de transit.
group			
	14 (par défaut)	Groupe 14 (2 048 bits)	Spécifie l'identifiant du groupe Diffie-Hellman, que les deux homologues IPsec utilisent pour dériver un secret partagé sans se le transmettre. Plus le numéro de groupe Diffie-Hellman est faible, moins il faut de temps CPU pour s'exécuter. Plus le numéro de groupe Diffie-Hellman est élevé, plus la sécurité est élevée. Le groupe par défaut est DH Group 14.
lifetime	integer value (valeur entière) (86 400 = par défaut)	120 à 2 147 483 647 secondes	Spécifie la durée de vie de la SA. La valeur par défaut est 86 400 secondes ou 24 heures. En règle générale, une durée de vie plus courte permet des négociations ISAKMP plus sécurisées (jusqu'à un certain point). Cependant, avec des durées de vie plus courtes, l'ASA configure les futures SA IPsec plus rapidement.

	Mot-clé	Signification	Description
integrity	sha (par défaut)	SHA-1 (variante HMAC)	Spécifie l'algorithme de hachage utilisé pour assurer l'intégrité des données. Il garantit qu'un paquet provient d'où il provient et qu'il n'a pas été modifié en cours de transit.
	sha256	SHA 2, condensé de 256 bits	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 256 bits.
	sha384	SHA 2, condensé de 384 bits	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 384 bits.
	sha512	SHA 2, condensé de 512 bits	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 512 bits.
	null (nul)		Lorsque AES-GCM est spécifié comme algorithme de chiffrement, un administrateur peut choisir NULL comme algorithme d'intégrité IKEv2.
encryption	aes (par défaut)	AES	Spécifie l'algorithme de chiffrement symétrique qui protège les données transmises entre deux homologues IPsec. La valeur par défaut est AES 128 bits.
	aes aes-192 aes-256		La norme de chiffrement avancé prend en charge les longueurs de clé de 128, 192 et 256 bits.

	Mot-clé	Signification	Description
	aes-gcm aes-gcm-192 aes-gcm-256 null	Options de l'algorithme AES-GCM à utiliser pour le chiffrement IKEv2	La norme de chiffrement avancé prend en charge les longueurs de clé de 128, 192 et 256 bits.
policy_index			Accède au sous-mode de politique IKEv2.
prf	sha (par défaut)	SHA-1 (variante HMAC)	Spécifie la fonction pseudo-aléatoire (PRF) — l'algorithme utilisé pour générer le matériel de dérivation de clés.
	sha256	SHA 2, condensé de 256 bits	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 256 bits.
	sha384	SHA 2, condensé de 384 bits	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 384 bits.
	sha512	SHA 2, condensé de 512 bits	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 512 bits.
priority			Étend le mode de politique pour prendre en charge les fonctionnalités IPsec V3 supplémentaires et intègre les paramètres AES-GCM et ECDH à la prise en charge de la suite B.
group	14 19 20 21 24	Groupe 14 (2 048 bits)	Spécifie l'identifiant du groupe Diffie-Hellman, que les deux homologues IPsec utilisent pour dériver un secret partagé sans se le transmettre. Plus le numéro de groupe Diffie-Hellman est faible, moins il faut de temps CPU pour s'exécuter. Plus le numéro de groupe Diffie-Hellman est élevé, plus la sécurité est élevée. La valeur par défaut est le groupe (DH) 14
lifetime	integer value (valeur entière) (86 400 = par défaut)	120 à 2 147 483 647 secondes	Spécifie la durée de vie de la SA. La valeur par défaut est 86 400 secondes ou 24 heures. En règle générale, une durée de vie plus courte permet des négociations ISAKMP plus sécurisées (jusqu'à un certain point). Cependant, avec des durées de vie plus courtes, l'ASA configure les futures SA IPsec plus rapidement.

Activer IKE sur l'interface externe.

Vous devez activer IKE sur l'interface qui termine le tunnel VPN. Il s'agit généralement de l'interface externe. Pour activer IKEv1 ou IKEv2, utilisez la commande `crypto [ikev1 | ikev2] enable interface-name` en mode de configuration globale, que ce soit en mode contexte unique ou multiple.

Par exemple :

```
hostname(config)# crypto ikev1 enable outside
```

Activer ou désactiver le mode agressif IKEv1

Les négociations IKEv1 de phase 1 peuvent utiliser le mode principal ou le mode agressif. Tous deux fournissent les mêmes services, mais le mode agressif ne nécessite que deux échanges entre les homologues pour un total de trois messages, plutôt que trois échanges pour un total de six messages. Le mode agressif est plus rapide, mais ne fournit pas de protection d'identité pour les parties qui communiquent. Par conséquent, les homologues doivent échanger des informations d'identification avant d'établir une SA sécurisée. Le mode agressif est activé par défaut.



Remarque

La désactivation du mode agressif empêche les clients VPN de Cisco d'utiliser l'authentification par clé prépartagée pour établir des tunnels vers l'ASA. Cependant, ils peuvent utiliser l'authentification basée sur les certificats (c'est-à-dire ASA ou RSA) pour établir les tunnels.

Pour activer le mode agressif pour les négociations de la phase 1 du protocole IKEv1, entrez la commande suivante en mode contexte unique ou multiple :

```
hostname(config)# crypto map <map-name> seq-num set ikev1 phase1-mode aggressive <group-name>
```

Pour désactiver le mode agressif, entrez la commande suivante en mode contexte unique ou multiple :

```
hostname(config)# crypto ikev1 am-disable
```

Si vous avez désactivé le mode agressif et que vous souhaitez le réactiver, utilisez la forme no de la commande. Par exemple :

```
hostname(config)# no crypto ikev1 am-disable
```

Configurer une méthode d'ID pour les homologues ISAKMP IKEv1 et IKEv2

Au cours des négociations de phase I ISAKMP IKEv1 ou IKEv2, les homologues doivent s'identifier les uns aux autres. Vous pouvez choisir la méthode d'identification parmi les options suivantes.

Address	Utilise les adresses IP des hôtes qui échangent des informations d'identité ISAKMP.
Automatic (par défaut)	Détermine la négociation ISAKMP par type de connexion : • Adresse IP pour la clé prépartagée • Nom distinctif du certificat pour l'authentification par certificat.
Hostname	Utilise le nom de domaine complet des hôtes échangeant les informations d'identité ISAKMP (par défaut). Ce nom comprend le nom d'hôte et le nom de domaine.
Key ID <i>key_id_string</i>	Spécifie la chaîne utilisée par l'homologue distant pour rechercher la clé prépartagée.

L'ASA utilise l'ID de phase I à envoyer à l'homologue. Cela est vrai pour tous les scénarios VPN, à l'exception des connexions IKEv1 LAN à LAN en mode principal qui s'authentifient au moyen de clés prépartagées.

Pour modifier la méthode d'identification des homologues, saisissez la commande suivante en mode monocontexte ou multicontexte :

crypto isakmp identity {*address* | *hostname* | **key-id** *id-string* | **auto**}

Par exemple, la commande suivante définit la méthode d'identification de l'homologue sur hostname :

```
hostname(config)# crypto isakmp identity hostname
```

Notification INVALID_SELECTORS

Si un système IPsec reçoit un paquet entrant sur une SA et que les champs d'en-tête du paquet ne sont pas cohérents avec les sélecteurs de la SA, il DOIT rejeter le paquet. L'entrée du journal d'audit pour cet événement comprend la date et l'heure actuelles, le SPI, le ou les protocoles IPsec, la source et la destination du paquet, toutes les autres valeurs de champ du paquet qui sont disponibles et les valeurs de sélecteur de l'entrée de SA correspondante. Le système génère et envoie une notification IKE de INVALID_SELECTORS à l'expéditeur (homologue IPsec), indiquant que le paquet reçu a été rejeté en raison d'un échec des vérifications du sélecteur.

L'ASA met déjà en œuvre la journalisation de cet événement dans CTM à l'aide du journal système existant affiché ci-dessous :

```
%ASA-4-751027: IKEv2 Received INVALID_SELECTORS Notification from peer: <peer IP>. Peer
received a packet (SPI=<spi>) from <local_IP>. The decapsulated inner packet didn't match
the negotiated policy in the SA. Packet destination <pkt_daddr>, port <pkt_dest_port>,
source <pkt_saddr>, port <pkt_src_port>, protocol <pkt_prot>
```

Un administrateur peut maintenant activer ou désactiver l'envoi d'une notification IKEv2 à l'homologue lorsqu'un paquet entrant est reçu sur une SA qui ne correspond pas aux sélecteurs de trafic de cette SA. Si elles sont activées, les messages de notification IKEv2 sont limités en fréquence à un message de notification par SA toutes les cinq secondes. La notification IKEv2 est envoyée dans un échange d'informations IKEv2 avec l'homologue.

Configurer la clé prépartagée IKEv2 en format hexadécimal

Vous pouvez configurer les clés prépartagées IKEv2 en hexadécimal en ajoutant le mot-clé *hex* aux commandes de clé prépartagée locale et distante.

```
ikev2 local-authentication pre-shared-key [ 0 | 8 | hex ] <string>
ikev2 remote-authentication pre-shared-key [ 0 | 8 | hex ] <string>
```

Activer ou désactiver l'envoi de la notification IKE

Un administrateur peut activer ou désactiver l'envoi d'une notification IKE à l'homologue lorsqu'un paquet entrant est reçu sur une connexion VPN IPsec IKEv2 qui ne correspond pas aux sélecteurs de trafic pour cette connexion. L'envoi de cette notification est désactivé par défaut. Envoi de notifications IKE INVALID_SELECTORS lorsque l'autorisation d'un nom d'utilisateur à partir du certificat ASDM est activée ou désactivée via la CLI suivante :

[no]crypto ikev2 notify invalid-selectors

Lors de l'authentification par certificat, le CN du certificat est le nom d'utilisateur, et l'autorisation est effectuée sur le serveur LOCAL. Si l'attribut « service-type » est récupéré, il est traité comme décrit précédemment.

Configurer les options de fragmentation IKEv2

Sur l'ASA, la fragmentation IKEv2 peut être activée ou désactivée, la MTU utilisée lors de la fragmentation des paquets IKEv2 peut être précisée et une méthode de fragmentation préférée peut être configurée par l'administrateur à l'aide de la commande suivante :

[no] crypto ikev2 fragmentation [mtu <mtu-size>] | [preferred-method [ietf | cisco]]

Par défaut, toutes les méthodes de fragmentation IKEv2 sont activées, la MTU est de 576 pour IPv4 ou de 1280 pour IPv6, et la méthode préférée est la norme IETF RFC-7383.

Précisez la **[mtu <mtu-size>]** en tenant compte des considérations suivantes :

- La valeur MTU utilisée doit inclure l'en-tête IP (IPv4/IPv6) et la taille d'en-tête UDP.
- Si elle n'est pas précisée par l'administrateur, la MTU par défaut est de 576 pour IPv4 ou de 1 280 pour IPv6.
- Une fois précisée, la même MTU sera utilisée pour IPv4 et IPv6.
- La plage valide est de 68 à 1 500.



Remarque

Vous devez prendre en compte le surdébit ESP lors de la configuration de la MTU. La taille des paquets augmente après le chiffrement en raison du surdébit ESP ajouté à la MTU pendant le chiffrement. Si vous obtenez l'erreur « paquet trop volumineux », veuillez à vérifier la taille de la MTU et à configurer une MTU inférieure.

L'une des méthodes de fragmentation suivantes prises en charge peut être configurée comme méthode de fragmentation préférée pour IKEv2 **[preferred-method [ietf | cisco]]** :

- Fragmentation IKEv2 basée sur la norme IETF RFC-7383.
 - Cette méthode sera utilisée lorsque les deux homologues précisent la prise en charge et la préférence durant la négociation.
 - À l'aide de cette méthode, le chiffrement est effectué après la fragmentation, ce qui assure une protection individuelle pour chaque message de fragment IKEv2.
- Fragmentation propriétaire Cisco.
 - Cette méthode sera utilisée s'il s'agit de la seule méthode fournie par un homologue, tel que le Secure Client (services client sécurisés), ou si les deux homologues précisent la prise en charge et les préférences pendant la négociation.
 - À l'aide de cette méthode, la fragmentation est effectuée après le chiffrement. L'homologue de réception ne peut pas déchiffrer ou authentifier le message tant que tous les fragments ne sont pas reçus.
 - Cette méthode n'est pas interopérable avec des homologues non Cisco.

La commande **show running-config crypto ikev2** affiche la configuration actuelle et **show crypto ikev2 sa detail** affiche la MTU appliquée si la fragmentation a été utilisée pour la SA.

Avant de commencer

- Le chemin de découverte de MTU n'est pas pris en charge, la MTU doit être configurée manuellement pour correspondre aux besoins du réseau.
- Cette configuration est globale et aura une incidence sur les futurs SA établies après son application. Les anciennes SA ne seront pas touchées. Le même comportement s'applique lorsque la fragmentation est désactivée.
- Un maximum de 100 fragments peut être reçu.

Exemples

- Pour désactiver la fragmentation IKEv2 :

```
no crypto ikev2 fragmentation
```

- Pour rétablir l'opération par défaut :

```
crypto ikev2 fragmentation
```

ou

```
crypto ikev2 fragmentation mtu 576  
preferred-method ietf
```

- Pour modifier la valeur MTU à 600 :

```
crypto ikev2 fragmentation mtu 600
```

- Pour restaurer la valeur MTU par défaut :

```
no crypto ikev2 fragmentation mtu 576
```

- Pour définir Cisco comme méthode de fragmentation préférée :

```
crypto ikev2 fragmentation preferred-method cisco
```

- Pour restaurer la méthode de fragmentation préférée dans IETF :

```
no crypto ikev2 fragmentation preferred-method cisco
```

ou

```
crypto ikev2 fragmentation preferred-method ietf
```

Authentification AAA avec autorisation

```
aaa authentication http console LOCAL  
aaa authorization http console radius
```

L'authentification AAA est effectuée sur le serveur LOCAL à l'aide du nom d'utilisateur et du mot de passe saisis par l'utilisateur. Une autorisation supplémentaire est effectuée sur le serveur *radius* en utilisant le même nom d'utilisateur. L'attribut *service-type*, s'il est récupéré, est traité comme décrit précédemment.

Activer IPsec sur NAT-T

NAT-T permet aux homologues IPsec d'établir une connexion par l'intermédiaire d'un périphérique NAT. Il le fait en encapsulant le trafic IPsec dans des datagrammes UDP, en utilisant le port 4500, qui fournit aux périphériques NAT des informations de port. NAT-T détecte automatiquement tous les périphériques NAT et encapsule le trafic IPsec uniquement lorsque cela est nécessaire.



Remarque

En raison d'une limitation de Secure Client (services client sécurisés), vous devez activer NAT-T pour que Secure Client (services client sécurisés) se connecte avec succès à l'aide de IKEv2. Cette exigence s'applique même si le client ne se trouve pas derrière un périphérique NAT-T.

L'ASA peut prendre en charge simultanément IPsec standard, IPsec sur TCP, NAT-T et IPsec sur UDP, selon le client avec lequel il échange des données.

La ventilation suivante montre les connexions pour chaque option activée.

Options	Fonction activée	Position du client	Fonction utilisée
Option 1	Si NAT-T est activé	et le client se trouve derrière la NAT, alors	NAT-T est utilisé
		et qu'aucune NAT n'existe, alors	L'IPsec natif (ESP) est utilisé
Option 2	Si IPsec sur UDP est activé	et le client se trouve derrière la NAT, alors	IPsec sur UDP est utilisé
		et qu'aucune NAT n'existe, alors	IPsec sur UDP est utilisé
Option 3	Si NAT-T et IPsec sur UDP sont activés	et le client se trouve derrière la NAT, alors	NAT-T est utilisé
		et qu'aucune NAT n'existe, alors	IPsec sur UDP est utilisé



Remarque

Lorsque IPsec sur TCP est activé, il prévaut sur toutes les autres méthodes de connexion.

Lorsque vous activez NAT-T, l'ASA ouvre automatiquement le port 4500 sur toutes les interfaces compatibles avec IPsec.

L'ASA prend en charge plusieurs homologues IPsec derrière un seul périphérique NAT/PAT fonctionnant dans des déploiements LAN à LAN ou d'accès à distance, mais pas simultanément pour les deux types sur le même équipement NAT/PAT. Dans un environnement mixte, les tunnels d'accès à distance échouent dans la négociation, car tous les homologues semblent provenir de la même adresse IP publique, celle du périphérique NAT. De plus, les tunnels d'accès à distance échouent dans un environnement mixte, car ils utilisent souvent le même nom que le groupe de tunnels LAN à LAN (c'est-à-dire l'adresse IP du périphérique NAT). Cette correspondance peut provoquer des échecs de négociation entre plusieurs homologues dans un environnement mixte de site à site et d'accès à distance d'homologues derrière le périphérique NAT.

Pour utiliser NAT-T, effectuez les étapes suivantes de site à site en mode contexte unique ou multiple :

Procédure

- Étape 1** Entrez la commande suivante pour activer IPsec sur NAT-T globalement sur l'ASA :
- ```
crypto isakmp nat-traversal natkeepalive
```
- La plage pour l'argument natkeepalive est de 10 à 3600 secondes. La valeur par défaut est de 20 secondes.
- Exemple :**
- Entrez la commande suivante pour activer NAT-T et définir la valeur keepalive à une heure :
- ```
hostname(config)# crypto isakmp nat-traversal 3600
```
- Étape 2** Sélectionnez l'option before-encryption pour la politique de fragmentation IPsec en entrant cette commande :
- ```
hostname(config)# crypto ipsec fragmentation before-encryption
```
- Cette option permet au trafic de traverser des périphériques NAT qui ne prennent pas en charge la fragmentation IP. Cela n'affecte pas le fonctionnement des périphériques NAT qui prennent en charge la fragmentation IP.

## Activer IPsec avec IKEv1 sur TCP

IPsec sur TCP encapsule les protocoles IKEv1 et IPsec dans un paquet de type TCP et permet la tunnellation sécurisée au travers des périphériques NAT et PAT ainsi que des pare-feu. Par défaut, cette fonction est désactivée. IPsec/IKEv1 sur TCP permet à un client VPN Cisco de fonctionner dans un environnement où l'ESP standard ou IKEv1 ne peut pas fonctionner, ou ne peut fonctionner qu'au prix d'une modification des règles de pare-feu existantes.



**Remarque** Cette fonctionnalité ne fonctionne pas avec les pare-feu basés sur un proxy.

IPsec sur TCP fonctionne avec les clients d'accès à distance. Vous activez IPsec sur TCP sur l'ASA et sur le client auquel il se connecte. Sur l'ASA, il est activé de façon globale et fonctionne sur toutes les interfaces où IKEv1 est activé. Il ne fonctionne pas pour les connexions LAN à LAN.

L'ASA peut prendre en charge simultanément IPsec standard, IPsec sur TCP, NAT-Traversal et IPsec sur UDP, selon le client avec lequel il échange des données. IPsec sur TCP, s'il est activé, prévaut sur toutes les autres méthodes de connexion.

Vous pouvez activer IPsec sur TCP pour un maximum de 10 ports que vous spécifiez. Si vous saisissez un port bien connu, par exemple le port 80 (HTTP) ou le port 443 (HTTPS), le système affiche un avertissement indiquant que le protocole associé à ce port ne fonctionne plus sur l'interface publique. Par conséquent, vous ne pouvez plus utiliser de navigateur pour gérer l'ASA au moyen de l'interface publique. Pour résoudre ce problème, reconfigurez la gestion HTTP/HTTPS sur différents ports.

Le port par défaut est 10 000.

Vous devez configurer les ports TCP sur le client ainsi que sur l'ASA. La configuration du client doit inclure au moins un des ports que vous avez définis pour l'ASA.

Pour activer globalement IPsec sur TCP pour IKEv1 sur l'ASA, saisissez la commande suivante en mode monocontexte ou multicontexte :

**crypto ikev1 ipsec-over-tcp [port port 1...port0]**

Cet exemple active IPsec sur TCP sur le port 45 :

```
hostname(config)# crypto ikev1 ipsec-over-tcp port 45
```

## Configurer la correspondance de groupe de certificats pour IKEv1

Les groupes de tunnels définissent les conditions de connexion et les autorisations des utilisateurs. La correspondance de groupe de certificats vous permet d'associer un utilisateur à un groupe de tunnels en utilisant soit le DN du sujet, soit le DN de l'émetteur du certificat utilisateur.



### Remarque

La correspondance de groupe de certificats s'applique uniquement aux connexions IKEv1 et IKEv2 LAN à LAN. Les connexions d'accès à distance IKEv2 prennent en charge la sélection de groupe dans une liste déroulante configurée dans les webvpn-attributes du tunnel-group et dans le mode de configuration webvpn pour certificate-group-map, et ainsi de suite.

Pour faire correspondre les utilisateurs aux groupes de tunnels en fonction de ces champs du certificat, vous devez d'abord créer des règles qui définissent un critère de correspondance, puis associer chaque règle au groupe de tunnels souhaité.

Pour créer une correspondance de certificats, utilisez la commande **use the crypto ca certificate map**. Pour définir un groupe de tunnels, utilisez la commande **tunnel-group**.

Vous devez également configurer une politique de correspondance de groupe de certificats, en précisant si la correspondance du groupe doit être établie à partir des règles, du champ de l'unité organisationnelle (OU) ou d'un groupe par défaut pour tous les utilisateurs de certificats. Vous pouvez utiliser une ou toutes ces méthodes.

## Procédure

### Étape 1

Pour configurer la politique et les règles selon lesquelles les sessions ISAKMP fondées sur des certificats sont associées à des groupes de tunnels, et pour associer les entrées de correspondance de certificats aux groupes de tunnels, saisissez la commande **tunnel-group-map** en mode monocontexte ou multicontexte.

**tunnel-group-map enable {rules | ou | ike-id | peer ip}**

**tunnel-group-map [rule-index] enable policy**

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>politique</i>      | <p>Spécifie la politique utilisée pour dériver le nom du groupe de tunnels à partir du certificat. La politique peut être l'une des suivantes :</p> <p><i>ike-id</i> : indique que si un groupe de tunnels n'est pas déterminé selon une recherche de règle ou tiré de l'OU, les sessions ISAKMP fondées sur des certificats sont alors associées à un groupe de tunnels en fonction du contenu de l'ID ISAKMP de phase1.</p> <p><i>ou</i> : indique que si un groupe de tunnels n'est pas déterminé selon une recherche de règle, il faut alors utiliser la valeur de l'OU dans le nom distinctif (DN) du sujet.</p> <p><i>peer-ip</i> : indique que si un groupe de tunnels n'est pas déterminé selon une recherche de règle ni tiré des méthodes OU ou ike-id, il faut alors utiliser l'adresse IP de l'homologue.</p> <p><i>rules</i> : indique que les sessions ISAKMP fondées sur des certificats sont associées à un groupe de tunnels selon les associations de correspondance de certificats configurées par cette commande.</p> |
| <i>index de règle</i> | (Facultatif) fait référence aux paramètres spécifiés par la commande <b>crypto ca certificate map</b> . Les valeurs sont comprises entre 1 et 65 535.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Tenez compte des éléments suivants :

- Vous pouvez appeler cette commande plusieurs fois tant que chaque appel est unique et que vous ne faites pas référence à un index de correspondance plus d'une fois.
- Les règles ne peuvent pas dépasser 255 caractères.
- Vous pouvez affecter plusieurs règles au même groupe. Pour ce faire, ajoutez d'abord la priorité de la règle et le groupe. Vous définissez ensuite autant de critères que nécessaires pour chaque groupe. Lorsque plusieurs règles sont affectées au même groupe, la première règle dont la condition est vérifiée est appliquée.
- En créant une règle unique, vous pouvez exiger que tous les critères soient satisfaits avant d'affecter un utilisateur à un groupe de tunnels spécifique. Exiger la mise en correspondance de tous les critères équivaut à une opération ET logique. Sinon, créez une règle pour chaque critère si vous souhaitez exiger qu'une seule correspondance avant d'affecter un utilisateur à un groupe de tunnels spécifique. L'exigence d'un seul critère pour la mise en correspondance équivaut à une opération OU logique.

## Étape 2

Précisez un groupe de tunnels par défaut à utiliser lorsque la configuration ne spécifie pas de groupe de tunnels.

La syntaxe est **tunnel-group-map** [*rule-index*] **default-group** *tunnel-group-name* où *rule-index* est la priorité de la règle, et le nom du groupe de tunnels doit correspondre à un groupe de tunnels qui existe déjà.

## Exemples

L'exemple suivant permet le mappage des sessions ISAKMP basées sur des certificats avec un groupe de tunnels en fonction du contenu de l'ID ISAKMP phase1 :

```
hostname(config)# tunnel-group-map enable ike-id
```

L'exemple suivant permet le mappage des sessions ISAKMP basées sur des certificats vers un groupe de tunnels en fonction de l'adresse IP de l'homologue :

```
hostname(config)# tunnel-group-map enable peer-ip
```

L'exemple suivant permet le mappage des sessions ISAKMP basées sur des certificats en fonction de l'unité d'organisation (OU) dans le nom distinctif (DN) du sujet :

```
hostname(config)# tunnel-group-map enable ou
```

L'exemple suivant permet le mappage des sessions ISAKMP basées sur des certificats en fonction des règles établies :

```
hostname(config)# tunnel-group-map enable rules
```

## Configurer IPsec

Cette section décrit les procédures requises pour configurer l'ASA lors de l'utilisation d'IPsec pour mettre en œuvre un VPN.

### Définir les cartes de chiffrement

*Les cartes de chiffrement* définissent la politique IPsec à négocier dans la SA IPsec. Elles comprennent les éléments suivants :

- ACL pour identifier les paquets que la connexion IPsec autorise et protège.
- Identification des homologues.
- Adresse locale pour le trafic IPsec. (Voir [Appliquer les cartes de chiffrement aux interfaces, à la page 29](#) pour plus de détails.)
- Jusqu'à 11 ensembles de transformation IKEv1 ou propositions IKEv2, avec lesquels tenter de faire correspondre les paramètres de sécurité homologues.

Un *ensemble de cartes de chiffrement* se compose d'une ou de plusieurs cartes de chiffrement qui ont le même nom de carte. Vous créez un ensemble de cartes de chiffrement lorsque vous créez sa première carte de chiffrement. La tâche de site à site suivante crée ou ajoute une carte de chiffrement en mode contexte unique ou multiple :

```
crypto map map-name seq-num match address access-list-name
```

Utilisez le nom de liste d'accès pour spécifier l'ID d'ACL, sous forme de chaîne ou d'entier d'une longueur maximale de 241 caractères.



#### Astuces

Utilisez toutes les lettres majuscules pour identifier plus facilement l'ID d'ACL dans votre configuration.

Vous pouvez continuer à entrer cette commande pour ajouter des cartes de chiffrement à l'ensemble de cartes de chiffrement. Dans l'exemple suivant, *mymap* est le nom de l'ensemble de cartes de chiffrement auquel vous pourriez ajouter des cartes de chiffrement :

### **crypto map mymap 10 match address 101**

Le *numéro de séquence (seq-num)* affiché dans la syntaxe ci-dessus distingue une carte de chiffrement d'une autre carte portant le même nom. Le numéro de séquence attribué à une carte de chiffrement détermine également sa priorité par rapport aux autres cartes de chiffrement d'un ensemble de cartes de chiffrement. Plus le numéro de séquence est bas, plus la priorité est élevée. Après avoir affecté un ensemble de cartes de chiffrement à une interface, l'ASA évalue tout le trafic IP passant par l'interface par rapport aux cartes de chiffrement de l'ensemble, en commençant par la carte de chiffrement ayant le numéro de séquence le plus bas.

**[no] crypto map map\_name map\_index set pfs [group14 | group15 | group16 | group19 | group20 | group21 ]**

Spécifie le groupe ECDH utilisé pour la confidentialité de transmission parfaite (PFS) pour la carte de chiffrement. Empêche de configurer les options group14 et group24 pour une carte de chiffrement (lors de l'utilisation d'une politique IKEv1).

**[no] crypto map map\_name seq-num set reverse-route [dynamic]**

Active l'injection de route inverse (RRI) pour toute connexion basée sur cette entrée de carte de chiffrement. Si *dynamic* n'est pas spécifié, la RRI est effectuée lors de la configuration et est considérée comme statique, restant en place jusqu'à ce que la configuration soit modifiée ou supprimée. En outre, chaque fois qu'une route RRI est configurée avec la même destination pour laquelle une route statique existe déjà, la route statique existante est supprimée et la route RRI est installée. L'ASA ajoute automatiquement des routes statiques à la table de routage et communique ces routes à son réseau privé ou aux routeurs de frontière à l'aide d'OSPF. N'activez pas RRI si vous spécifiez une source/destination (0.0.0.0/0.0.0.0) comme réseau protégé, car cela aura une incidence sur le trafic qui utilise votre route par défaut.



**Remarque** Utilisez un réseau spécifique pour RRI, car cela ne fonctionnera pas si vous choisissez le réseau protégé comme « any ».

Si *dynamic* est spécifié, les routes sont créées lors de l'établissement réussi des associations de sécurité (SA) IPsec et supprimées après la suppression des SA IPsec.

Vous ne pouvez pas configurer une carte de chiffrement dynamique portant le même nom qu'une carte de chiffrement statique, et vice versa, même si l'une des cartes de chiffrement n'est pas actuellement utilisée.



**Remarque** La RRI dynamique est prise en charge sur les cartes de chiffrement statiques basées sur IKEv2 uniquement.

**[no] crypto map name priority set validate-icmp-errors**

OU

**[no]crypto dynamic-map name priority set validate-icmp-errors**

Spécifie si les messages d'erreur ICMP entrants sont validés pour la carte de chiffrement ou de chiffrement dynamique.

**[no] crypto map <name> <priority> set df-bit [clear-df | copy-df | set-df]**

OU

**[no] crypto map dynamic-map <name> <priority> set df-bit [clear-df | copy-df | set-df]**

Configure la politique existante de ne pas fragmenter (DF) (à un niveau d'association de sécurité) pour la carte de chiffrement ou de chiffrement dynamique.

- *clear-df* : ignore le bit DF.
- *copy-df* : maintient le bit DF.
- *set-df* : définit et utilise le bit DF.

**[no] crypto map <name> <priority> set tfc-packets [burst <length | auto>] [payload-size <bytes | auto>] [timeout <seconds | auto>]**

OU

**[no] crypto dynamic-map <name> <priority> set tfc-packets [burst <length | auto>] [payload-size <bytes | auto>] [timeout <seconds | auto>]**

Un administrateur peut activer des paquets factices de confidentialité de flux de trafic (TFC) à des longueurs et à des intervalles aléatoires sur une association de sécurité IPsec. Vous devez avoir une proposition IKEv2 IPsec définie avant d'activer TFC.



#### Remarque

L'activation des paquets de confidentialité du flux de trafic empêche le délai d'expiration d'inactivité du VPN.

L'ACL attribuée à une carte de chiffrement se compose de toutes les ACE ayant le même nom d'ACL, comme indiqué dans la syntaxe de commande suivante :

**access-list access-list-name {deny | permit} ip source source-netmask destination destination-netmask**

Vous créez une ACL lorsque vous créez sa première ACE. La syntaxe de commande suivante crée ou ajoute à une ACL :

**access-list access-list-name {deny | permit} ip source source-netmask destination destination-netmask**

Dans l'exemple suivant, l'ASA applique les protections IPsec attribuées à la carte de chiffrement à tout le trafic circulant du sous-réseau 10.0.0.0 vers le sous-réseau 10.1.1.0 :

**access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0**

La carte de chiffrement qui correspond au paquet détermine les paramètres de sécurité utilisés dans les négociations d'une SA. Si l'ASA local amorce la négociation, il utilise la politique spécifiée dans la carte de chiffrement statique pour créer l'offre à envoyer à l'homologue spécifié. Si l'homologue amorce la négociation, l'ASA tente de faire correspondre la politique à une carte de chiffrement statique et, en cas d'échec, tente de la faire correspondre à l'une des cartes de chiffrement dynamiques de l'ensemble de cartes de chiffrement, afin de décider s'il accepte ou refuse l'offre de l'homologue.

Pour que deux homologues réussissent à établir une SA, ils doivent avoir au moins une carte de chiffrement compatible. Pour être compatible, une carte de chiffrement doit respecter les critères suivants :

- La carte de chiffrement doit contenir des listes de contrôle d'accès de chiffrement compatibles (par exemple, listes de contrôle d'accès d'image miroir). Si l'homologue qui répond utilise des cartes de chiffrement dynamiques, l'ASA doit également contenir des listes de contrôle d'accès de chiffrement compatibles comme condition requise pour appliquer IPsec.

- Chaque carte de chiffrement identifie l'autre homologue (sauf si l'homologue qui répond utilise des cartes de chiffrement dynamiques).
- Les cartes de chiffrement ont au moins un ensemble de transformation ou une proposition en commun.

Vous ne pouvez appliquer qu'un seul ensemble de cartes de chiffrement à une seule interface. Créez plusieurs cartes de chiffrement pour une interface particulière sur l'ASA si l'une des conditions suivantes existe :

- Vous souhaitez que des homologues spécifiques gèrent différents flux de données.
- Vous souhaitez que différentes sécurités IPsec s'appliquent à différents types de trafic.

Par exemple, créez une carte de chiffrement et attribuez une liste de contrôle d'accès pour identifier le trafic entre deux sous-réseaux et attribuez un ensemble de transformation IKEv1 ou une proposition IKEv2. Créez une autre carte de chiffrement avec une liste de contrôle d'accès différente pour identifier le trafic entre deux autres sous-réseaux et appliquez un ensemble de transformation ou une proposition avec des paramètres VPN différents.

Si vous créez plusieurs cartes de chiffrement pour une interface, spécifiez un numéro de séquence (seq-num) pour chaque entrée de carte afin de déterminer sa priorité dans l'ensemble de cartes de chiffrement.

Chaque ACE contient une instruction d'autorisation ou de refus. Le tableau suivant explique les significations particulières des ACE permit et deny dans les listes de contrôle d'accès appliquées aux cartes de chiffrement.

| Résultat de l'évaluation de la carte de chiffrement                                                          | Intervention                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Critère de correspondance dans une commande ACE contenant une déclaration d'autorisation                     | Interrompt l'évaluation du paquet par rapport aux ACE restantes dans l'ensemble de cartes de chiffrement, puis évalue les paramètres de sécurité du paquet par rapport à ceux des ensembles de transformation IKEv1 ou des propositions IKEv2 attribués à la carte de chiffrement. Après avoir fait correspondre les paramètres de sécurité à ceux d'un ensemble ou d'une proposition de transformation, l'ASA applique les paramètres IPsec associés. En règle générale, pour le trafic sortant, cela signifie qu'il chiffre, authentifie et achemine le paquet. |
| Critère de correspondance dans une ACE contenant une instruction de refus                                    | Interrompt l'évaluation du paquet par rapport aux ACE restantes dans la carte de chiffrement en cours d'évaluation, puis reprend l'évaluation par rapport aux ACE de la carte de chiffrement suivante, selon le numéro de séquence suivant qui lui est attribué.                                                                                                                                                                                                                                                                                                  |
| Échec de la correspondance de toutes les ACE d'autorisation testées dans l'ensemble de cartes de chiffrement | Acheminez le paquet sans le chiffrer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Les ACE contenant des instructions de refus filtrent le trafic sortant qui ne nécessite pas de protection IPsec (par exemple, le trafic de protocole de routage). Par conséquent, insérez des instructions de refus initiales pour filtrer le trafic sortant qui ne doit pas être évalué en fonction des instructions d'autorisation dans une liste de contrôle d'accès de chiffrement.

Pour un paquet entrant chiffré, l'appareil de sécurité utilise l'adresse source et le SPI ESP pour déterminer les paramètres de déchiffrement. Après que l'appareil de sécurité a déchiffré le paquet, il compare l'en-tête interne du paquet déchiffré aux ACE permit de l'ACL associée à la SA du paquet. Si l'en-tête interne ne

correspond pas au proxy, l'appareil de sécurité abandonne le paquet. Si l'en-tête interne correspond au proxy, l'appareil de sécurité achemine le paquet.

Lors de la comparaison de l'en-tête interne d'un paquet entrant qui n'a pas été chiffré, l'appareil de sécurité ignore toutes les règles de refus, car elles empêcheraient l'établissement d'une SA de phase 2.

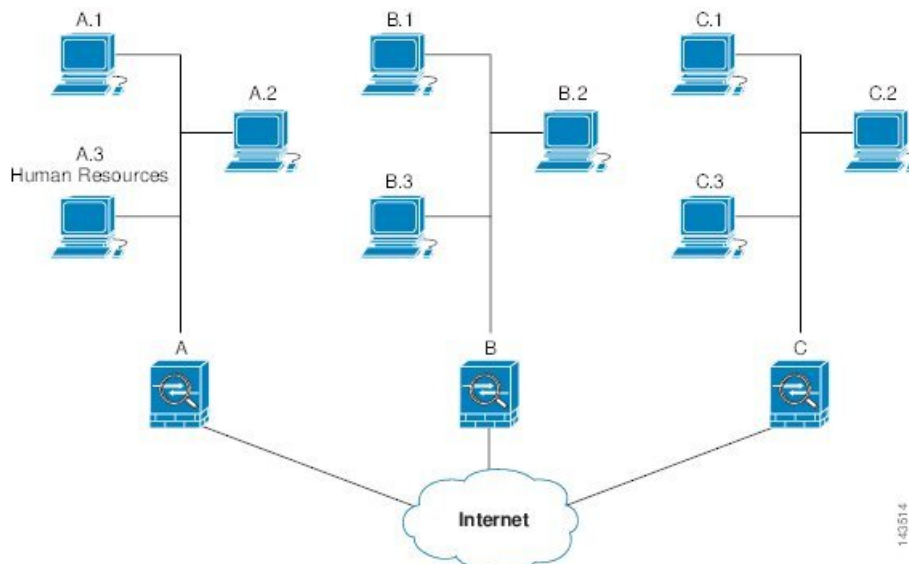


#### Remarque

Pour acheminer le trafic entrant non chiffré en texte clair, insérez les ACE de refus avant les ACE d'autorisation. L'ASA ne peut pas transmettre plus de 28 ACE dans une liste d'accès de tunnellation fractionnée.

## Exemple de cartes de chiffrement LAN à LAN

L'objectif de la configuration des appareils de sécurité A, B et C dans cet exemple de réseau LAN à LAN est de permettre la tunnellation de tout le trafic provenant de l'un des hôtes et destiné à l'un des autres hôtes. Cependant, comme le trafic de l'hôte A.3 contient des données sensibles du service des ressources humaines, il nécessite un chiffrement renforcé et un renouvellement plus fréquent que l'autre trafic. Vous voudrez donc attribuer un ensemble de transformation spécial pour le trafic de l'hôte A.3.



La notation d'adresse simple indiquée dans cette figure et utilisée dans l'explication suivante est une expression conceptuelle. Un exemple avec des adresses IP réelles suit l'explication.

Pour configurer l'appareil de sécurité A pour le trafic sortant, vous créez deux cartes de chiffrement, l'une pour le trafic de l'hôte A.3 et l'autre pour le trafic des autres hôtes du réseau A, comme illustré dans l'exemple suivant :

```
Crypto Map Seq_No_1
 deny packets from A.3 to B
 deny packets from A.3 to C
 permit packets from A to B
 permit packets from A to C
Crypto Map Seq_No_2
 permit packets from A.3 to B
 permit packets from A.3 to C
```

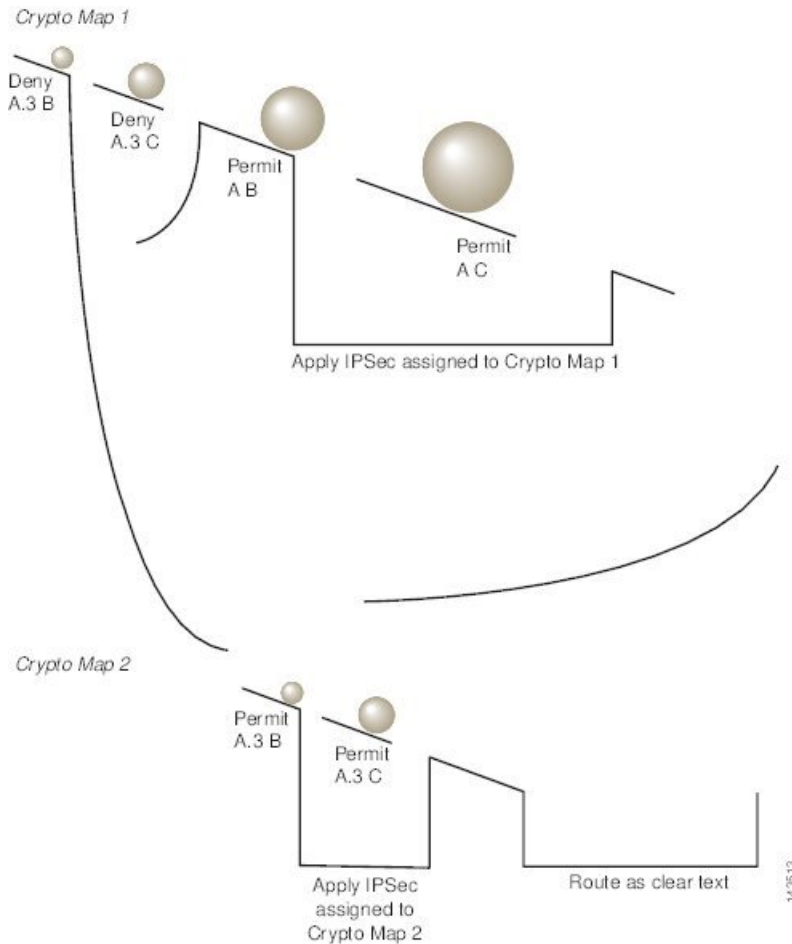


Après avoir créé les listes de contrôle d'accès, vous attribuez un ensemble de transformation à chaque carte de chiffrement pour appliquer l'IPsec requis à chaque paquet correspondant.

Les ACL en cascade consistent à insérer des ACE de refus pour contourner l'évaluation par rapport à une ACL et reprendre l'évaluation par rapport à une ACL suivante dans l'ensemble de cartes de chiffrement. Comme vous pouvez associer chaque carte de chiffrement à des paramètres IPsec différents, vous pouvez utiliser les ACE de refus pour exclure le trafic spécial d'une évaluation plus approfondie dans la carte de chiffrement correspondante et faire correspondre le trafic spécial pour permettre aux instructions d'une autre carte de chiffrement de fournir ou d'exiger une sécurité différente. Le numéro de séquence attribué à l'ACL de chiffrement détermine sa position dans la séquence d'évaluation au sein de l'ensemble de cartes de chiffrement.

L'illustration suivante montre les ACL en cascade créées à partir des ACE conceptuelles dans cet exemple. La signification de chaque symbole est définie comme suit :

|                                                                                     |                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | Carte de chiffrement dans un ensemble de cartes de chiffrement.                                                                                                                                                                                                                         |
|    | (Espace sur une ligne droite) Quitter une carte de chiffrement lorsqu'un paquet correspond à une entrée ACE.                                                                                                                                                                            |
|    | Paquet qui correspond à la description d'une ACE. Chaque cercle de taille différente représente un paquet distinct correspondant à l'ACE concernée dans la figure. Les différences de taille représentent simplement les différences dans la source et la destination de chaque paquet. |
|   | Redirection vers la carte de chiffrement suivante dans l'ensemble de cartes de chiffrement.                                                                                                                                                                                             |
|  | Réponse lorsqu'un paquet correspond à une ACE ou ne parvient pas à correspondre à toutes les ACE autorisées dans un ensemble de cartes de chiffrement.                                                                                                                                  |

**Illustration 2 : ACL en cascade dans un ensemble de cartes de chiffrement**

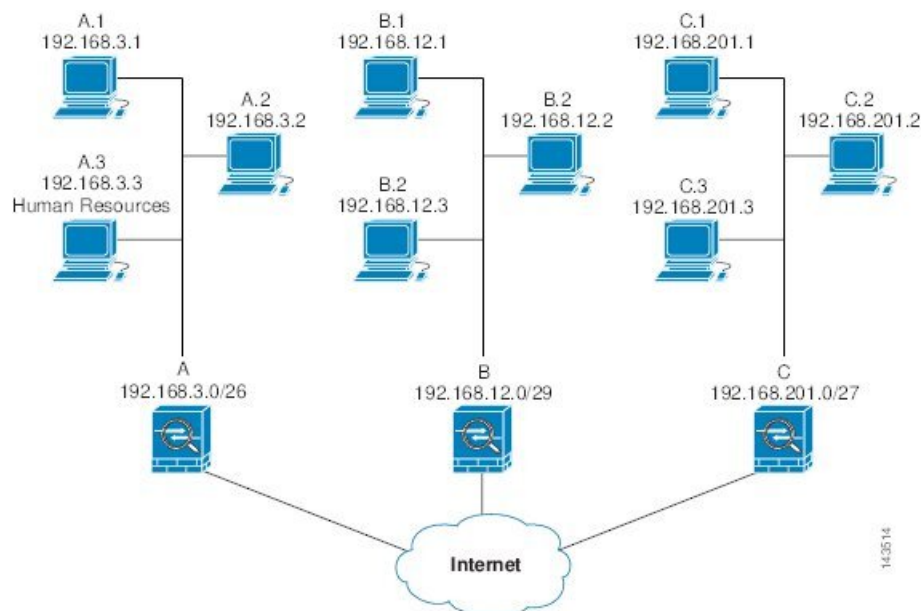
L'appareil de sécurité A évalue un paquet provenant de l'hôte A.3 jusqu'à ce qu'il corresponde à une ACE permit, puis tente d'appliquer la sécurité IPsec associée à la carte de chiffrement. Chaque fois que le paquet correspond à une ACE deny, l'ASA ignore les ACE restantes dans la carte de chiffrement et reprend l'évaluation avec la carte de chiffrement suivante, selon le numéro de séquence qui lui est attribué. Ainsi, dans l'exemple, si l'appareil de sécurité A reçoit un paquet provenant de l'hôte A.3, il le fait correspondre à une ACE deny dans la première carte de chiffrement, puis reprend l'évaluation de ce paquet avec la carte de chiffrement suivante. Lorsqu'il fait correspondre le paquet à l'ACE permit de cette carte de chiffrement, il applique la sécurité IPsec associée (chiffrement renforcé et renouvellement fréquent).

Pour terminer la configuration ASA dans le réseau d'exemple, nous attribuons des cartes de chiffrement miroir aux ASA B et C. Toutefois, comme les ASA ignorent les ACE deny lors de l'évaluation du trafic entrant chiffré, nous pouvons omettre les équivalents miroir des ACE deny A.3 B et deny A.3 C, et donc aussi les équivalents miroir de la Crypto Map 2. La configuration des ACL en cascade dans les ASA B et C est donc inutile.

Le tableau suivant présente les listes de contrôle d'accès attribuées aux cartes de chiffrement configurées pour les trois ASA, A, B et C :

| appareil de sécurité A |              | appareil de sécurité B |            | appareil de sécurité C |            |
|------------------------|--------------|------------------------|------------|------------------------|------------|
| Carte de chiffrement   | Modèle ACE   | Carte de chiffrement   | Modèle ACE | Carte de chiffrement   | Modèle ACE |
| Séquence               |              | Séquence               |            | Séquence               |            |
| Non.                   |              | Non.                   |            | Non.                   |            |
| 1                      | deny A.3 B   | 1                      | permit B A | 1                      | permit C A |
|                        | deny A.3 C   |                        |            |                        |            |
|                        | permit A B   |                        |            |                        |            |
|                        | permit A C   |                        | permit B C |                        | permit C B |
| 2                      | permit A.3 B |                        |            |                        |            |
|                        | permit A.3 C |                        |            |                        |            |

L'illustration suivante fait correspondre les adresses conceptuelles présentées précédemment aux adresses IP réelles.



Les ACE réelles affichées dans le tableau suivant garantissent que tous les paquets IPsec soumis à l'évaluation dans ce réseau reçoivent les paramètres IPsec appropriés.

| Appareil de sécurité | Crypto-carte<br>Séquence<br>Non. | Modèle ACE   | ACE réelles                                                       |
|----------------------|----------------------------------|--------------|-------------------------------------------------------------------|
| A                    | 1                                | deny A.3 B   | deny 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248     |
|                      |                                  | deny A.3 C   | deny 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224    |
|                      |                                  | permit A B   | permit 192.168.3.0 255.255.255.192 192.168.12.0 255.255.255.248   |
|                      |                                  | permit A C   | permit 192.168.3.0 255.255.255.192 192.168.201.0 255.255.255.224  |
|                      | 2                                | permit A.3 B | permit 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248   |
|                      |                                  | permit A.3 C | permit 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224  |
| B                    | Non nécessaire                   | permit B A   | permit 192.168.12.0 255.255.255.248 192.168.3.0 255.255.255.192   |
|                      |                                  | permit B C   | permit 192.168.12.0 255.255.255.248 192.168.201.0 255.255.255.224 |
| C                    | Non nécessaire                   | permit C A   | permit 192.168.201.0 255.255.255.224 192.168.3.0 255.255.255.192  |
|                      |                                  | permit C B   | permit 192.168.201.0 255.255.255.224 192.168.12.0 255.255.255.248 |

Vous pouvez appliquer le même raisonnement affiché dans l'exemple de réseau pour utiliser les ACL en cascade afin d'affecter différents paramètres de sécurité à différents hôtes ou sous-réseaux protégés par un ASA.



#### Remarque

Par défaut, l'ASA ne prend pas en charge le trafic IPsec destiné à la même interface que celle par laquelle il entre. Les appellations de ce type de trafic incluent « demi-tour », « hub-and-spoke » et « hairpinning ». Cependant, vous pouvez configurer IPsec pour prendre en charge le trafic en demi-tour en ajoutant une entrée ACE qui autorise le trafic vers et depuis le réseau. Par exemple, pour prendre en charge le trafic en demi-tour sur l'appareil de sécurité B, ajoutez une entrée ACE conceptuelle « permit B B » à ACL1. L'ACE réelle serait la suivante : **permit 192.168.12.0 255.255.255.248 192.168.12.0 255.255.255.248**

## Définir les clés de l'infrastructure à clé publique (PKI)

Vous devez définir l'infrastructure à clé publique (PKI) pour qu'un administrateur puisse choisir les algorithmes ECDSA de la suite B lors de la génération ou de la mise à zéro d'une paire de clés :

### Avant de commencer

Si vous configurez une carte de chiffrement pour utiliser un point de confiance RSA ou ECDSA pour l'authentification, vous devez d'abord générer l'ensemble de clés. Vous pouvez ensuite créer le point de confiance et le référencer dans la configuration du groupe de tunnels.

## Procédure

- 
- Étape 1** Choisissez l'algorithme ECDSA Suite B lors de la génération d'une paire de clés :
- ```
crypto key generate [rsa [general-keys | label <name> | modules [512 | 768 | 1024 | 2048 | 4096] | noconfirm  
| usage-keys] | ecdsa [label <name> | elliptic-curve [256 | 384 | 521] | noconfirm]]
```
- Étape 2** Choisissez l'algorithme ECDSA Suite B lors de la réinitialisation d'une paire de clés :
- ```
crypto key zeroize [rsa | ecdsa] [default | label <name> | noconfirm]
```
- 

## Appliquer les cartes de chiffrement aux interfaces

Vous devez attribuer un ensemble de cartes de chiffrement à chaque interface par laquelle le trafic IPsec passe. L'ASA prend en charge IPsec sur toutes les interfaces. L'affectation de l'ensemble de cartes de chiffrement à une interface demande à l'ASA d'évaluer tout le trafic par rapport à l'ensemble de cartes de chiffrement et d'utiliser la politique précisée lors de la connexion ou de la négociation de la SA.

L'affectation d'une carte de chiffrement à une interface initialise également les structures de données d'exécution, telles que la base de données SA et la base de données des politiques de sécurité. La réaffectation d'une carte de chiffrement modifiée à l'interface resynchronise les structures de données d'exécution avec la configuration de la carte de chiffrement. De plus, l'ajout de nouveaux homologues par l'utilisation de nouveaux numéros de séquence et la réaffectation de la carte de chiffrement ne supprime pas les connexions existantes.

## Utiliser les listes de contrôle d'interface

Par défaut, l'ASA permet aux paquets IPsec de contourner les listes de contrôle d'interface. Si vous souhaitez appliquer les listes de contrôle d'interface au trafic IPsec, utilisez la forme **no** de la commande **sysopt connection permit-vpn**.

La liste de contrôle d'accès de carte de chiffrement liée à l'interface sortante autorise ou refuse les paquets IPsec dans le tunnel VPN. IPsec authentifie et déchiffre les paquets qui arrivent d'un tunnel IPsec et les soumet à une évaluation par rapport à l'ACL associée au tunnel.

Les listes de contrôle d'accès définissent le trafic IP à protéger. Par exemple, vous pouvez créer des listes de contrôle d'accès pour protéger tout le trafic IP entre deux sous-réseaux ou deux hôtes. (Ces listes de contrôle d'accès sont similaires aux listes de contrôle d'accès utilisées avec la commande **access-group**. Cependant, avec la commande **access-group**, l'ACL détermine le trafic à transférer ou à bloquer au niveau d'une interface.)

Avant l'affectation aux cartes de chiffrement, les listes de contrôle d'accès ne sont pas spécifiques à IPsec. Chaque carte de chiffrement fait référence aux listes de contrôle d'accès et détermine les propriétés IPsec à appliquer à un paquet s'il correspond à une autorisation dans l'une des listes de contrôle d'accès.

Les ACL attribuées aux cartes de chiffrement IPsec ont quatre fonctions principales :

- Sélectionner le trafic sortant à protéger par IPsec (autoriser = protéger).
- Déclencher une négociation ISAKMP pour les données circulant sans SA établie.
- Traiter le trafic entrant pour filtrer et ignorer le trafic qui aurait dû être protégé par IPsec.

- Déterminer s'il faut accepter les demandes de SA IPsec lors du traitement de la négociation IKE de l'homologue. (La négociation s'applique uniquement aux entrées **ipsec-isakmp crypto map**.) L'homologue doit permettre un flux de données associé à une entrée de commande **ipsec-isakmp crypto map** afin d'assurer l'acceptation pendant la négociation.



**Remarque** Si vous supprimez le seul élément d'une ACL, l'ASA supprime également la carte de chiffrement associée.

Si vous modifiez une ACL actuellement référencée par une ou plusieurs cartes de chiffrement, utilisez la commande **crypto map interface** pour réinitialiser la base de données SA d'exécution. Consultez la commande **crypto map** pour obtenir plus d'informations.

Nous vous recommandons que, pour chaque ACL de chiffrement spécifiée pour une carte de chiffrement statique que vous définissez sur l'homologue local, vous définissiez une ACL de chiffrement « image miroir » sur l'homologue distant. Les cartes de chiffrement doivent également prendre en charge des transformations communes et faire référence à l'autre système en tant qu'homologue. Cela garantit un traitement correct d'IPsec par les deux homologues.



**Remarque** Chaque carte de chiffrement statique doit définir une ACL et un homologue IPsec. Si l'un des deux éléments manque, la carte de chiffrement est incomplète et l'ASA abandonne tout trafic qu'il n'a pas déjà mis en correspondance avec une carte de chiffrement antérieure complète. Utilisez la commande **show conf** pour vous assurer que chaque carte de chiffrement est complète. Pour corriger une carte de chiffrement incomplète, supprimez-la, ajoutez les entrées manquantes, puis réappliquez-la.

L'ACL de chiffrement ne prend pas en charge les entrées en double ou qui se chevauchent.

Nous déconseillons l'utilisation du mot-clé **any** pour spécifier les adresses de source ou de destination dans les ACL cryptographiques, car elles causent des problèmes. Nous vous déconseillons fortement l'instruction de commande **permit any any**, car elle fait ce qui suit :

- Protège tout le trafic sortant, y compris tout le trafic protégé envoyé à l'homologue spécifié dans le crypto map correspondant.
- Nécessite une protection pour tout le trafic entrant.

Dans ce scénario, l'ASA abandonne secrètement tous les paquets entrants qui ne disposent pas de protection IPsec.

Assurez-vous de définir les paquets à protéger. Si vous utilisez le mot-clé **any** dans une instruction **permit**, préfacez-le d'une série d'instructions **deny** pour filtrer le trafic qui, autrement, correspondrait à cette instruction **permit** que vous ne souhaitez pas protéger.

**Remarque**

Le trafic traversant déchiffré est autorisé à partir du client malgré la présence d'un groupe d'accès sur l'interface externe, qui appelle une liste de contrôle d'accès deny ip any any, alors que **no sysopt connection permit-vpn** est configuré.

Les utilisateurs qui souhaitent contrôler l'accès au réseau protégé via un VPN de site à site ou d'accès à distance en utilisant la commande **no sysopt permit** en conjonction avec une liste de contrôle d'accès (ACL) sur l'interface externe ne réussissent pas.

Dans cette situation, lorsque l'accès de gestion interne est activé, l'ACL n'est pas appliquée et les utilisateurs peuvent toujours se connecter à l'appareil de sécurité à l'aide de SSH. Le trafic vers les hôtes sur le réseau interne est bloqué correctement par la liste de contrôle d'accès, mais le trafic traversant déchiffré vers l'interface interne n'est pas bloqué.

Les commandes **ssh** et **http** ont une priorité plus élevée que les ACL. En d'autres termes, pour refuser le trafic SSH, Telnet ou ICMP vers le périphérique à partir de la session VPN, utilisez les commandes **ssh**, **telnet** et **icmp**, auxquelles l'ensemble local d'adresses IP refusé doit être ajouté.

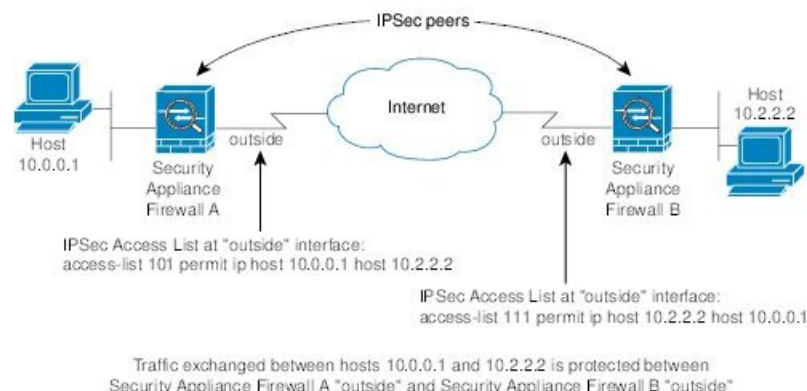
Que le trafic soit entrant ou sortant, l'ASA évalue le trafic en fonction des ACL attribuées à une interface. Suivez ces étapes pour affecter IPsec à une interface :

**Procédure**

- Étape 1** Créez les ACL à utiliser pour IPsec.
- Étape 2** Mappez les listes à une ou plusieurs cartes de chiffrement, en utilisant le même nom de carte de chiffrement.
- Étape 3** Mappez les ensembles de transformation IKEv1 ou les propositions IKEv2 aux cartes de chiffrement pour appliquer IPsec aux flux de données.
- Étape 4** Appliquez les cartes de chiffrement collectivement en tant qu'ensemble de cartes de chiffrement en attribuant le nom de carte de chiffrement qu'elles partagent à l'interface.

**Exemple**

Dans cet exemple, la protection IPsec s'applique au trafic entre l'hôte 10.0.0.1 et l'hôte 10.2.2.2, car les données quittent l'interface externe sur l'ASA A vers l'hôte 10.2.2.2.



L'ASA A évalue le trafic de l'hôte 10.0.0.1 à l'hôte 10.2.2.2, comme suit :

- source = hôte 10.0.0.1
- dest = hôte 10.2.2.2

L'ASA A évalue également le trafic de l'hôte 10.2.2.2 à l'hôte 10.0.0.1, comme suit :

- source = hôte 10.2.2.2
- dest = hôte 10.0.0.1

La première instruction permet qui correspond au paquet évalué détermine la portée de la SA IPsec.

## Modifier la durée de vie des SA IPsec

Vous pouvez modifier les valeurs de durée de vie globale que l'ASA utilise lors de la négociation de nouvelles SA IPsec. Vous pouvez remplacer ces valeurs de durée de vie globale pour une carte de chiffrement particulière.

Les SA IPsec utilisent une clé secrète partagée et dérivée. La clé fait partie intégrale de la SA ; les clés expirent ensemble pour exiger l'actualisation de la clé. Chaque SA a deux durées de vie : temporelle et en fonction du volume du trafic. Une SA expire après la durée de vie respective et les négociations commencent pour une nouvelle. Les durées de vie par défaut sont de 28 800 secondes (8 heures) et de 4 608 000 kilooctets (10 mA par seconde pendant une heure).

Si vous modifiez une durée de vie globale, l'ASA abandonne le tunnel. Il utilise la nouvelle valeur lors de la négociation des SA établies ultérieurement.

Lorsqu'une carte de chiffrement n'a pas de valeurs de durée de vie configurées et que l'ASA demande un nouveau SA, il insère les valeurs de durée de vie globale utilisées dans la SA existante dans la demande envoyée à l'homologue. Lorsqu'un homologue reçoit une demande de négociation, il utilise la plus petite des durées de vie proposées par l'homologue ou configurées localement comme durée de vie des nouvelles SA.

Les homologues négocient un nouveau SA avant de dépasser le seuil de durée de vie de la SA existante pour s'assurer qu'un nouveau SA est prêt à l'expiration de la SA existante. Les homologues négocient une nouvelle SA lorsqu'il reste environ 5 à 15 % de la durée de vie de la SA existante.



### Remarque

Nous vous recommandons de configurer différents temporisateurs d'association de sécurité de chaque côté du tunnel IKEv2 de site à site pour éviter la collision de renouvellement.

## Modifier le routage VPN

Par défaut, des recherches d'adjacence par paquet sont effectuées pour les paquets ESP externes ; aucune recherche n'est effectuée pour les paquets envoyés via le tunnel IPsec.

Dans certaines topologies de réseau, lorsqu'une mise à jour de routage a modifié le chemin du paquet interne, mais que le tunnel IPsec local est toujours actif, les paquets qui passent par le tunnel peuvent ne pas être acheminés correctement et ne pas atteindre leur destination.

Pour éviter cela, activez les recherches de routage par paquet pour les paquets internes IPsec.



**Avant de commencer**

Pour éviter tout impact sur les performances de ces recherches, cette fonctionnalité est désactivée par défaut. Activez-le uniquement lorsque cela est nécessaire.

**Procédure**

Activez les recherches de routage par paquet pour les paquets internes IPsec.

**[no] [crypto] ipsec inner-routing-lookup**

**Remarque**

Une fois configurée, cette commande s'applique uniquement aux tunnels qui ne sont pas fondés sur une VTI.

**Exemple**

```
ciscoasa(config)# crypto ipsec inner-routing-lookup
ciscoasa(config)# show run crypto ipsec
crypto ipsec ikev2 ipsec-proposal GCM
protocol esp encryption aes-gcm
protocol esp integrity null
crypto ipsec inner-routing-lookup
```

## Créer des cartes de chiffrement statiques

Pour créer une configuration IPsec de base à l'aide d'une carte de chiffrement statique, procédez comme suit :

**Procédure****Étape 1**

Pour créer une ACL afin de définir le trafic à protéger, saisissez la commande suivante :

**access-list access-list-name {deny | permit} ip source source-netmask destination destination-netmask**

L'argument *access-list-name* précise l'identifiant de l'ACL, sous la forme d'une chaîne ou d'un entier d'une longueur maximale de 241 caractères. Les *destination-netmask* et *source-netmask* spécifient une adresse réseau IPv4 et un masque de sous-réseau. Dans cet exemple, le mot-clé **permit** fait en sorte que tout trafic correspondant aux conditions spécifiées soit protégé par chiffrement.

**Exemple :**

```
hostname(config)# access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

**Étape 2**

Pour configurer un ensemble de transformation IKEv1 qui définit la protection du trafic, saisissez la commande suivante :

**crypto ipsec ikev1 transform-set transform-set-name encryption [authentication]**

Le *chiffrement* spécifie quelle méthode de chiffrement protège les flux de données IPsec :

- esp-aes : utilise AES avec une clé de 128 bits.
- esp-aes-192 : utilise AES avec une clé de 192 bits.
- esp-aes-256 : utilise AES avec une clé de 256 bits.
- esp-null : pas de chiffrement.

*L'authentification* spécifie la méthode d'authentification pour protéger les flux de données IPsec :

- esp-sha-hmac : utilise SHA/HMAC-160 comme algorithme de hachage.
- esp-none : aucune authentification HMAC.

#### Exemple :

Dans cet exemple, myset1, myset2 et aes\_set sont les noms des ensembles de transformation.

```
hostname(config)# crypto ipsec ikev1 transform-set myset1 esp-aes esp-sha-hmac
hostname(config)#
hostname(config)# crypto ipsec ikev1 transform-set aes_set esp-md5-hmac esp-aes-256
```

### Étape 3

Pour configurer une proposition IKEv2 qui définit également la protection du trafic, saisissez la commande suivante :

**crypto ipsec ikev2 ipsec-proposal** [*proposal tag*]

*La balise de proposition* est le nom de la proposition IKEv2 IPsec, une chaîne de 1 à 64 caractères.

Créez la proposition et passez en mode de configuration ipsec proposal, où vous pouvez spécifier plusieurs types de chiffrement et d'intégrité pour la proposition.

#### Exemple :

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
```

Dans cet exemple, secure est le nom de la proposition. Saisissez un protocole et les types de chiffrement :

```
hostname(config-ipsec-proposal)# protocol esp encryption aes
```

#### Exemple :

Cette commande choisit l'algorithme AES-GCM ou AES-GMAC à utiliser :

**[no] protocol esp encryption** [ aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | null ]

Si SHA-2 ou null est choisi, vous devez choisir l'algorithme à utiliser comme algorithme d'intégrité IPsec. Vous devez choisir l'algorithme d'intégrité null si AES-GCM/GMAC est configuré comme algorithme de chiffrement :

**[no] protocol esp integrity** [ sha-1 | sha-256 | sha-384 | sha-512 | null ]

#### Remarque

Vous devez choisir l'algorithme d'intégrité nulle si AES-GCM/GMAC a été configuré comme algorithme de chiffrement. SHA-256 peut être utilisé pour l'intégrité et PRF pour établir des tunnels IKEv2, mais il peut également être utilisé pour la protection de l'intégrité ESP.

### Étape 4

(Facultatif) Un administrateur peut activer le vieillissement de la PMTU du chemin et définir l'intervalle auquel la valeur PMTU est réinitialisée à sa valeur d'origine.

[no] **crypto ipsec security-association pmtu-aging reset-interval**

## Étape 5

Pour créer une carte cryptographique, effectuez les étapes site à site suivantes en mode monocontexte ou multicontexte :

- a) Attribuez une ACL à une carte de chiffrement :

**crypto map** *map-name seq-num match address access-list-name*

Un ensemble de cartes de chiffrement est un ensemble d'entrées de cartes de chiffrement, chacune avec un numéro de séquence différent (*seq-num*), mais le même *nom de carte*. Utilisez l'argument *access-list-name* pour préciser l'identifiant de l'ACL, sous la forme d'une chaîne ou d'un entier d'une longueur maximale de 241 caractères. Dans l'exemple suivant, mymap est le nom de l'ensemble de cartes de chiffrement. Le numéro de séquence 10 de l'ensemble de cartes de chiffrement est utilisé pour classer plusieurs entrées au sein d'un même ensemble. Plus le numéro de séquence est bas, plus la priorité est élevée.

### Exemple :

Dans cet exemple, l'ACL nommée 101 est affectée à la carte de chiffrement mymap.

```
crypto map mymap 10 match address 101
```

- b) Précisez l'homologue vers lequel le trafic protégé par IPsec peut être acheminé :

**crypto map** *map\_name sequence numberset peer ip\_address1 [ip\_address2] [...]*

### Exemple :

```
crypto map mymap 10 set peer 192.168.1.100
```

L'ASA configure une SA avec l'homologue auquel est attribuée l'adresse IP 192.168.1.100.

### Remarque

À partir de la version 9.14(1), l'ASA prend en charge plusieurs homologues dans la carte de chiffrement IKEv2. Vous pouvez ajouter un maximum de 10 homologues à la liste.

- c) Précisez quels ensembles de transformation IKEv1 ou propositions IKEv2 sont autorisés pour cette carte de chiffrement. Répertoirez plusieurs ensembles de transformation ou propositions par ordre de priorité (priorité la plus élevée en premier). Vous pouvez spécifier jusqu'à 11 ensembles de transformation ou propositions dans une carte de chiffrement à l'aide de l'une ou l'autre de ces deux commandes :

**crypto map** *map-name seq-num set ikev1 transform-set transform-set-name1 [transform-set-name2, ...transform-set-name11]*

OU

**crypto map** *map-name seq-num set ikev2 ipsec-proposal proposal-name1 [proposal-name2, ...proposal-name11]*

*Proposal-name1* et *proposal-name11* spécifient un ou plusieurs noms des propositions IPsec pour IKEv2. Chaque entrée de carte de chiffrement prend en charge jusqu'à 11 propositions.

### Exemple :

Dans cet exemple pour IKEv1, lorsque le trafic correspond à l'ACL 101, la SA peut utiliser myset1 (première priorité) ou myset2 (seconde priorité), selon l'ensemble de transformation qui correspond aux ensembles de transformation de l'homologue.

```
crypto map mymap 10 set ikev1 transform-set myset1 myset2
```

- d) (Optionnel) Pour IKEv2, spécifiez le **mode** pour appliquer le chiffrement et l'authentification ESP au tunnel. Cela permet de déterminer quelle partie du paquet IP d'origine a été appliquée à l'ESP.

```
crypto map map-name seq-num set ikev2 mode [transport | tunnel | transport-require]
```

- **Mode tunnel** : (par défaut) le mode d'encapsulation est réglé sur Mode tunnel. Le mode tunnel applique le chiffrement et l'authentification ESP à l'ensemble du paquet IP d'origine (en-tête IP et données), masquant ainsi les adresses source et destination finales. Le datagramme IP d'origine entier est chiffré et devient la charge utile d'un nouveau paquet IP.

Ce mode permet à un périphérique réseau, comme un routeur, de servir de serveur mandataire IPsec. C'est-à-dire que le routeur effectue le chiffrement au nom des hôtes. Le routeur source chiffre les paquets et les transfère dans le tunnel IPsec. Le routeur de destination déchiffre le datagramme IP d'origine et le transmet au système de destination.

Le principal avantage du mode de tunnel est qu'il n'est pas nécessaire de modifier les systèmes d'extrémité pour profiter des avantages d'IPsec. Le mode tunnel offre également une protection contre l'analyse du trafic; Avec le mode tunnel, un attaquant ne peut déterminer que les points terminaux du tunnel, et non la source et la destination réelles des paquets acheminés dans le tunnel, même s'ils sont identiques aux points terminaux du tunnel.

- **Mode transport** : le mode d'encapsulation est le mode transport avec option de repli en mode tunnel, si l'homologue ne le prend pas en charge. En mode transport, seules les données utiles IP sont chiffrées, et les en-têtes IP d'origine demeurent inchangés.

Ce mode présente l'avantage d'ajouter seulement quelques octets à chaque paquet et de permettre aux périphériques du réseau public de voir la source et la destination finales du paquet. Le mode de transport vous permet d'activer le traitement spécial (par exemple, QoS) sur le réseau intermédiaire en fonction des informations contenues dans l'en-tête IP. Cependant, l'en-tête de couche 4 est chiffré, ce qui limite l'examen du paquet.

- **Transport requis** : le mode d'encapsulation est réglé au mode transport uniquement, le retour au mode tunnel n'est pas autorisé.

Où le mode d'encapsulation **tunnel** est le mode par défaut. Le mode d'encapsulation **transport** est le mode transport avec option de repli en mode tunnel si l'homologue ne le prend pas en charge, et le mode d'encapsulation **transport-require** impose uniquement le mode transport.

#### Remarque

Le mode transport n'est pas recommandé pour les VPN d'accès à distance.

Des exemples de négociation du mode d'encapsulation sont les suivants :

- Si l'initiateur propose le mode transport et que le répondeur répond en mode tunnel, l'initiateur passera en mode tunnel.
- Si l'initiateur propose le mode tunnel et que le répondeur répond en mode transport, le répondeur passera en mode tunnel.
- Si l'initiateur propose le mode tunnel et que le répondeur est en mode transport-require, le message NO PROPOSAL CHOSEN sera envoyé par le répondeur.
- De même, si l'initiateur est en mode transport-require et que le répondeur est en mode tunnel, le message NO PROPOSAL CHOSEN sera envoyé par le répondeur.

- e) (Facultatif) Précisez une durée de vie de SA pour la carte de chiffrement si vous souhaitez remplacer la durée de vie globale.

**crypto map** *map-name seq-num set security-association lifetime* {seconds *number* | kilobytes {*number* | unlimited}}

*Map-name* spécifie le nom de l'ensemble de cartes de chiffrement. *Seq-num* spécifie le numéro que vous attribuez à l'entrée de carte de chiffrement. Vous pouvez définir les deux durées de vie en fonction du temps ou des données transmises. Cependant, la durée de vie des données transmises s'applique uniquement au VPN de site à site et ne s'applique pas au VPN d'accès à distance.

**Exemple :**

Cet exemple raccourcit la durée de vie de la carte de chiffrement mymap 10 à 2 700 secondes (45 minutes). La durée de vie du volume du trafic n'est pas modifiée.

```
crypto map mymap 10 set security-association lifetime seconds 2700
```

- f) (Facultatif) Précisez qu'IPsec exige la Perfect Forward Secrecy (PFS) lors de la demande d'une nouvelle SA pour cette carte de chiffrement, ou qu'il exige la PFS dans les demandes reçues de l'homologue :

**crypto map** *map\_name seq-num set pfs* [group14 | group15 | group16 | group19 | group20 | group21]

**Exemple :**

Cet exemple exige la PFS lors de la négociation d'une nouvelle SA pour la carte de chiffrement mymap 10. L'ASA utilise le groupe de module premier Diffie-Hellman de 2 048 bits dans la nouvelle SA.

```
crypto map mymap 10 set pfs group14
```

- g) (Facultatif) Activez l'injection de route inverse (RRI) pour toute connexion basée sur cette entrée de carte de chiffrement.

**crypto map** *map\_name seq-num set reverse-route* [dynamic]

Si *dynamic* n'est pas spécifié, la RRI est effectuée lors de la configuration et est considérée comme statique, restant en place jusqu'à ce que la configuration soit modifiée ou supprimée. L'ASA ajoute automatiquement des routes statiques à la table de routage et communique ces routes à son réseau privé ou aux routeurs de frontière à l'aide d'OSPF. N'activez pas RRI si vous spécifiez une source/destination (0.0.0.0/0.0.0.0) comme réseau protégé, car cela aura une incidence sur le trafic qui utilise votre route par défaut.

Si *dynamic* est spécifié, les routes sont créées lors de l'établissement réussi des associations de sécurité (SA) IPsec et supprimées après la suppression des SA IPsec.

**Remarque**

La RRI dynamique est prise en charge sur les cartes de chiffrement statiques basées sur IKEv2 uniquement.

**Exemple :**

```
crypto map mymap 10 set reverse-route dynamic
```

## Étape 6

Appliquez un ensemble de cartes de chiffrement à une interface pour évaluer le trafic IPsec :

**crypto map** *map-name interface interface-name*

*Map-name* spécifie le nom de l'ensemble de cartes de chiffrement. *Interface-name* spécifie le nom de l'interface sur laquelle activer ou désactiver la négociation ISAKMP IKEv1.

#### Exemple :

Dans cet exemple, l'ASA évalue le trafic passant par l'interface externe en fonction de la carte de chiffrement `mymap` afin de déterminer s'il doit être protégé.

```
crypto map mymap interface outside
```

## Créer des cartes de chiffrement dynamiques

Une carte de chiffrement dynamique est une carte de chiffrement sans que tous les paramètres soient configurés. Elle agit comme un modèle de politique où les paramètres manquants sont ensuite appris dynamiquement, à la suite d'une négociation IPsec, pour correspondre aux exigences de l'homologue. L'ASA applique une carte de chiffrement dynamique pour permettre à un homologue de négocier un tunnel si son adresse IP n'est pas déjà identifiée dans une carte de chiffrement statique. Cela se produit avec les types d'homologues suivants :

- Homologues avec des adresses IP publiques attribuées dynamiquement.

Les homologues de site à site et d'accès à distance peuvent utiliser DHCP pour obtenir une adresse IP publique. L'ASA utilise cette adresse uniquement pour amorcer le tunnel.

- Homologues avec des adresses IP privées attribuées dynamiquement.

Les homologues demandant des tunnels d'accès à distance ont généralement des adresses IP privées attribuées par la tête de réseau. En général, les tunnels de site à site ont un ensemble prédéfini de réseaux privés utilisés pour configurer des cartes statiques et, par conséquent, pour établir des SA IPsec.

En tant qu'administrateur configurant des cartes de chiffrement statiques, vous ne connaissez peut-être pas les adresses IP attribuées dynamiquement (par DHCP ou toute autre méthode), et vous pourriez ne pas connaître les adresses IP privées d'autres clients, quelle que soit la façon dont elles ont été attribuées. Les clients VPN n'ont généralement pas d'adresses IP statiques ; ils nécessitent une carte de chiffrement dynamique pour permettre la négociation IPsec. Par exemple, la tête de réseau attribue l'adresse IP à un client VPN Cisco lors de la négociation IKE, que le client utilise ensuite pour négocier les SA IPsec.



#### Remarque

Une carte de chiffrement dynamique ne nécessite que le paramètre **transform-set**.

Les cartes de chiffrement dynamiques peuvent faciliter la configuration IPsec, et nous les recommandons pour une utilisation dans les réseaux où les homologues ne sont pas toujours prédéfinis. Utilisez des cartes de chiffrement dynamiques pour les clients VPN Cisco (comme les utilisateurs mobiles) et les routeurs qui obtiennent des adresses IP attribuées dynamiquement.



#### Astuces

Faites preuve de prudence lorsque vous utilisez le mot-clé **any** dans les entrées **permit** des cartes de chiffrement dynamiques. Si le trafic couvert par une telle entrée **permit** (d'autorisation) peut inclure du trafic de multidiffusion ou de diffusion, insérez des entrées **deny** (de refus) pour la plage d'adresses appropriée dans la liste de contrôle d'accès. N'oubliez pas d'insérer des entrées **deny** (de refus) pour le trafic de diffusion en réseau et en sous-réseau, et pour tout autre trafic qu'IPsec ne doit pas protéger.

Les cartes de chiffrement dynamiques fonctionnent uniquement pour négocier les SA avec les homologues distants qui amorcent la connexion. L'ASA ne peut pas utiliser de cartes de chiffrement dynamiques pour établir des connexions à un homologue distant. Avec une carte de chiffrement dynamique, si le trafic sortant correspond à une entrée d'autorisation dans une liste de contrôle d'accès et que la SA correspondante n'existe pas encore, l'ASA abandonne le trafic.

Un ensemble de cartes de chiffrement peut inclure une carte de chiffrement dynamique. Les ensembles de cartes de chiffrement dynamiques doivent être les cartes de chiffrement de priorité la plus basse dans l'ensemble de cartes de chiffrement (c'est-à-dire qu'ils doivent avoir les numéros de séquence les plus élevés) pour que l'ASA évalue les autres cartes de chiffrement en premier. Il examine l'ensemble de cartes de chiffrement dynamiques uniquement lorsque les autres entrées de carte (statiques) ne correspondent pas.

Comme pour les ensembles de cartes de chiffrement statiques, un ensemble de cartes de chiffrement dynamiques se compose de toutes les cartes de chiffrement dynamiques ayant le même nom de carte dynamique. Le `dynamic-seq-num` différencie les cartes de chiffrement dynamiques dans un ensemble. Si vous configurez une carte de chiffrement dynamique, insérez une ACL permit pour identifier le flux de données de l'homologue IPsec pour l'ACL de chiffrement. Sinon, l'ASA accepte toute identité de flux de données proposée par l'homologue.



#### Mise en garde

N'affectez pas de routes par défaut au module pour le trafic à tunneliser vers une interface ASA configurée avec un ensemble de cartes de chiffrement dynamiques. Pour identifier le trafic qui doit être tunnelisé, ajoutez les listes de contrôle d'accès à la carte de chiffrement dynamique. Faites attention à identifier les ensembles d'adresses appropriés lors de la configuration des listes de contrôle d'accès associées aux tunnels d'accès à distance. Utilisez l'injection de route inverse pour installer les routes uniquement une fois que le tunnel est opérationnel.

Créez une entrée de carte de chiffrement dynamique en mode contexte unique ou multiple. Vous pouvez combiner des entrées de carte statiques et dynamiques dans un seul ensemble de cartes de chiffrement.

### Procédure

#### Étape 1

(Facultatif) Attribuez une liste de contrôle d'accès à une carte de chiffrement dynamique :

**crypto dynamic-map** *dynamic-map-name* *dynamic-seq-num* **match address** *access-list-name*

Cela détermine quel trafic doit être protégé et non protégé. *Dynamic-map-name* spécifie le nom de l'entrée de carte de chiffrement qui fait référence à une carte de chiffrement dynamique préexistante. *Dynamic-seq-num* spécifie le numéro de séquence qui correspond à l'entrée de carte de chiffrement dynamique.

#### Exemple :

Dans cet exemple, l'ACL 101 est affecté à la carte de chiffrement dynamique dyn1. Le numéro de séquence de carte est 10.

```
crypto dynamic-map dyn1 10 match address 101
```

#### Étape 2

Précisez quels ensembles de transformation IKEv1 ou propositions IKEv2 sont autorisés pour cette carte de chiffrement dynamique. Énumérez plusieurs ensembles de transformations ou propositions en ordre de priorité (la priorité la plus élevée en premier) en utilisant la commande pour les ensembles de transformation IKEv1 ou les propositions IKEv2 :

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set ikev1 transform-set transform-set-name1,
[transform-set-name2, ...transform-set-name9]
```

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set ikev2 ipsec-proposal proposal-name1
[proposal-name2, ... proposal-name11]
```

*Dynamic-map-name* spécifie le nom de l'entrée de carte de chiffrement qui fait référence à une carte de chiffrement dynamique préexistante. *Dynamic-seq-num* spécifie le numéro de séquence qui correspond à l'entrée de carte de chiffrement dynamique. Le *transform-set-name* est le nom de l'ensemble de transformation en cours de création ou de modification. Le *nom de la proposition* spécifie un ou plusieurs noms des propositions IPsec pour IKEv2.

#### Exemple :

Dans cet exemple pour IKEv1, lorsque le trafic correspond à l'ACL 101, la SA peut utiliser myset1 (première priorité) ou myset2 (seconde priorité), selon l'ensemble de transformation qui correspond aux ensembles de transformation de l'homologue.

```
crypto dynamic-map dyn 10 set ikev1 transform-set myset1 myset2
```

### Étape 3

(Facultatif) Précisez la durée de vie de la SA pour l'entrée de carte de chiffrement dynamique si vous souhaitez remplacer la valeur de durée de vie globale :

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set security-association lifetime {seconds
number | kilobytes {number | unlimited}}
```

*Dynamic-map-name* spécifie le nom de l'entrée de carte de chiffrement qui fait référence à une carte de chiffrement dynamique préexistante. *Dynamic-seq-num* spécifie le numéro de séquence qui correspond à l'entrée de carte de chiffrement dynamique. Vous pouvez définir les deux durées de vie en fonction du temps ou des données transmises. Cependant, la durée de vie des données transmises s'applique uniquement au VPN de site à site et ne s'applique pas au VPN d'accès à distance.

#### Exemple :

Cet exemple raccourcit la durée de vie de la carte de chiffrement dynamique dyn1 10 à 2 700 secondes (45 minutes). La durée de vie en volume de trafic n'est pas modifiée.

```
crypto dynamic-map dyn1 10 set security-association lifetime seconds 2700
```

### Étape 4

(Facultatif) Précisez qu'IPsec demande PFS lors de la demande de nouveaux SA pour cette carte de chiffrement dynamique, ou devrait exiger PFS dans les demandes reçues de l'homologue :

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set
pfs [group14 | group15 | group16 | group19 | group20 | group21]
```

*Dynamic-map-name* spécifie le nom de l'entrée de carte de chiffrement qui fait référence à une carte de chiffrement dynamique préexistante. *Dynamic-seq-num* spécifie le numéro de séquence qui correspond à l'entrée de carte de chiffrement dynamique.

#### Exemple :

```
crypto dynamic-map dyn1 10 set pfs group14
```

### Étape 5

Ajoutez l'ensemble de cartes de chiffrement dynamique dans un ensemble de cartes de chiffrement statiques.



Veillez à définir les cartes de chiffrement qui référencent des cartes dynamiques comme entrées de priorité la plus basse (numéros de séquence les plus élevés) dans un ensemble de cartes de chiffrement.

**crypto map** *map-name* *seq-num* **ipsec-isakmp** **dynamic** *dynamic-map-name*

*Map-name* spécifie le nom de l'ensemble de cartes de chiffrement. *Dynamic-map-name* spécifie le nom de l'entrée de carte de chiffrement qui fait référence à une carte de chiffrement dynamique préexistante.

**Exemple :**

```
crypto map mymap 200 ipsec-isakmp dynamic dyn1
```

## Configurer la redondance de site à site

Vous pouvez définir plusieurs homologues IKEv1 en utilisant des cartes de chiffrement pour assurer la redondance. Cette configuration est utile pour les VPN de site à site. Cette fonctionnalité n'est pas prise en charge avec IKEv2.

Si un homologue échoue, l'ASA établit un tunnel vers l'homologue suivant associé à la carte de chiffrement. Il envoie des données à l'homologue avec lequel il a négocié avec succès, et cet homologue devient l'homologue actif. L'homologue actif est l'homologue que l'ASA continue d'essayer en premier pour les négociations de suivi jusqu'à ce qu'une négociation échoue. À ce stade, l'ASA passe à l'homologue suivant. L'ASA revient au premier homologue lorsque tous les homologues associés à la carte de chiffrement ont échoué.

## Gestion des VPN IPsec

### Affichage d'une configuration IPsec

Il s'agit des commandes que vous pouvez saisir en mode contexte unique ou multiple pour afficher les informations sur votre configuration IPsec.

**Tableau 3 : Commandes pour afficher les informations de configuration IPsec**

|                                               |                                                                                                                                                    |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show running-configuration crypto</b>      | Affiche l'ensemble de la configuration du chiffrement, y compris IPsec, les cartes de chiffrement, les cartes de chiffrement dynamiques et ISAKMP. |
| <b>show running-config crypto ipsec</b>       | Affiche la configuration IPsec complète.                                                                                                           |
| <b>show running-config crypto isakmp</b>      | Affiche la configuration ISAKMP complète.                                                                                                          |
| <b>show running-config crypto map</b>         | Affiche la configuration complète de la carte de chiffrement.                                                                                      |
| <b>show running-config crypto dynamic-map</b> | Affiche la configuration de la carte de chiffrement dynamique.                                                                                     |

|                                    |                                                                                                                                                                                                       |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show all crypto map</b>         | Affiche tous les paramètres de configuration, y compris ceux avec des valeurs par défaut.                                                                                                             |
| <b>show crypto ikev2 sa detail</b> | Affiche la prise en charge de l'algorithme Suite B dans les statistiques de chiffrement.                                                                                                              |
| <b>show crypto ipsec sa</b>        | Affiche la prise en charge de l'algorithme Suite B et la sortie IPsec ESPv3 en mode contexte unique ou multiple.                                                                                      |
| <b>show ipsec stats</b>            | Affiche les informations sur le sous-système IPsec en mode contexte unique ou multiple. Les statistiques ESPv3 sont affichées dans les paquets TFC et les erreurs ICMP valides et non valides reçues. |

## Attendre la fin des sessions actives avant de redémarrer

Vous pouvez planifier un redémarrage de l'ASA qui ne se produira qu'une fois que toutes les sessions actives auront pris fin volontairement. Par défaut, cette fonction est désactivée.

Utilisez la commande **reload** pour redémarrer l'ASA. Si vous définissez la commande **reload-wait**, vous pouvez utiliser la commande **reload quick** pour outrepasser le paramètre **reload-wait**. Les commandes **reload** et **reload-wait** sont disponibles en mode d'exécution privilégié ; aucune des deux n'inclut le préfixe **isakmp**.

### Procédure

Pour faire en sorte que l'ASA attende la fin volontaire de toutes les sessions actives avant de redémarrer, effectuez la tâche de site à site suivante en mode monocontexte ou multicontexte :

**crypto isakmp reload-wait**

**Exemple :**

```
hostname(config)# crypto isakmp reload-wait
```

## Alerter les homologues avant la déconnexion

Les sessions d'accès à distance ou LAN-à-LAN peuvent être interrompues pour plusieurs raisons, comme l'arrêt ou le redémarrage de l'ASA, le délai d'inactivité de la session, le dépassement de la durée maximale de connexion ou une interruption par l'administrateur.

L'ASA peut avertir les homologues admissibles, dans les configurations LAN-à-LAN ou les clients VPN, des sessions sur le point d'être déconnectées. L'homologue ou le client qui reçoit l'alerte decode la raison et l'affiche dans le journal des événements ou dans une fenêtre contextuelle. Par défaut, cette fonction est désactivée.

Les clients et homologues admissibles sont les suivants :

- périphériques de sécurité avec alertes activées

- Clients VPN Cisco exécutant le logiciel version 4.0 ou ultérieure, sans configuration requise

Pour activer la notification de déconnexion aux homologues IPsec, entrez la commande **crypto isakmp disconnect-notify** en mode contexte unique ou multiple.

## Effacer les associations de sécurité

Certaines modifications de configuration ne prennent effet que pendant la négociation des SA suivantes. Si vous souhaitez que les nouveaux paramètres prennent effet immédiatement, effacez les SA existantes pour les rétablir avec la configuration modifiée. Si l'ASA traite activement le trafic IPsec, effacez uniquement la partie de la base de données SA affectée par les modifications de configuration. Réservez l'effacement de la base de données SA complète pour les modifications à grande échelle ou lorsque l'ASA traite une petite quantité de trafic IPsec.

Le tableau suivant répertorie les commandes que vous pouvez saisir pour effacer et réinitialiser les SA IPsec en mode contexte unique ou multiple.

**Tableau 4 : Commandes pour effacer et réinitialiser les SA IPsec**

|                                             |                                                                                                                                                      |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>clear configure crypto</b>               | Supprime une configuration complète de chiffrement, y compris IPsec, les cartes de chiffrement, les cartes de chiffrement dynamiques et ISAKMP.      |
| <b>clear configure crypto ca trustpoint</b> | Supprime tous les points de confiance.                                                                                                               |
| <b>clear configure crypto dynamic-map</b>   | Supprime toutes les cartes de chiffrement dynamiques. Inclut des mots-clés permettant de supprimer des cartes de chiffrement dynamiques spécifiques. |
| <b>clear configure crypto map</b>           | Supprime toutes les cartes de chiffrement. Inclut des mots-clés permettant de supprimer des cartes de chiffrement spécifiques.                       |
| <b>clear configure crypto isakmp</b>        | Supprime l'ensemble de la configuration ISAKMP.                                                                                                      |
| <b>clear configure crypto isakmp policy</b> | Supprime toutes les politiques ISAKMP ou une politique spécifique.                                                                                   |
| <b>clear crypto isakmp sa</b>               | Supprime l'ensemble de la base de données des SA ISAKMP.                                                                                             |

## Effacer les configurations de cartes de chiffrement

La commande **clear configure crypto** comprend des arguments qui vous permettent de supprimer des éléments de la configuration cryptographique, notamment IPsec, les cartes de chiffrement, les cartes de chiffrement dynamiques, les points de confiance d'autorité de certification, tous les certificats, les configurations de mappage de certificats et ISAKMP.

Sachez que si vous saisissez la commande **clear configure crypto** sans arguments, vous supprimez l'ensemble de la configuration crypto, y compris tous les certificats.

Pour en savoir plus, consultez la commande **clear configure crypto** dans la *Référence des commandes de la série Cisco Secure Firewall ASA*.





## CHAPITRE 2

# L2TP sur IPsec

Ce chapitre décrit comment configurer L2TP sur IPsec/IKEv1 sur l'ASA.

- À propos des VPN L2TP sur IPsec/IKEv1, à la page 45
- Exigences de licence pour L2TP sur IPsec, à la page 47
- Conditions préalables à la configuration de L2TP sur IPsec, à la page 47
- Lignes directrices et limites relatives à la licence, à la page 47
- Configuration de L2TP sur Eclipse avec l'interface de ligne de commande, à la page 49
- Historique des fonctionnalités pour L2TP sur IPsec, à la page 54

## À propos des VPN L2TP sur IPsec/IKEv1

Le protocole de tunnelisation pour la couche 2 (L2TP) est un protocole de tunnelisation VPN qui permet aux clients distants d'utiliser le réseau IP public pour communiquer en toute sécurité avec les serveurs de réseau privés d'entreprise. L2TP utilise PPP sur UDP (port 1701) pour tunneliser les données.

Le protocole L2TP est basé sur le modèle client/serveur. La fonction est répartie entre le serveur de réseau L2TP (LNS) et le concentrateur d'accès L2TP (LAC). Le LNS s'exécute généralement sur une passerelle réseau telle qu'un routeur, tandis que le LAC peut être un serveur d'accès réseau (NAS) commuté ou un périphérique terminal doté d'un client L2TP intégré, comme Microsoft Windows, Apple iPhone ou Android.

Le principal avantage de la configuration de L2TP avec IPsec/IKEv1 dans un scénario d'accès à distance est que les utilisateurs distants peuvent accéder à un VPN sur un réseau IP public sans passerelle ni ligne dédiée, ce qui permet un accès à distance à partir de pratiquement n'importe où avec le service POTS. Un autre avantage est qu'aucun logiciel client supplémentaire, comme le logiciel client VPN Cisco, n'est requis.



---

**Remarque** L2TP sur IPsec ne prend en charge que IKEv1. IKEv2 n'est pas pris en charge.

---

La configuration de L2TP avec IPsec/IKEv1 prend en charge l'authentification par certificats ainsi que les méthodes par clé prépartagée ou signature RSA, ainsi que l'utilisation de cartes de chiffrement dynamiques (par opposition à statiques). Ce résumé des tâches suppose l'achèvement d'IKEv1, ainsi que la configuration des clés prépartagées ou de la signature RSA. Consultez le chapitre 41, « Certificats numériques », dans le guide de configuration des opérations générales pour connaître les étapes à suivre pour configurer les clés prépartagées, le RSA et les cartes de chiffrement dynamiques.

**Remarque**

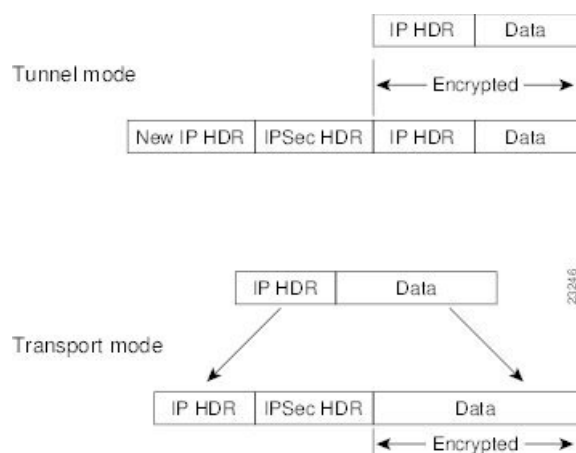
L2TP avec IPsec sur l'ASA permet au LNS d'interopérer avec des clients VPN natifs intégrés à des systèmes d'exploitation tels que Windows, Mac OS X, Android et Cisco IOS. Seul L2TP avec IPsec est pris en charge ; L2TP natif lui-même n'est pas pris en charge sur l'ASA. La durée de vie minimale d'une association de sécurité IPsec prise en charge par le client Windows est de 300 secondes. Si la durée de vie configurée sur l'ASA est inférieure à 300 secondes, le client Windows l'ignore et la remplace par une durée de vie de 300 secondes.

## Modes de transport et de tunnel IPsec

Par défaut, l'ASA utilise le mode tunnel IPsec : l'ensemble du datagramme IP d'origine est chiffré et devient la charge utile d'un nouveau paquet IP. Ce mode permet à un périphérique réseau, comme un routeur, de servir de proxy IPsec. C'est-à-dire que le routeur effectue le chiffrement au nom des hôtes. Le routeur source chiffre les paquets et les transfère dans le tunnel IPsec. Le routeur de destination déchiffre le datagramme IP d'origine et le transmet au système de destination. Le principal avantage du mode de tunnel est qu'il n'est pas nécessaire de modifier les systèmes d'extrémité pour profiter des avantages d'IPsec. Le mode tunnel offre également une protection contre l'analyse du trafic ; Avec le mode tunnel, un attaquant ne peut déterminer que les points terminaux du tunnel, et non la source et la destination réelles des paquets acheminés dans le tunnel, même s'ils sont identiques aux points terminaux du tunnel.

Cependant, le client Windows L2TP/IPsec utilise le mode transport IPsec—seule la charge utile IP est chiffrée, et les en-têtes IP d'origine demeurent inchangés. Ce mode présente l'avantage d'ajouter seulement quelques octets à chaque paquet et de permettre aux périphériques du réseau public de voir la source et la destination finales du paquet. La figure suivante illustre les différences entre les modes de tunnel IPsec et de transport.

**Illustration 3 : IPsec en modes tunnel et transport**



Pour que les clients Windows L2TP et IPsec se connectent à l'ASA, vous devez configurer le mode transport IPsec pour un ensemble de transformation à l'aide de la commande **crypto ipsec transform-set trans\_name mode transport**. Cette commande est utilisée dans la procédure de configuration.

**Remarque**

L'ASA ne peut pas pousser plus de 28 ACE dans la liste d'accès de tunnel fractionné.

Grâce à ce mode transport, vous pouvez activer un traitement spécifique (par exemple, QoS) sur le réseau intermédiaire en fonction des informations contenues dans l'en-tête IP. Cependant, l'en-tête de couche 4 est chiffré, ce qui limite l'examen du paquet. Cependant, si l'en-tête IP est transmis en clair, le mode transport permet à un attaquant d'effectuer une analyse du trafic.

## Exigences de licence pour L2TP sur IPsec



**Remarque** Cette fonctionnalité n'est pas disponible sur les modèles sans chiffrement de charge utile.

Le VPN d'accès à distance IPsec utilisant IKEv2 nécessite une licence AnyConnect Plus ou Apex, disponible séparément. Le VPN d'accès à distance IPsec utilisant IKEv1 et le VPN de site à site IPsec utilisant IKEv1 ou IKEv2 utilise la licence Autre VPN fournie avec la licence Essentials. Consultez [Licences de fonctionnalités de la gamme Cisco ASA](#) pour connaître les valeurs maximales par modèle.

## Conditions préalables à la configuration de L2TP sur IPsec

La configuration de L2TP sur IPsec nécessite les conditions préalables suivantes :

- Stratégie de groupe : vous pouvez configurer la stratégie de groupe par défaut, DfltGrpPolicy, ou une stratégie de groupe définie par l'utilisateur pour les connexions L2TP/IPsec. Dans les deux cas, la stratégie de groupe doit être configurée pour utiliser le protocole de tunnellation L2TP/IPsec. Si le protocole de tunnellation L2TP/IPsec n'est pas configuré pour votre stratégie de groupe définie par l'utilisateur, configurez DfltGrpPolicy pour le protocole de tunnellation L2TP/IPsec et permettez à votre stratégie de groupe définie par l'utilisateur d'hériter de cet attribut.
- Profil de connexion : vous devez configurer le profil de connexion par défaut (groupe de tunnels), DefaultRAGroup, si vous effectuez une authentification par « clé prépartagée ». Si vous effectuez une authentification basée sur des certificats, vous pouvez utiliser un profil de connexion défini par l'utilisateur qui peut être choisi en fonction des identifiants de certificat.
- La connectivité IP doit être établie entre les homologues. Pour tester la connectivité, essayez d'effectuer un ping vers l'adresse IP de l'ASA depuis votre terminal, puis vers l'adresse IP de votre terminal depuis l'ASA.
- Assurez-vous que le port UDP 1701 n'est pas bloqué le long du chemin de la connexion.
- Si un terminal Windows 7 s'authentifie à l'aide d'un certificat qui spécifie un type de signature SHA, le type de signature doit correspondre à celui de l'ASA, soit SHA1 ou SHA2.

## Lignes directrices et limites relatives à la licence

Cette section comprend les lignes directrices et les limites de cette fonctionnalité.

### Directives relatives au mode contextuel

Pris en charge en mode contexte unique

### Directives sur le mode pare-feu

Pris en charge uniquement en mode pare-feu routé. Le mode transparent n'est pas pris en charge.

### Directives en matière de basculement

Les sessions L2TP sur IPsec ne sont pas prises en charge par le basculement avec état.

### Directives IPv6

Il n'y a pas de prise en charge native de la configuration de tunnel IPv6 pour L2TP sur IPsec.

### Limitation logicielle sur toutes les plateformes

Nous prenons actuellement en charge uniquement 4 096 tunnels L2TP sur IPsec.

### Directives d'authentification

L'ASA prend en charge uniquement les authentifications PPP PAP et Microsoft CHAP, versions 1 et 2, sur la base de données locale. EAP et CHAP sont effectuées par des serveurs proxy d'authentification. Par conséquent, si un utilisateur distant appartient à un groupe de tunnels configuré avec les commandes **authentication eap-proxy** ou **authentication chap** et que l'ASA est configuré pour utiliser la base de données locale, cet utilisateur ne pourra pas se connecter.

### Types d'authentification PPP pris en charge

Les connexions L2TP sur IPsec sur l'ASA prennent en charge uniquement les types d'authentification PPP, comme indiqué :

**Tableau 5 : Prise en charge des serveurs AAA et types d'authentification PPP**

| Type de serveur AAA | Types d'authentification PPP pris en charge |
|---------------------|---------------------------------------------|
| LOCAL               | PAP, MSCHAPv1, MSCHAPv2                     |
| RADIUS              | PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-Proxy    |
| TACACS+             | PAP, CHAP, MSCHAPv1                         |
| LDAP                | PAP                                         |
| NT                  | PAP                                         |
| Kerberos            | PAP                                         |
| SDI                 | SDI                                         |

**Tableau 6 : Caractéristiques du type d'authentification PPP**

| Mot-clé     | Type d'authentification | Caractéristiques                                                                                                                                                                                               |
|-------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>chap</b> | CHAP                    | En réponse au défi du serveur, le client renvoie le [challenge plus password] chiffré avec un nom d'utilisateur en texte clair. Ce protocole est plus sécurisé que le PAP, mais il ne chiffre pas les données. |



| Mot-clé                                | Type d'authentification                                | Caractéristiques                                                                                                                                                                                                                                    |
|----------------------------------------|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>eap-proxy</b>                       | EAP                                                    | Active EAP, ce qui permet au périphérique de sécurité de relayer le processus d'authentification PPP vers un serveur d'authentification RADIUS externe.                                                                                             |
| <b>ms-chap-v1</b><br><b>ms-chap-v2</b> | Microsoft CHAP, version 1<br>Microsoft CHAP, version 2 | Similaire à CHAP, mais plus sécurisé, car le serveur stocke et compare uniquement les mots de passe chiffrés plutôt que les mots de passe en clair comme dans CHAP. Ce protocole génère également une clé pour le chiffrement des données par MPPE. |
| <b>pap</b>                             | PAP                                                    | Le PAP transmet un nom d'utilisateur et un mot de passe en clair lors de l'authentification et n'est pas sécurisé.                                                                                                                                  |

## Configuration de L2TP sur Eclipse avec l'interface de ligne de commande

Vous devez configurer les paramètres de politique IKEv1 (ISAKMP) pour permettre aux clients VPN natifs d'établir une connexion VPN avec l'ASA à l'aide du protocole L2TP sur Eclipse.

- IKEv1 phase 1 : chiffrement AES avec méthode de hachage SHA1.
- Eclipse phase 2 : chiffrement AES avec méthode de hachage SHA.
- Authentification PPP : PAP, MS-CHAPv1 ou MSCHAPv2 (préféré).
- Clé partagée (uniquement pour iPhone).

### Procédure

**Étape 1** Créez un ensemble de transformation avec un type de chiffrement ESP et un type d'authentification spécifiques.

**crypto ipsec ike\_version transform-set transform\_name ESP\_Encryption\_Type ESP\_Authentication\_Type**

**Exemple :**

```
crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-aes esp-sha-hmac
```

**Étape 2** Configurez Eclipse pour utiliser le mode transport plutôt que le mode tunnel.

**crypto ipsec ike\_version transform-set trans\_name mode transport**

**Exemple :**

```
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
```

**Étape 3** Précisez L2TP/Eclipse comme protocole de tunnelisation VPN.

**vpn-tunnel-protocol tunneling\_protocol**

**Exemple :**

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# vpn-tunnel-protocol l2tp-ipsec
```

**Étape 4** (Facultatif) Demandez à l'appareil de sécurité adaptatif d'envoyer les adresses IP du serveur DNS au client pour la stratégie de groupe.

**dns value** [none | IP\_Primary | IP\_Secondary]

**Exemple :**

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# dns value 209.165.201.1 209.165.201.2
```

**Étape 5** (Facultatif) Demandez à l'appareil de sécurité adaptatif d'envoyer les adresses IP du serveur WINS au client pour la stratégie de groupe.

**wins-server value** [none | IP\_primary [IP\_secondary]]

**Exemple :**

```
hostname(config)# group-policy DfltGrpPolicy attributes
hostname (config-group-policy)# wins-server value 209.165.201.3 209.165.201.4
```

**Étape 6** (Facultatif) Créer un ensemble d'adresses IP.

**ip local pool** pool\_name starting\_address-ending\_address mask subnet\_mask

**Exemple :**

```
hostname(config)# ip local pool sales_addresses 10.4.5.10-10.4.5.20 mask 255.255.255.0
```

**Étape 7** (Facultatif) Associez l'ensemble d'adresses IP au profil de connexion (groupe de tunnels).

**address-pool** pool\_name

**Exemple :**

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# address-pool sales_addresses
```

**Étape 8** Associez le nom d'une stratégie de groupe au profil de connexion (groupe de tunnels).

**default-group-policy** name

**Exemple :**

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# default-group-policy DfltGrpPolicy
```

**Étape 9** Précisez un serveur d'authentification pour vérifier les utilisateurs tentant L2TP sur les connexions IPsec. Si vous souhaitez que l'authentification revienne à l'authentification locale lorsque le serveur n'est pas disponible, ajoutez LOCAL à la fin de la commande.

**authentication-server-group** server\_group [local]

**Exemple :**

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# authentication-server-group sales_server LOCAL
```

**Étape 10** Précisez une méthode pour authentifier les utilisateurs tentant des connexions L2TP sur les connexions Eclipse, pour le profil de connexion (groupe de tunnels). Si vous n'utilisez pas l'ASA pour effectuer l'authentification locale et que vous souhaitez revenir à l'authentification locale, ajoutez LOCAL à la fin de la commande.

**authentication** auth\_type

**Exemple :**

```
hostname(config)# tunnel-group DefaultRAGroup ppp-attributes
hostname(config-ppp)# authentication ms-chap-v1
```

**Étape 11** Définissez la clé prépartagée pour votre profil de connexion (groupe de tunnels).

**tunnel-group tunnel group name ipsec-attributes**

**Exemple :**

```
hostname(config)# tunnel-group DefaultRAGroup ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key cisco123
```

**Étape 12** (Facultatif) Générez des enregistrements de début et de fin de comptabilité AAA pour une session L2TP pour le profil de connexion (groupe de tunnels).

**accounting-server-group aaa\_server\_group**

**Exemple :**

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# accounting-server-group sales_aaa_server
```

**Étape 13** Configurez l'intervalle (en secondes) entre les messages hello. La plage est de 10 à 300 secondes. L'intervalle par défaut est de 60 secondes.

**l2tp tunnel hello seconds**

**Exemple :**

```
hostname(config)# l2tp tunnel hello 100
```

**Étape 14** (Facultatif) Activez la traversée NAT pour que les paquets ESP puissent passer par un ou plusieurs périphériques NAT.

Si vous vous attendez à ce que plusieurs clients L2TP derrière un périphérique NAT tentent des connexions L2TP sur des connexions Eclipse avec l'appareil de sécurité adaptatif, vous devez activer la traversée NAT.

**crypto isakmp nat-traversal seconds**

Pour activer la traversée NAT globalement, vérifiez qu'ISAKMP est activé (vous pouvez l'activer avec la commande **crypto isakmp enable**) en mode de configuration globale, puis utilisez la commande **crypto isakmp nat-traversal**.

**Exemple :**

```
hostname(config)# crypto isakmp enable
hostname(config)# crypto isakmp nat-traversal 1500
```

**Étape 15** (Facultatif) Configurez la commutation de groupe de tunnels. L'objectif de la commutation de groupe de tunnels est de donner aux utilisateurs davantage de chances d'établir une connexion VPN lorsqu'ils s'authentifient à l'aide d'un proxy d'authentification. Le groupe de tunnels est synonyme de profil de connexion.

**strip-group**

**strip-realm**

**Exemple :**

```
hostname(config)# tunnel-group DefaultRAGroup general-attributes
hostname(config-tunnel-general)# strip-group
hostname(config-tunnel-general)# strip-realm
```

**Étape 16** (Facultatif) Créez un utilisateur avec le nom d'utilisateur **jdoe**, le mot de passe **j!doe1**. L'option **mschap** spécifie que le mot de passe est converti en Unicode et haché à l'aide de MD4 après sa saisie.

Cette étape est nécessaire uniquement si vous utilisez une base de données d'utilisateurs locale.

**username name password password mschap**

**Exemple :**

```
asa2(config)# username jdoe password j!doe1 mschap
```

**Étape 17** Créez la politique IKE pour la phase 1 et attribuez-y un numéro.

**crypto ikev1 policy priority**

**group Diffie-Hellman Group**

Il existe plusieurs paramètres de la politique IKE que vous pouvez configurer. Vous pouvez également spécifier un groupe Diffie-Hellman pour la politique. La politique **isakmp** est utilisée par l'ASA pour terminer la négociation IKE.

**Exemple :**

```
hostname(config)# crypto ikev1 policy 14
hostname(config-ikev1-policy)# group14
```

## Créer des politiques IKE pour répondre aux propositions Windows 7

Les clients Windows 7 L2TP/IPsec envoient plusieurs propositions de politique IKE pour établir une connexion VPN avec l'ASA. Définissez l'une des politiques IKE suivantes pour faciliter les connexions depuis les clients VPN natifs Windows 7.

Suivez la procédure *Configuring L2TP over IPsec for ASA*. Ajoutez les étapes supplémentaires dans cette tâche pour configurer la politique IKE pour les clients VPN natifs de Windows 7.

### Procédure

**Étape 1** Affichez les attributs ainsi que le nombre de politiques IKE existantes.

**Exemple :**

```
hostname(config)# show run crypto ikev1
```

**Étape 2** Configurez une politique IKE. L'argument **number** spécifie le numéro de la politique IKE que vous configurez. Ce numéro figurait dans la sortie de la commande **show run crypto ikev1**.

**crypto ikev1 policy nombre**

**Étape 3** Définissez la méthode d'authentification que l'ASA utilise pour établir l'identité de chaque homologue IPsec afin d'employer des clés prépartagées.

**Exemple :**

```
hostname(config-ikev1-policy)# authentication pre-share
```

- Étape 4** Choisissez une méthode de chiffrement symétrique qui protège les données transmises entre deux homologues IPsec. Pour Windows 7, choisissez **aes** pour AES 128 bits, ou **aes-256**.
- encryption** {|aes|aes-256}
- Étape 5** Choisissez l'algorithme de hachage qui garantit l'intégrité des données. Pour Windows 7, spécifiez **sha** pour l'algorithme SHA-1.
- Exemple :**
- ```
hostname (config-ikev1-policy) # hash sha
```
- Étape 6** Choisissez l'identifiant de groupe Diffie-Hellman. Vous pouvez spécifier 14 pour les types de chiffrement aes et aes-256.
- Exemple :**
- ```
hostname (config-ikev1-policy) # group 14
```
- Étape 7** Précisez la durée de vie de la SA en secondes. Pour Windows 7, spécifiez 86 400 secondes pour représenter 24 heures.
- Exemple :**
- ```
hostname (config-ikev1-policy) # lifetime 86400
```

Exemple de configuration pour L2TP sur IPsec

L'exemple suivant montre les commandes de fichier de configuration qui assurent la compatibilité de l'ASA avec un client VPN natif sur n'importe quel système d'exploitation :

```
ip local pool sales_addresses 209.165.202.129-209.165.202.158
group-policy sales_policy internal
group-policy sales_policy attributes
  wins-server value 209.165.201.3 209.165.201.4
  dns-server value 209.165.201.1 209.165.201.2
  vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
  default-group-policy sales_policy
  address-pool sales_addresses
tunnel-group DefaultRAGroup ipsec-attributes
  pre-shared-key *
tunnel-group DefaultRAGroup ppp-attributes
  no authentication pap
  authentication chap
  authentication ms-chap-v1
  authentication ms-chap-v2

crypto ipsec ikev1 transform-set trans esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set trans mode transport
crypto dynamic-map dyno 10 set ikev1 transform-set trans
crypto map vpn 20 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
  authentication pre-share
```

```

encryption aes
hash sha

```

```

group 14
lifetime 86400

```

Historique des fonctionnalités pour L2TP sur IPsec

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
L2TP sur IPsec	7.2(1)	L2TP sur IPsec permet de déployer et d'utiliser une solution VPN L2TP des services de VPN et de pare-feu IPsec sur une plateforme unique. Le principal avantage de la configuration de L2TP sur IPsec dans un scénario d'accès à distance est que les utilisateurs distants peuvent accéder à un réseau IP public sans passerelle ni ligne dédiée, ce qui permet l'accès depuis pratiquement n'importe quel endroit disposant du réseau téléphonique commuté (POTS). Un avantage supplémentaire est que la seule exigence pour l'accès au VPN est l'utilisation de Windows avec la mise en réseau Dial-Up Networking (DUN). Aucun logiciel client supplémentaire, tel que le logiciel client VPN Cisco, n'est requis. Les commandes suivantes ont été introduites ou modifiées : authentication eap-proxy, authentication ms-chap-v1, authentication ms-chap-v2, authentication pap, l2tp tunnel hello, vpn-tunnel-protocol l2tp-ipsec.
Dépréciation des chiffrements IKE/IPsec et des chiffrements d'intégrité/PRF Prise en charge du groupe DH 14 pour IKEv1	9.13(1)	Les chiffrements/intégrité/PRF suivants sont obsolètes et seront supprimés dans la version ultérieure 9.14(1) : • Chiffrement 3DES • Chiffrement DES • Intégrité MD5 Ajout de la prise en charge du groupe DH 14 (par défaut) pour IKEv1. Les commandes de groupe 2 et groupe 5 sont obsolètes et seront supprimées dans la version ultérieure 9.14(1).



CHAPITRE 3

Options de haute disponibilité

- Options de haute disponibilité, à la page 55
- Équilibrage de la charge VPN, à la page 57

Options de haute disponibilité

Distributed VPN Clustering (Mise en grappe VPN distribuée), Load balancing (Équilibrage de charge) et Failover (Basculement) sont des fonctionnalités de haute disponibilité qui fonctionnent différemment et ont des exigences différentes. Dans certains cas, vous pouvez utiliser plusieurs capacités dans votre déploiement. Les sections suivantes décrivent ces fonctionnalités. Reportez-vous à la version appropriée du [Guide de configuration de l'interface de ligne de commande pour les opérations générales d'ASA](#) pour en savoir plus sur Distributed VPN (VPN distribué) et Failover (Basculement). Les détails de l'équilibrage de la charge sont inclus ici.

VPN et mise en grappe sur le châssis Cisco Secure Firewall eXtensible Operating System (FXOS)

Une grappe ASA FXOS prend en charge l'un des deux modes mutuellement exclusifs pour le VPN de S2S, centralisé ou distribué :

- Mode VPN centralisé. Le mode par défaut. En mode centralisé, les connexions VPN sont établies avec l'unité de commande de grappe uniquement.

La fonctionnalité VPN est limitée à l'unité de contrôle et ne tire pas parti des capacités de haute disponibilité de la grappe. Si l'unité de contrôle tombe en panne, toutes les connexions VPN existantes sont perdues et les utilisateurs connectés au VPN subissent une interruption de service. Lorsqu'une nouvelle unité de contrôle est choisie, vous devez rétablir les connexions VPN.

Lorsque vous connectez un tunnel VPN à une adresse d'interface étendue, les connexions sont automatiquement transférées à l'unité de contrôle. Les clés et les certificats VPN sont répliqués sur toutes les unités.

- Mode de VPN distribué. Dans ce mode, les connexions VPN S2S IPsec IKEv2 sont réparties sur les membres d'une grappe ASA, ce qui offre une grande évolutivité. La distribution des connexions VPN entre les membres d'une grappe permet d'utiliser pleinement la capacité et le débit de la grappe, ce qui augmente considérablement la prise en charge des VPN au-delà des capacités VPN centralisées.

**Remarque**

Le mode de mise en grappe VPN centralisée prend en charge S2S IKEv1 et S2S IKEv2.

Le mode de mise en grappe du VPN distribué prend uniquement en charge S2S, IKEv2.

Le mode de mise en grappe du VPN distribué est pris en charge sur le Firepower 9300 uniquement.

Le VPN d'accès à distance n'est pas pris en charge en mode de mise en grappe de VPN centralisé ou distribué.

Équilibrage de la charge VPN

L'équilibrage de charge VPN est un mécanisme permettant de distribuer équitablement le trafic VPN d'accès à distance entre les périphériques d'un groupe d'équilibrage de charge VPN. L'équilibrage de charge VPN est basé sur une répartition simple du trafic sans prendre en compte le débit ou d'autres facteurs. Un groupe d'équilibrage de la charge VPN se compose d'au moins deux périphériques. L'un des périphériques sert de directeur et les autres périphériques sont des périphériques membres. Il n'est pas nécessaire que les périphériques d'un groupe soient exactement du même type ou aient des versions de logiciels ou des configurations identiques.

Tous les périphériques actifs dans un groupe d'équilibrage de la charge VPN transportent des charges de session. L'équilibrage de charge VPN dirige le trafic vers le périphérique le moins chargé du groupe, distribuant la charge sur tous les périphériques. Il utilise efficacement les ressources système et offre des performances accrues et une disponibilité élevée.

Basculement

Une configuration de basculement nécessite deux ASA identiques connectés l'un à l'autre par une liaison de basculement dédiée et, éventuellement, une liaison de basculement avec état. L'intégrité des unités actives et des interfaces est surveillée pour déterminer si les conditions spécifiques au basculement sont respectées. Si ces conditions sont remplies, le basculement se produit. Le basculement prend en charge les configurations VPN et pare-feu.

L'ASA prend en charge deux configurations de basculement : basculement actif/actif et basculement actif/en veille.

Avec le basculement actif/actif, les deux unités peuvent transmettre le trafic réseau. Il ne s'agit pas d'un véritable équilibrage de charge, bien qu'il puisse sembler avoir le même effet. En cas de basculement, l'unité active restante prend le relais en transmettant le trafic combiné, en fonction des paramètres configurés. Par conséquent, lors de la configuration du basculement actif/actif, vous devez vous assurer que le trafic combiné des deux unités demeure dans la capacité de chacune.

Avec le basculement actif/en veille, une seule unité transmet le trafic, tandis que l'autre attend en état de veille et ne transmet pas de trafic. Le basculement actif/en veille vous permet d'utiliser un second ASA pour prendre le relais des fonctions d'une unité défaillante. Lorsque l'unité active tombe en panne, elle passe à l'état de veille, tandis que l'unité en veille passe à l'état actif. L'unité qui devient active adopte les adresses IP (ou, pour le pare-feu transparent, l'adresse IP de gestion) et les adresses MAC de l'unité défaillante et commence à transmettre le trafic. L'unité maintenant en veille reprend les adresses IP de veille de l'unité active. En cas de défaillance d'une unité active, l'unité en veille prend le relais sans interruption du tunnel VPN client.

Équilibrage de la charge VPN

À propos de l'équilibrage de charge VPN

Si vous avez une configuration client distant dans laquelle vous utilisez deux périphériques de sécurité adaptables Cisco ou plus connectés au même réseau pour gérer les sessions à distance, vous pouvez configurer ces périphériques pour partager leur charge de session en créant un groupe d'équilibrage de charge VPN. L'équilibrage de charge VPN dirige le trafic vers le périphérique le moins chargé du groupe, distribuant la charge sur tous les périphériques. Il utilise efficacement les ressources système et offre des performances accrues et une disponibilité élevée.

Tous les périphériques d'un groupe d'équilibrage de charge VPN transportent des charges de session. Un périphérique du groupe, le *directeur*, dirige les demandes de connexion entrantes vers les autres périphériques, appelés *périphériques membres*. Le directeur surveille tous les périphériques du groupe, suit le niveau de charge de chaque périphérique et répartit la charge de session en conséquence. Le rôle de directeur n'est pas lié à un appareil physique; il peut se déplacer entre les périphériques. Par exemple, si le directeur actuel tombe en panne, l'un des périphériques membres du groupe assume ce rôle et devient immédiatement le nouveau directeur.

Le groupe d'équilibrage de charges VPN apparaît aux clients externes comme une adresse IP virtuelle unique. Cette adresse IP n'est pas liée à un périphérique physique particulier. Elle appartient au directeur actuel. Un client VPN qui tente d'établir une connexion se connecte d'abord à l'adresse IP virtuelle. Le directeur renvoie ensuite au client l'adresse IP publique de l'hôte disponible le moins chargé du groupe. Dans une deuxième transaction (transparente pour l'utilisateur), le client se connecte directement à cet hôte. De cette manière, le directeur de groupe d'équilibrage de charge du VPN dirige le trafic de manière uniforme et efficace entre les ressources.

En cas de défaillance d'un ASA dans le groupe, les sessions interrompues peuvent se reconnecter immédiatement à l'adresse IP virtuelle. Le directeur dirige ensuite ces connexions vers un autre périphérique actif du groupe. Si le directeur tombe en panne, un périphérique membre du groupe prend immédiatement et automatiquement le relais en tant que nouveau directeur. Même en cas de défaillance de plusieurs périphériques du groupe, les utilisateurs peuvent continuer à se connecter au groupe tant qu'un périphérique du groupe est opérationnel et disponible.

Pour chaque périphérique de grappe d'équilibrage de charge VPN, vous devez configurer les interfaces publiques/externes (lpublic) et privées/internes (lprivate).

- Interface publique : interface externe du périphérique utilisée pour la communication initiale avec l'adresse IP de la grappe. Cette interface est utilisée pour l'établissement de liaison Hello.
- Interface privée : interface interne du périphérique utilisée pour la messagerie entre les membres de la grappe d'équilibrage de charge. Ces messages comprennent des messages keepalives, des messages de topologie et des messages de hors-service liés à l'équilibrage de charge.

Algorithme d'équilibrage de charge VPN

Le directeur de groupe d'équilibrage de charge VPN conserve une liste triée des membres du groupe dans l'ordre croissant des adresses IP. La charge de chaque membre est calculée sous la forme d'un pourcentage entier (le nombre de sessions actives). Les sessions inactives Secure Client (services client sécurisés) ne sont pas prises en compte dans la charge VPN SSL pour l'équilibrage de charge VPN. Le directeur redirige les tunnels IPsec et SSL vers le périphérique ayant la charge la plus faible jusqu'à ce qu'il soit de 1 % supérieur

à celui des autres. Lorsque tous les membres sont supérieurs de 1 % au directeur, le directeur redirige le trafic vers lui-même.

Par exemple, si vous avez un directeur et deux membres, le cycle suivant s'applique :



Remarque Tous les nœuds commencent par 0 %, et tous les pourcentages sont arrondis à la moitié.

1. Le directeur établit la connexion si tous les membres ont une charge de 1 % supérieure à celle du directeur.
2. Si le directeur ne prend pas la connexion, la session est prise en charge par le périphérique membre ayant le pourcentage de charge le plus bas.
3. Si tous les membres ont le même pourcentage de charge, le membre ayant le moins de sessions obtient la session.
4. Si tous les membres ont le même pourcentage de charge et le même nombre de sessions, le membre ayant l'adresse IP la plus basse obtient la session.

Configurations de groupes d'équilibrage de charge VPN

Un groupe d'équilibrage de charge VPN peut être composé de l'ASA de la même version ou de versions mixtes sous réserve des restrictions suivantes :

- Les groupes d'équilibrage de charge VPN qui se composent des deux mêmes versions ASA peuvent exécuter l'équilibrage de charge VPN pour un mélange de sessions IPsec, Secure Client (services client sécurisés) et de VPN SSL sans client.
- Les groupes d'équilibrage de charge VPN qui comprennent des versions mixtes de l'ASA peuvent prendre en charge les sessions IPsec. Dans une telle configuration, cependant, les ASA peuvent ne pas atteindre leur pleine capacité IPsec.

Le directeur du groupe attribue des demandes de session aux membres du groupe. L'ASA considère toutes les sessions, SSL VPN ou IPsec, comme égales, et les affecte en conséquence. Vous pouvez configurer le nombre de sessions VPN IPsec et SSL à autoriser, jusqu'au nombre maximal autorisé par votre configuration et votre licence.

Nous avons testé jusqu'à 10 nœuds dans un groupe d'équilibrage de charge VPN. Des groupes plus importants peuvent fonctionner, mais nous ne prenons pas en charge publiquement ces topologies.

Élection du directeur d'équilibrage de charge VPN

Processus d'élection du directeur

Chaque non-maître dans la grappe virtuelle gère une base de données de topologie locale. Cette base de données est mise à jour par le maître chaque fois que la topologie de la grappe est modifiée. Chaque non-maître passe à l'état d'élection de maître lorsqu'aucune réponse Hello n'est reçue du maître ou qu'aucune réponse keepalive n'est reçue du maître après un nombre maximal de tentatives.

Le membre effectue les fonctions suivantes pendant l'élection du directeur :

- Compare la priorité de chaque unité d'équilibrage de charge trouvée dans la base de données de topologie locale.

- Si deux unités avec la même priorité sont trouvées, une avec l'adresse IP la plus basse est choisie.
- Si le membre lui-même est choisi, il réclame l'adresse IP virtuelle.
- Si l'un des autres membres est choisi, le membre envoie une demande Hello au maître choisi.
- Lorsque deux unités membres tentent de réclamer l'adresse IP virtuelle, le sous-système ARP détecte la condition d'adresse IP en double et envoie une notification pour demander au membre ayant l'adresse MAC la plus élevée d'abandonner le rôle de directeur.

Établissement de liaison Hello

Chaque membre envoie une demande Hello à l'adresse IP de la grappe virtuelle sur l'interface externe au démarrage. Si une demande Hello est reçue, le maître envoie sa propre demande Hello au membre. Le membre non-directeur renvoie une réponse Hello à la réception d'une demande Hello du directeur. Cela met fin à l'établissement de liaison Hello.

Une fois l'établissement de liaison Hello terminé, la connexion est lancée sur l'interface interne si le chiffrement est configuré. Si aucune réponse Hello n'est reçue par le membre après un nombre maximal de tentatives, le membre passe à l'état d'élection de maître.

Messages keepalive

Une fois l'établissement de liaison Hello effectué entre un membre et le directeur, chaque unité membre envoie des demandes keepalive périodiques au maître avec ses informations de charge. Les demandes keepalive sont envoyées par une unité membre à des intervalles d'une seconde pendant le traitement normal s'il n'y a aucune réponse keepalive en attente du directeur. Cela signifie que la prochaine demande keepalive est envoyée la seconde suivante, tant que les réponses keepalive de la demande précédente ont été reçues. Si le membre n'a pas reçu de réponse keepalive du directeur pour la demande keepalive précédente, aucune demande keepalive n'est envoyée la seconde suivante. Au lieu de cela, la logique de délai d'expiration keepalive du membre démarre.

Le délai d'expiration keepalive fonctionne comme suit :

1. Si un membre attend une réponse keepalive du directeur, le membre n'envoie pas la demande keepalive normale d'une seconde.
2. Le membre attend pendant 3 secondes et envoie une demande keepalive à la 4e seconde.
3. Le membre répète l'étape 2 ci-dessus cinq (5) fois tant qu'il n'y a pas de réponse keepalive du directeur.
4. Ensuite, le membre déclare le directeur comme parti et commence un nouveau cycle d'élection de directeur.

Foire aux questions sur l'équilibrage de la charge VPN

- [Mode contexte multiple](#)
- [Épuisement de l'ensemble d'adresses IP](#)
- [Ensembles d'adresses IP uniques](#)
- [Utilisation de l'équilibrage de la charge et du basculement VPN sur le même périphérique](#)
- [Équilibrage de la charge VPN sur plusieurs interfaces](#)
- [Nombre maximal de sessions simultanées pour les groupes d'équilibrage de la charge VPN](#)

Mode contexte multiple

- Q.** L'équilibrage de la charge VPN est-il pris en charge en mode de contexte multiple?
- A.** Ni l'équilibrage de la charge VPN ni le basculement avec état ne sont pris en charge en mode de contexte multiple.

Épuisement de l'ensemble d'adresses IP

- Q.** L'ASA prend-elle en compte l'épuisement de l'ensemble d'adresses IP dans le cadre de sa méthode d'équilibrage de la charge VPN?
- A.** Non. Si la session VPN d'accès à distance est dirigée vers un périphérique qui a épuisé ses ensembles d'adresses IP, la session ne s'établit pas. L'algorithme d'équilibrage de la charge est basé sur la charge et est calculé comme un pourcentage entier (nombre de sessions actives et nombre maximal) que chaque membre fournit.

Ensembles d'adresses IP uniques

- Q.** Pour mettre en œuvre l'équilibrage de la charge VPN, les ensembles d'adresses IP pour les clients Secure Client (services client sécurisés) ou IPsec sur différents ASA doivent-ils être uniques?
- A.** Oui. Les ensembles d'adresses IP doivent être uniques pour chaque périphérique.

Utilisation de l'équilibrage de la charge et du basculement VPN sur le même périphérique

- Q.** Un seul périphérique peut-il utiliser à la fois l'équilibrage de la charge et le basculement VPN?
- A.** Oui. Dans cette configuration, le client se connecte à l'adresse IP du groupe et est redirigé vers l'ASA le moins chargé dans le groupe. Si ce périphérique tombe en panne, l'unité de secours prend le relais immédiatement et il n'y a aucune incidence sur le tunnel VPN.

Équilibrage de la charge VPN sur plusieurs interfaces

- Q.** Si nous activons le VPN SSL sur plusieurs interfaces, est-il possible de mettre en œuvre l'équilibrage de la charge VPN pour les deux interfaces?
- A.** Vous ne pouvez définir qu'une seule interface pour participer au groupe d'équilibrage de la charge VPN en tant qu'interface publique. L'objectif est d'équilibrer les charges de processeur. Plusieurs interfaces convergent sur le même processeur, de sorte que le concept d'équilibrage de la charge VPN sur plusieurs interfaces n'améliorera pas les performances.

Nombre maximal de sessions simultanées pour les groupes d'équilibrage de la charge VPN

- Q.** Envisagez un déploiement de deux Firepower 1150, chacun avec une licence VPN SSL de 100 utilisateurs. Dans un groupe d'équilibrage de charge VPN, le nombre total maximal d'utilisateurs autorise-t-il 200

sessions simultanées, ou seulement 100 ? Si nous ajoutons un troisième périphérique ultérieurement avec une licence pour 100 utilisateurs, pouvons-nous prendre en charge 300 sessions simultanées ?

- A. Avec l'équilibrage de charge VPN, tous les périphériques sont actifs, de sorte que le nombre maximal de sessions que votre groupe peut prendre en charge est le nombre total de sessions pour chacun des périphériques du groupe, dans ce cas 300.

Licences pour l'équilibrage de charge VPN

L'équilibrage de charge VPN comporte les exigences de licence suivantes :

- Une licence 3DES/AES active.

L'ASA vérifie l'existence de cette licence de chiffrement avant d'activer l'équilibrage de charges VPN. S'il ne détecte pas de licence 3DES ou AES active, l'ASA empêche l'activation de l'équilibrage de charge VPN et empêche également la configuration interne de 3DES par le système d'équilibrage de charge VPN, sauf si la licence autorise cet usage.

- Une licence Security Plus valide pour cette fonctionnalité activée sur votre pare-feu.
- Vous devez avoir suffisamment de ces licences Security Plus dans votre compte Smart pour respecter la conformité.

Conditions préalables à l'équilibrage de la charge VPN

Veuillez consulter également le [Directives et limites pour l'équilibrage de charge VPN, à la page 62](#).

- L'équilibrage de charge VPN est désactivé par défaut. Vous devez activer explicitement l'équilibrage de charge VPN.

- Vous devez d'abord configurer les interfaces publique (externe) et privée (interne). Les références ultérieures dans cette section utilisent les noms `outside` et `inside`.

Vous pouvez utiliser les commandes **interface** et **nameif** pour configurer différents noms pour ces interfaces.

- Vous devez avoir préalablement configuré l'interface à laquelle l'adresse IP virtuelle fait référence. Établissez une adresse IP virtuelle commune, un port UDP (si nécessaire) et un secret partagé IPsec pour le groupe.
- Tous les périphériques qui font partie d'un groupe doivent partager les mêmes valeurs propres à la grappe : adresse IP, paramètres de chiffrement, clé de chiffrement et port.
- Pour utiliser le chiffrement de groupe d'équilibrage de charge VPN, activez d'abord IKEv1 sur l'interface interne à l'aide de la commande **crypto ikev1 enable**, avec l'interface interne spécifiée ; sinon, vous obtiendrez un message d'erreur lorsque vous tenterez de configurer le chiffrement de groupe d'équilibrage de charge VPN.
- La fonctionnalité d'autorité de certification locale n'est pas prise en charge si vous utilisez le basculement avec état actif/actif ou l'équilibrage de charge VPN. L'autorité de certification locale ne peut pas être subordonnée à une autre autorité de certification ; elle ne peut servir que d'autorité de certification racine.

Directives et limites pour l'équilibrage de charge VPN

Clients admissibles

L'équilibrage de charge VPN est efficace uniquement pour les sessions distantes lancées avec les clients suivants :

- Secure Client (version 3.0 et ultérieure)
- ASA 5505 (en tant que client VPN facile)
- Firepower 1010 (en tant que client VPN facile)
- Périphériques clients IOS EZVPN prenant en charge la redirection IKE (IOS 831/871)

Points à considérer

L'équilibrage de charge VPN fonctionne avec les clients IPsec et les sessions client VPN SSL. Tous les autres types de connexion VPN (L2TP, PPTP, L2TP/IPsec), y compris les connexions de site à site, peuvent se connecter à un ASA sur lequel l'équilibrage de charge VPN est activé, mais ils ne peuvent pas participer à l'équilibrage de charge VPN.

Lorsque plusieurs nœuds ASA sont regroupés pour l'équilibrage de charge et que l'utilisation des URL de groupe est souhaitée pour les connexions Secure Client (services client sécurisés), les nœuds ASA individuels doivent :

- Configurez chaque profil de connexion d'accès à distance avec une URL de groupe pour chaque adresse virtuelle d'équilibrage de charge VPN (IPv4 et IPv6).
- Configurez une URL de groupe pour l'adresse publique d'équilibrage de charge VPN de ce nœud.

Groupes d'équilibrage de charge

- L'ASA prend en charge 10 périphériques par groupe d'équilibrage de charge VPN.
- Le mode UCAPL ne prend pas en charge l'équilibrage de charge VPN, même lorsque le chiffrement est désactivé. En mode UCAPL, utilisez IKEv2 pour établir un tunnel sécurisé.

Mode contextuel

L'équilibrage de charge VPN n'est pas pris en charge en mode de contexte multiple.

FIPS

Le chiffrement de grappe n'est pas pris en charge avec FIPS.

Vérification du certificat

Lors de la vérification du certificat pour l'équilibrage de charge VPN avec Secure Client (services client sécurisés), si la connexion est redirigée par une adresse IP, le client effectue toutes ses vérifications de nom à l'aide de cette adresse IP. Assurez-vous que l'adresse IP de redirection est répertoriée dans le nom commun des certificats ou le nom alternatif du sujet. Si l'adresse IP n'est pas présente dans ces champs, le certificat sera considéré comme non fiable.

Suivant les directives définies dans la RFC 2818, si un **subject alt name** (nom alternatif du sujet) est inclus dans le certificat, nous utilisons uniquement le **subject alt name** (nom alternatif du sujet) pour les vérifications de nom, et nous ignorons le nom commun. Assurez-vous que l'adresse IP du serveur présentant le certificat est définie dans le **subject alt name** (nom alternatif du sujet) du certificat.

Pour un ASA autonome, l'adresse IP est l'adresse IP de cet ASA. Dans une situation de groupe d'équilibrage de charge VPN, cela dépend de la configuration du certificat. Si le groupe utilise un seul certificat, celui-ci doit comporter des extensions SAN pour l'adresse IP virtuelle et le FQDN du groupe, et doit contenir des extensions Subject Alternative Name incluant l'adresse IP et le FQDN de chaque ASA. Si le groupe utilise plusieurs certificats, le certificat de chaque ASA doit comporter des extensions SAN pour l'adresse IP virtuelle, le FQDN du groupe, ainsi que l'adresse IP et le FQDN de l'ASA concerné.

Équilibrage de charge de VPN géographique

Dans un environnement d'équilibrage de charge VPN géographique où les résolutions DNS sont modifiées à intervalles réguliers, vous devez examiner attentivement la façon de définir la valeur de durée de vie (TTL). Pour que la configuration d'équilibrage de charge DNS fonctionne correctement avec Secure Client (services client sécurisés), le mappage nom-adresse de l'ASA doit rester identique entre le moment où l'ASA est sélectionné et celui où le tunnel est entièrement établi. Si trop de temps s'écoule avant que les informations d'authentification soient saisies, la recherche redémarre et une adresse IP différente peut devenir l'adresse résolue. Si le mappage DNS passe à un autre ASA avant la saisie des informations d'authentification, le tunnel VPN échoue.

L'équilibrage de charge géographique pour le VPN utilise souvent un sélecteur de site global Cisco (GSS). Le GSS utilise DNS pour l'équilibrage de charge, et la valeur de durée de vie (TTL) pour la résolution DNS est par défaut de 20 secondes. Vous pouvez réduire considérablement la probabilité d'échecs de connexion si vous augmentez la valeur TTL sur le GSS. L'augmentation à une valeur beaucoup plus élevée permet de disposer de suffisamment de temps pour la phase d'authentification lorsque l'utilisateur saisit les informations d'authentification et établit le tunnel.

Pour augmenter le temps de saisie des informations d'authentification, vous pouvez également envisager de désactiver la connexion au démarrage.

Associations de sécurité IKE/IPSec

Les sessions de chiffrement de grappe ne se synchronisent pas en mode veille dans une topologie d'équilibreur de charge VPN.

Configuration de l'équilibrage de charge du VPN

Si vous avez une configuration client distant dans laquelle vous utilisez deux périphériques ASA ou plus connectés au même réseau pour gérer les sessions à distance, vous pouvez configurer ces périphériques pour partager leur charge de session. L'équilibrage de charge VPN dirige le trafic de session vers le périphérique le moins chargé du groupe, distribuant la charge sur tous les périphériques. L'équilibrage de charge VPN utilise efficacement les ressources système et offre des performances accrues et une disponibilité élevée.

Pour utiliser l'équilibrage de charge VPN, procédez comme suit sur chaque périphérique du groupe :

- Configurez le groupe d'équilibrage de charge VPN en établissant des attributs de groupe d'équilibrage de charge VPN communs. Cela inclut une adresse IP virtuelle, un port UDP (si nécessaire) et un secret partagé IPsec pour le groupe. Tous les participants du groupe doivent avoir une configuration de groupe identique, à l'exception de la priorité du périphérique dans le groupe.

- Configurez un périphérique participant en activant l'équilibrage de charge VPN sur le périphérique et en définissant les propriétés spécifiques au périphérique. Ces valeurs varient d'un appareil à l'autre.

Configurer les interfaces publique et privée pour l'équilibrage de charge VPN

Pour configurer les interfaces publique (externe) et privée (interne) pour les périphériques du groupe d'équilibrage de charge VPN, procédez comme suit.

Procédure

- Étape 1** Configurez l'interface publique sur l'ASA en saisissant la commande **interface** avec le mot-clé **lbpublic** en mode de configuration vpn-load-balancing. Cette commande spécifie le nom ou l'adresse IP de l'interface publique pour l'équilibrage de charge VPN pour ce périphérique :

Exemple :

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic outside
hostname(config-load-balancing)#
```

- Étape 2** Configurez l'interface privée sur l'ASA en saisissant la commande **interface** avec le mot-clé **lbprivate** en mode de configuration vpn-load-balancing. Cette commande spécifie le nom ou l'adresse IP de l'interface privée pour l'équilibrage de charge VPN pour ce périphérique :

Exemple :

```
hostname(config-load-balancing)# interface lbprivate inside
hostname(config-load-balancing)#
```

- Étape 3** Définissez la priorité à attribuer à ce périphérique dans le groupe. La plage est de 1 à 10. La priorité indique la probabilité que ce périphérique devienne le directeur de groupe, soit au démarrage du périphérique, soit lorsqu'un directeur existant tombe en panne. Plus la priorité définie est élevée, par exemple 10, plus il est probable que ce périphérique devienne le directeur de groupe.

Exemple :

Par exemple, pour attribuer à ce périphérique une priorité de 6 dans le groupe, saisissez la commande suivante :

```
hostname(config-load-balancing)# priority 6
hostname(config-load-balancing)#
```

- Étape 4** Si vous souhaitez appliquer la traduction d'adresses réseau à ce périphérique, entrez la commande **nat** avec l'adresse attribuée par la NAT pour ce périphérique. Vous pouvez définir une adresse IPv4 et IPv6 ou préciser le nom d'hôte du périphérique.

Exemple :

Par exemple, pour attribuer à ce périphérique une adresse NAT de 192.168.30.3 et 2001:DB8::1, saisissez la commande suivante :


```
hostname(config-load-balancing)# nat 192.168.30.3 2001:DB8::1
hostname(config-load-balancing)#
```

Configurer les attributs du groupe d'équilibrage de charge VPN

Pour configurer les attributs du groupe d'équilibrage de charge VPN pour chaque périphérique du groupe, procédez comme suit :

Procédure

Étape 1 Configurez l'équilibrage de charges VPN en saisissant la commande **vpn load-balancing** en mode de configuration globale :

Exemple :

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)#
```

Il passe en mode de configuration vpn-load-balancing, dans lequel vous pouvez configurer les attributs d'équilibrage de charge restants.

Étape 2 Configurez l'adresse IP ou le nom de domaine complet du groupe auquel ce périphérique appartient. Cette commande spécifie l'adresse IP unique ou le nom de domaine complet (FQDN) qui représente l'ensemble du groupe d'équilibrage de charge VPN. Choisissez une adresse IP comprise dans la plage d'adresses de sous-réseau public partagée par tous les ASAs du groupe. Vous devez spécifier un IPv4 (obligatoire). Vous pouvez éventuellement fournir une adresse IPv6.

Exemple :

Pour configurer les adresses virtuelles IPv4 et IPv6, entrez la commande suivante :

```
hostname(config-load-balancing)# cluster ip address 192.168.10.1 1000::2
hostname(config-load-balancing)# show running-config vpn load-balancing
vpn load-balancing
redirect-fqdn enable
cluster key *****
cluster ip address 192.168.10.1 1000::2
cluster encryption
```

Pour configurer une adresse IPv6 pour une grappe d'équilibrage de charge VPN, une configuration d'adresse IPv4 est obligatoire. Si vous configurez uniquement une adresse IPv6 virtuelle, un message d'erreur s'affiche.

```
hostname(config-load-balancing)# show running-config vpn load-balancing
vpn load-balancing
redirect-fqdn enable
cluster key *****
cluster encryption
participate
hostname(config-load-balancing)# cluster ip address 1000::2
ERROR: Virtual IPv4 address is not set
```

Étape 3 Configurez le port de groupe. Cette commande spécifie le port UDP pour le groupe d'équilibrage de charge VPN auquel ce périphérique participe. La valeur par défaut est 9023. Si une autre application utilise ce port, saisissez le numéro de port de destination UDP que vous souhaitez utiliser pour l'équilibrage de charge.

Exemple :

Par exemple, pour définir le port de groupe à 4444, entrez la commande suivante :

```
hostname(config-load-balancing)# cluster port 4444
hostname(config-load-balancing)#
```

Étape 4 (Facultatif) Activez le chiffrement IPsec pour le groupe d'équilibrage de charge VPN.

La valeur par défaut est sans chiffrement. Cette commande active ou désactive le chiffrement IPsec. Si vous configurez cet attribut, vous devez d'abord spécifier et vérifier un secret partagé. Les ASA du groupe d'équilibrage de charge VPN communiquent au moyen de tunnels LAN à LAN utilisant IPsec. Pour vous assurer que toutes les informations d'équilibrage de charge communiquées entre les périphériques sont chiffrées, activez cet attribut.

Remarque

Pour utiliser le chiffrement de groupe d'équilibrage de charge VPN, activez d'abord IKEv1 sur l'interface interne à l'aide de la commande **crypto ikev1 enable**, avec l'interface interne spécifiée ; sinon, vous obtiendrez un message d'erreur lorsque vous tenterez de configurer le chiffrement de groupe d'équilibrage de charge VPN.

Si IKEv1 a été activé lorsque vous avez configuré le chiffrement de groupe, mais a été désactivé avant d'avoir configuré la participation du périphérique dans le groupe, vous recevez un message d'erreur lorsque vous entrez la commande **participate**, et le chiffrement n'est pas activé pour le groupe.

Exemple :

```
hostname(config)# crypto ikev1 enable inside
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)#
```

Étape 5 Si vous activez le chiffrement de groupe, vous devez également spécifier le secret partagé IPsec en saisissant la commande **cluster key**. Cette commande spécifie le secret partagé entre les homologues IPsec lorsque vous avez activé le chiffrement IPsec. La valeur que vous saisissez dans le champ s'affiche sous forme d'astérisques consécutifs. Si vous devez saisir une clé déjà chiffrée (par exemple, vous l'avez copiée à partir d'une autre configuration), saisissez la commande **cluster key 8 key**.

Exemple :

Par exemple, pour définir le secret partagé à 123456789, entrez la commande suivante :

```
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)#
```

Étape 6 Activez la participation de ce périphérique au groupe en saisissant la commande **participate** :

Exemple :

```
hostname(config-load-balancing) # participate
hostname(config-load-balancing) #
```

Prochaine étape

Lorsque plusieurs nœuds ASA sont regroupés pour l'équilibrage de la charge et que l'utilisation des URL de groupe est souhaitée pour les connexions Secure Client (services client sécurisés), sur les nœuds ASA individuels, vous devez :

- Configurez chaque profil de connexion d'accès à distance avec une URL de groupe pour chaque adresse virtuelle d'équilibrage de charge (IPv4 et IPv6).
- Configurez une URL de groupe pour l'adresse publique d'équilibrage de charge VPN de ce nœud.

Utilisez la commande **tunnel-group**, **general-attributes**, **group-url** pour configurer ces URL de groupe.

Activation de la redirection à l'aide d'un nom de domaine complet

Par défaut, l'ASA envoie uniquement les adresses IP dans la redirection de l'équilibrage de charge VPN à un client. Si des certificats utilisés sont basés sur les noms DNS, les certificats ne seront pas valides lorsqu'ils sont redirigés vers un périphérique membre.

En tant que directeur d'équilibrage de charge VPN, cet ASA peut envoyer un nom de domaine complet (FQDN), à l'aide de la recherche DNS inversée, d'un périphérique membre (un autre ASA dans le groupe) au lieu de son adresse IP externe lors de la redirection des connexions client VPN vers ce périphérique membre.

Pour activer ou désactiver la redirection à l'aide d'un nom de domaine complet en mode d'équilibrage de charge VPN, utilisez la commande **redirect-fqdn enable** en mode de configuration globale. Le paramètre par défaut est désactivé.

Avant de commencer

Toutes les interfaces réseau externes et internes des périphériques d'équilibrage de charge VPN d'un groupe doivent se trouver sur le même réseau IP.

Procédure

Étape 1 Activez l'utilisation des noms de domaine complets pour l'équilibrage de charge VPN.

```
redirect-fqdn {enable | disable}
```

Exemple :

```
hostname(config) # vpn load-balancing
hostname(config-load-balancing) # redirect-fqdn enable
hostname(config-load-balancing) #
```

Étape 2 Ajoutez une entrée pour chacune de vos interfaces externes ASA dans votre serveur DNS si ces entrées ne sont pas déjà présentes. Chaque adresse IP externe ASA doit être associée à une entrée DNS pour les recherches. Ces entrées DNS doivent également être activées pour la recherche inversée.

- Étape 3** Activez les recherches DNS sur votre ASA avec la commande **dns domain-lookup inside** ou selon l'interface ayant une voie de routage vers votre serveur DNS.
- Étape 4** Définissez l'adresse IP de votre serveur DNS sur l'ASA. Par exemple : **dns name-server 10.2.3.4** (adresse IP de votre serveur DNS).

Exemples de configuration pour l'équilibrage de charge VPN

Configuration de base de l'interface CLI d'équilibrage de charge VPN

Voici un exemple de séquence de commandes d'équilibrage de charge VPN qui comprend une commande d'interface qui permet la redirection pour un nom de domaine complet, spécifie l'interface publique du groupe en tant que **test** et l'interface privée du groupe en tant que **foo**

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)# participate
```

Affichage des informations d'équilibrage de charge VPN

Le directeur de groupe d'équilibrage de charge VPN reçoit un message périodique de chaque ASA du groupe avec le nombre de sessions actives Secure Client (services client sécurisés) et sans client, ainsi que le nombre maximal de sessions autorisées en fonction des limites configurées ou de licence. Si un ASA dans le groupe affiche une capacité de 100 %, le directeur de groupe ne peut pas rediriger d'autres connexions vers celui-ci. Bien que l'ASA puisse s'afficher comme complet, certains utilisateurs peuvent être dans un état inactif ou en attente de reprise, ce qui gaspille les licences. En guise de solution de rechange, chaque ASA fournit le nombre total de sessions moins les sessions à l'état inactif, plutôt que le nombre total de sessions. Reportez-vous à la commande **-sessiondb summary** dans la référence des commandes ASA. En d'autres termes, les sessions inactives ne sont pas signalées au directeur de groupe. Même si l'ASA est complet (avec certaines sessions inactives), le directeur de groupe redirige toujours les connexions vers celui-ci si nécessaire. Lorsque l'ASA reçoit la nouvelle connexion, la session qui a été inactive le plus longtemps est déconnectée, ce qui permet aux nouvelles connexions de prendre sa licence.

L'exemple suivant montre 100 sessions SSL (actives uniquement) et une charge SSL de 2 %. Ces chiffres n'incluent pas les sessions inactives. En d'autres termes, les sessions inactives ne sont pas prises en compte dans la charge pour l'équilibrage de charge VPN.

```
hostname# show vpn load-balancing
```

```

Status :    enabled
Role :      Master
Failover :   Active
Encryption : enabled
Cluster IP : 192.168.1.100
Peers :      1

```

Load %

Sessions

```

Public IP      Role  Pri Model      IPsec SSL IPsec SSL
192.168.1.9    Master 7  ASA-5540 4      2   216   100
192.168.1.19   Backup 9  ASA-5520 0      0    0     0

```

Historique des fonctionnalités pour l'équilibrage de charge VPN

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Équilibrage de charges VPN avec SAML	9.17(1)	L'ASA prend désormais en charge l'équilibrage VPN avec l'authentification SAML.
Équilibrage de la charge VPN	7.2(1)	Cette fonctionnalité a été introduite.



CHAPITRE 4

Paramètres VPN généraux

La mise en œuvre des réseaux privés virtuels par l'ASA comprend des fonctionnalités utiles qui ne s'inscrivent pas clairement dans des catégories précises. Ce chapitre décrit certaines de ces fonctionnalités.

- [Lignes directrices et limites relatives à la licence, à la page 71](#)
- [Configurer IPsec pour contourner les ACL, à la page 72](#)
- [Permettre le trafic intra-interface \(hairpinning\), à la page 72](#)
- [Définition du nombre maximal de sessions VPN IPsec ou SSL actives, à la page 74](#)
- [Utiliser la mise à jour du client pour assurer des niveaux de révision acceptables du client IPsec, à la page 75](#)
- [Mettre en œuvre une connexion entre une adresse IP attribuée par NAT et une adresse IP publique, à la page 77](#)
- [Configurer les limites de session VPN, à la page 78](#)
- [Utilisation d'un certificat d'identité lors de la négociation, à la page 80](#)
- [Configurer le pool de cœurs de chiffrement, à la page 80](#)
- [Configurer la tunnellation fractionnée dynamique, à la page 81](#)
- [Configuration du tunnel VPN de gestion, à la page 82](#)
- [Affichage des sessions VPN actives, à la page 83](#)
- [À propos de l'application des politiques ISE :, à la page 84](#)
- [Configurer les paramètres avancés SSL, à la page 89](#)
- [Flux persistants tunnelisés IPsec, à la page 95](#)
- [Effacer les configurations WebVPN de l'ASA, à la page 98](#)

Lignes directrices et limites relatives à la licence

Cette section comprend les lignes directrices et les limites de cette fonctionnalité.

Directives relatives au mode contextuel

Pris en charge en mode contexte unique et multiple. Dans la version appropriée du [Guide de configuration de l'interface de ligne de commande pour les opérations générales d'ASA](#), consultez les sections *Lignes directrices pour le mode contexte multiple* pour obtenir la liste de ce qui n'est pas pris en charge en mode contexte multiple et *Nouvelles fonctionnalités* qui présente le détail des éléments ajoutés au fil des versions.

Directives sur le mode pare-feu

Pris en charge uniquement en mode pare-feu routé. Le mode transparent n'est pas pris en charge.

Traduction d'adresses réseau (NAT)

Pour obtenir des lignes directrices et des renseignements sur la configuration de NAT, consultez la section *NAT pour VPN* du *Guide de configuration de l'interface de ligne de commande de Cisco Secure Firewall ASA*.

Configurer IPsec pour contourner les ACL

Pour autoriser tous les paquets provenant d'un tunnel IPsec sans vérifier les ACL des interfaces source et destination, saisissez la commande **sysopt connection permit-vpn** en mode de configuration globale.

Vous pouvez contourner les ACL d'interface pour le trafic IPsec si vous utilisez un concentrateur VPN distinct derrière l'ASA et que vous souhaitez maximiser les performances de l'ASA. En règle générale, vous créez une ACL qui autorise les paquets IPsec à l'aide de la commande **access-list** et l'appliquez à l'interface source. L'utilisation d'une liste de contrôle d'accès (ACL) vous permet de spécifier le trafic exact que vous souhaitez autoriser sur l'ASA.

L'exemple suivant autorise le trafic IPsec à travers l'ASA sans vérifier les ACL :

```
hostname(config)# sysopt connection permit-vpn
```

**Remarque**

Le trafic déchiffré de transit est autorisé depuis le client malgré la présence d'un groupe d'accès sur l'interface externe, qui appelle une ACL **deny ip any any**, alors que **no sysopt connection permit-vpn** est configuré.

La tentative de contrôler l'accès au réseau protégé au moyen d'un VPN de site à site ou d'accès à distance à l'aide de la commande **no sysopt permit-vpn** conjuguée à une ACL sur l'interface externe ne réussit pas.

sysopt connection permit-vpn contourne les ACL de l'interface, tant entrantes que sortantes, où la carte de chiffrement pour ce trafic intéressant est activée, ainsi que les ACL de sortie de toutes les autres interfaces, mais non les ACL d'entrée.

Dans cette situation, lorsque l'accès de gestion interne est activé, l'ACL n'est pas appliquée et les utilisateurs peuvent toujours se connecter à l'ASA à l'aide de SSH. Le trafic vers les hôtes sur le réseau interne est bloqué correctement par la liste de contrôle d'accès, mais le trafic traversant déchiffré vers l'interface interne n'est pas bloqué.

Les commandes **ssh** et **http** ont une priorité supérieure à celle des ACL. Pour refuser le trafic SSH, Telnet ou ICMP vers le boîtier depuis la session VPN, utilisez les commandes **ssh**, **telnet** et **icmp**.

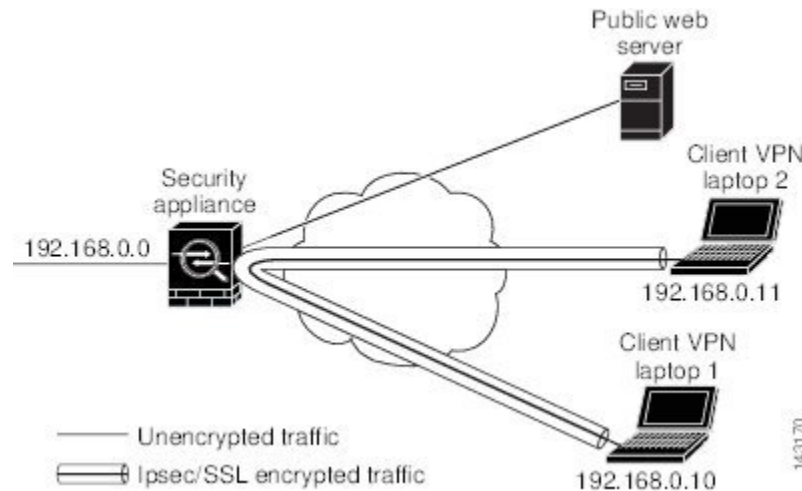
Permettre le trafic intra-interface (hairpinning)

L'ASA comprend une fonctionnalité qui permet à un client VPN d'envoyer un trafic protégé par IPsec à un autre utilisateur VPN en autorisant ce trafic à entrer et à sortir de la même interface. C'est ce qu'on appelle également le « hairpinning », qu'on peut considérer comme des sites distants VPN (clients) se connectant par l'intermédiaire d'un concentrateur VPN (l'ASA).

Le hairpinning peut également rediriger le trafic VPN entrant vers l'extérieur par la même interface que le trafic non chiffré. Cela peut être utile, par exemple, pour un client VPN qui n'a pas de tunnellation fractionnée, mais qui doit à la fois accéder à un VPN et naviguer sur le Web.

La figure ci-dessous montre le client VPN 1 qui envoie un trafic IPsec sécurisé au client VPN 2 tout en envoyant un trafic non chiffré à un serveur Web public.

Illustration 4 : Client VPN utilisant la fonctionnalité intra-interface pour le hairpinning



Pour configurer cette fonctionnalité, utilisez la commande **same-security-traffic** en mode de configuration globale avec son argument **intra-interface**.

La syntaxe de la commande est `same-security-traffic permit {inter-interface | intra-interface}`.

L'exemple suivant montre comment activer le trafic intra-interface :

```
hostname(config)# same-security-traffic permit intra-interface
hostname(config)#
```



Remarque

Utilisez la commande **same-security-traffic** avec l'argument **inter-interface** pour autoriser la communication entre les interfaces ayant le même niveau de sécurité. Cette fonctionnalité n'est pas propre aux connexions IPsec. Pour en savoir plus, consultez le chapitre « Configuration des paramètres d'interface » de ce guide.

Pour utiliser le hairpinning, vous devez appliquer les règles NAT appropriées à l'interface ASA, comme décrit dans les considérations NAT pour le trafic intra-interface.

Considérations sur la NAT pour le trafic intra-interface

Pour que l'ASA renvoie le trafic non chiffré par l'interface, vous devez activer la NAT pour l'interface afin que les adresses routables publiquement remplacent vos adresses IP privées (sauf si vous utilisez déjà des adresses IP publiques dans votre ensemble d'adresses IP locales). L'exemple suivant applique une règle PAT d'interface au trafic provenant de l'ensemble d'adresses IP du client :

```
hostname(config)# ip local pool clientpool 192.168.0.10-192.168.0.100
hostname(config)# object network vpn_nat
```

```
hostname(config-network-object)# subnet 192.168.0.0 255.255.255.0
hostname(config-network-object)# nat (outside,outside) interface
```

Lorsque l'ASA renvoie le trafic VPN chiffré à partir de cette même interface, la NAT est facultative. L'épinglage de VPN à VPN fonctionne avec ou sans NAT. Pour appliquer la NAT à tout le trafic sortant, mettez en œuvre uniquement les commandes ci-dessus. Pour exempter le trafic de VPN à VPN de la NAT, ajoutez des commandes (à l'exemple ci-dessus) qui mettent en œuvre l'exemption de NAT pour le trafic de VPN à VPN, comme par exemple :

```
hostname(config)# nat (outside,outside) source static vpn_nat vpn_nat destination static
vpn_nat vpn_nat
```

Pour en savoir plus sur les règles de NAT, consultez le chapitre « Application de la NAT » de ce guide.

Définition du nombre maximal de sessions VPN IPsec ou SSL actives

Pour limiter les sessions VPN à une valeur inférieure à celle autorisée par l'ASA, saisissez la commande **vpn-sessiondb** en mode de configuration globale :

vpn-sessiondbmax-anyconnect-premium-or-essentials-limit <number> | **max-other-vpn-limit** <number>

Le mot-clé **max-AnyConnect-premium-or-essentials-limit** spécifie le nombre maximal de Secure Client (services client sécurisés) sessions, de 1 au nombre maximal de sessions autorisées par la licence.



Remarque

La licence, la durée, le niveau et le nombre d'utilisateurs appropriés ne sont plus déterminés avec ces commandes. Consultez le Secure Client (services client sécurisés) guide de commande : <http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf>

Le mot-clé **max-other-vpn-limit** spécifie le nombre maximal de sessions VPN autres que les sessions Secure Client (services client sécurisés), de 1 au nombre maximal de sessions autorisées par la licence. Cela inclut le client VPN Cisco (IPsec IKEv1) et les sessions VPN LAN à LAN (IPsec).

Cette limite affecte le pourcentage de charge calculé pour l'équilibrage de charge VPN.

L'exemple suivant montre comment définir une limite maximale de session VPN AnyConnect de 450 :

```
hostname(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 450
hostname(config)#
```

Utiliser la mise à jour du client pour assurer des niveaux de révision acceptables du client IPsec



Remarque Les renseignements de cette section s'appliquent uniquement aux connexions IPsec.

La fonctionnalité de mise à jour du client permet aux administrateurs d'un emplacement central d'aviser automatiquement les utilisateurs du client VPN qu'il est temps de mettre à jour le logiciel client VPN.

Les utilisateurs distants peuvent utiliser des versions logicielles ou matérielles obsolètes du client VPN. Vous pouvez utiliser la commande **client-update** à tout moment pour activer la mise à jour des révisions client, préciser les types et les numéros de révision des clients auxquels la mise à jour s'applique, fournir une URL ou une adresse IP à partir de laquelle obtenir la mise à jour et, dans le cas des clients Windows, aviser éventuellement les utilisateurs qu'ils doivent mettre à jour la version de leur client VPN. Pour les clients Windows, vous pouvez fournir un mécanisme permettant aux utilisateurs d'effectuer cette mise à jour. Cette commande s'applique uniquement au type de groupe de tunnels d'accès à distance IPsec.

Pour effectuer une mise à jour de client, saisissez la commande **client-update** en mode de configuration générale ou en mode de configuration tunnel-group ipsec-attributes. Si le client exécute déjà une version de logiciel dans la liste des numéros de révision, il n'a pas besoin de mettre à jour son logiciel. Si le client n'exécute pas de version logicielle dans la liste, il doit être mis à jour. La procédure suivante explique comment effectuer une mise à jour du client :

Procédure

Étape 1 En mode de configuration globale, activez la mise à jour du client en saisissant cette commande :

```
hostname(config)# client-update enable
hostname(config)#
```

Étape 2 En mode de configuration globale, précisez les paramètres de mise à jour client que vous souhaitez appliquer à tous les clients d'un type particulier. C'est-à-dire préciser le type de client, l'URL ou l'adresse IP à partir desquels obtenir l'image mise à jour, ainsi que le ou les numéros de révision acceptables pour ce client. Vous pouvez spécifier jusqu'à quatre numéros de révision, séparés par des virgules.

Si le numéro de révision du client correspond à l'un des numéros de révision spécifiés, il n'est pas nécessaire de mettre à jour le client. Cette commande spécifie les valeurs de mise à jour de clients pour tous les clients du type spécifié dans l'ensemble de l'ASA.

Utilisez cette syntaxe :

```
hostname(config)# client-update type type url url-string rev-nums rev-numbers
hostname(config)#
```

Les types de clients disponibles sont **win9X** (comprend les plateformes Windows 95, Windows 98 et Windows ME), **winnt** (comprend les plateformes Windows NT 4.0, Windows 2000 et Windows XP), **windows** (comprend toutes les plateformes basées sur Windows).

Si le client exécute déjà une version de logiciel dans la liste des numéros de révision, il n'a pas besoin de mettre à jour son logiciel. Si le client n'exécute pas de version logicielle dans la liste, il doit être mis à jour. Vous pouvez spécifier jusqu'à trois de ces entrées de mise à jour client. Le mot-clé **windows** couvre toutes les plateformes Windows autorisées. Si vous spécifiez **windows**, ne spécifiez pas les types de clients Windows individuels.

Remarque

Pour tous les clients Windows, vous devez utiliser le protocole `http://` ou `https://` comme préfixe de l'URL.

L'exemple suivant configure les paramètres de mise à jour de client pour le groupe de tunnels d'accès à distance. Il désigne le numéro de révision 4.6.1 et l'URL permettant de récupérer la mise à jour, soit `https://support/updates`.

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums 4.6.1
hostname(config)#
```

Vous pouvez également configurer la mise à jour client uniquement pour des groupes de tunnels individuels, plutôt que pour tous les clients d'un type particulier. (Consultez l'étape 3.)

Remarque

Vous pouvez faire en sorte que le navigateur lance automatiquement une application en ajoutant le nom de l'application à la fin de l'URL ; par exemple : `https://support/updates/vpnclient.exe`.

Étape 3

Définissez un ensemble de paramètres de mise à jour client pour un groupe de tunnels ipsec-ra particulier.

En mode tunnel-group ipsec-attributes, précisez le nom et le type de groupe de tunnels, l'URL ou l'adresse IP à partir desquels obtenir l'image mise à jour, ainsi qu'un numéro de révision. Si le numéro de révision du client de l'utilisateur correspond à l'un des numéros de révision précisés, il n'est pas nécessaire de mettre à jour le client ; par exemple, pour un client Windows, saisissez cette commande :

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type windows url https://support/updates/
rev-nums 4.6.1
hostname(config-tunnel-ipsec)#
```

Étape 4

(Facultatif) Envoyez un avis aux utilisateurs actifs dont les clients Windows sont obsolètes pour les informer que leur client doit être mis à jour. Pour ces utilisateurs, une fenêtre contextuelle s'affiche et leur offre la possibilité de lancer un navigateur et de télécharger le logiciel mis à jour à partir du site précisé dans l'URL. La seule partie de ce message que vous pouvez configurer est l'URL. (Consultez l'étape 2 ou 3.) Les utilisateurs qui ne sont pas actifs reçoivent un message de notification lors de leur prochaine connexion. Vous pouvez envoyer cet avis à tous les clients actifs de tous les groupes de tunnels, ou aux clients d'un groupe de tunnels particulier. Par exemple, pour aviser tous les clients actifs de tous les groupes de tunnels, saisissez la commande suivante en mode EXEC privilégié :

```
hostname# client-update all
hostname#
```

Si le numéro de révision du client de l'utilisateur correspond à l'un des numéros de révision spécifiés, il n'est pas nécessaire de mettre à jour le client, et aucun message de notification n'est envoyé à l'utilisateur.

Prochaine étape



Remarque

Si vous spécifiez le type de mise à jour client comme **windows** (spécifiant toutes les plateformes basées sur Windows) et que vous souhaitez ultérieurement saisir un type de mise à jour client **win9x** ou **winnt** pour la même entité, vous devez d'abord supprimer le type de client Windows avec le **no** de la commande, puis utilisez les nouvelles commandes client-update pour préciser les nouveaux types de clients.

Mettre en œuvre une connexion entre une adresse IP attribuée par NAT et une adresse IP publique

Dans de rares cas, vous pouvez vouloir 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 vouloir retraduire l'adresse IP locale en adresse IP publique réelle de l'homologue si, par exemple, vos serveurs internes et la sécurité du réseau reposent sur l'adresse IP réelle de l'homologue.

L'ASA a introduit un moyen de traduire l'adresse IP attribuée au client VPN sur le réseau interne/protégé en son adresse IP publique (source). Cette fonctionnalité prend en charge le scénario dans lequel les serveurs et services cibles sur le réseau interne ainsi que la politique de sécurité réseau exigent une communication avec l'adresse IP publique/source du client VPN plutôt qu'avec l'adresse IP attribuée sur le réseau interne de l'entreprise.

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 lorsqu'elle est déconnectée.

En raison de problèmes de routage, nous ne recommandons pas d'utiliser cette fonctionnalité, sauf si vous savez que vous en avez besoin.

- Prend uniquement en charge l'ancien protocole (IKEv1) et Secure Client (services client sécurisés).
- Le trafic de retour vers les adresses IP publiques doit être réacheminé vers l'ASA afin que la politique NAT et la politique VPN puissent être appliquées.
- Prend uniquement en charge les adresses IPv4 attribuées et publiques.
- Plusieurs homologues derrière un périphérique NAT/PAT ne sont pas pris en charge.
- Ne prend pas en charge l'équilibrage de charge (en raison d'un problème de routage).
- Ne prend pas en charge l'itinérance.

Procédure

Étape 1 En mode de configuration globale, saisissez **tunnel general (tunnel général)**.

Étape 2 Utilisez cette syntaxe pour activer la traduction d'adresse :

```
hostname(config-tunnel-general)# nat-assigned-to-public-ip interface
```

Cette commande installe dynamiquement des politiques NAT pour traduire l'adresse IP attribuée en adresse IP publique de la source. L'*interface* détermine où appliquer la NAT.

Étape 3 Utilisez cette syntaxe pour désactiver la traduction d'adresse :

```
hostname(config-tunnel-general)# no nat-assigned-to-public-ip
```

Affichage des politiques de NAT du VPN

La traduction d'adresses utilise les mécanismes NAT de l'objet sous-jacent ; par conséquent, la politique de NAT VPN s'affiche tout comme les politiques de NAT d'objets configurées manuellement. Cet exemple utilise 95.1.226.4 comme adresse IP attribuée et 75.1.224.21 comme adresse IP publique de l'homologue :

```
hostname# show nat
Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_95.1.226.4 75.1.224.21
   translate_hits = 315, untranslate_hits = 315

prompt# show nat detail

Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_95.1.226.4 75.1.224.21
   translate_hits = 315, untranslate_hits = 315
   Source - Origin: 95.1.226.4/32, Translated: 75.1.224.21/32
```

Outside est l'interface à laquelle le Secure Client (services client sécurisés) se connecte et *inside* est l'interface spécifique au nouveau groupe de tunnels.



Remarque

Comme les politiques de NAT VPN sont dynamiques et non ajoutées à la configuration, les commandes **show run object** et **show run nat** sont masquées dans l'objet d'exécution d'affichage et les rapports d'exécution de NAT.

Configurer les limites de session VPN

Vous pouvez exécuter autant de sessions IPsec et SSL que votre plateforme et votre licence ASA en prennent en charge. Pour afficher les renseignements sur la licence, y compris le nombre maximal de sessions pour votre ASA, saisissez la commande **show version** en mode de configuration globale et recherchez la section des licences. L'exemple suivant montre la commande et les renseignements de licence tirés de sa sortie ; le reste de la sortie est expurgé pour plus de clarté.

```
hostname(config)# show version
...
Licensed features for this platform:
Maximum Physical Interfaces      : Unlimited      perpetual
Maximum VLANs                   : 500           perpetual
Inside Hosts                     : Unlimited      perpetual
Failover                        : Active/Active  perpetual
Encryption-DES                  : Enabled       perpetual
```

```

Encryption-3DES-AES      : Enabled      perpetual
Security Contexts       : 100           perpetual
Carrier                  : Enabled      perpetual
AnyConnect Premium Peers : 5000      perpetual
AnyConnect Essentials    : 5000      perpetual
Other VPN Peers          : 5000      perpetual
Total VPN Peers          : 5000      perpetual
AnyConnect for Mobile    : Enabled      perpetual
AnyConnect for Cisco VPN Phone : Enabled  perpetual
Advanced Endpoint Assessment : Enabled  perpetual
Shared License           : Disabled     perpetual
Total TLS Proxy Sessions : 3000      perpetual
Botnet Traffic Filter    : Disabled     perpetual
IPS Module                : Disabled     perpetual
Cluster                  : Enabled      perpetual
Cluster Members          : 2            perpetual

```

This platform has an ASA5555 VPN Premium license.

Afficher l'allocation des ressources de licence

Utilisez la commande suivante pour afficher l'allocation des ressources :

```

asa2(config)# sh resource allocation
Resource      Total      % of Avail
Conns[rate]   100 (U)    0.00%
Inspects[rate] unlimited
Syslogs[rate] unlimited
Conns         unlimited
Hosts         unlimited
IPsec         unlimited
Mac-addresses unlimited
ASDM          10         5.00%
SSH           10         10.00%
Telnet        10         10.0%
Xlates        unlimited
AnyConnect    1000       10%
AnyConnectBurst 200        2%
OtherVPN      2000       20%
OtherVPNBurst 1000       10%

```

Afficher l'utilisation des ressources de licence

Utilisez la commande suivante pour afficher l'utilisation des ressources :



Remarque

Vous pouvez également utiliser la commande **sh resource usage system controller all 0** pour afficher l'utilisation au niveau du système avec la limite comme limite de la plateforme.

```

ASA(config-ca-trustpoint)# sh resource usage
Resource      Current  Peak  Limit  Denied  Context
Conns         1        16    280000 0        System
Hosts         2        10    N/A    0        System
AnyConnect    2        25    1000   0        cust1
AnyConnectBurst 0        0     200   0        cust1
OtherVPN      1        1     2000   0        cust2
OtherVPNBurst 0        0     1000   0        cust2

```

Limiter les sessions VPN

Pour limiter les sessions VPN AnyConnect (IPsec/IKEv2 ou SSL) à une valeur inférieure à celle autorisée par l'ASA, utilisez la commande **vpn-sessiondb max-anyconnect-premium-or-essentials-limit** en mode de configuration globale. Pour supprimer la limite de session, utilisez la version **no** de cette commande.

Si la licence ASA autorise 500 sessions VPN SSL et que vous souhaitez limiter le nombre de sessions VPN AnyConnect à 250, saisissez la commande suivante :

```
hostname(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 250
hostname(config)#
```

Pour supprimer la limite de session, utilisez la version **no** de cette commande :

```
hostname(config)# no vpn-sessiondb max-anyconnect-premium-or-essentials-limit 250
hostname(config)#
```

Utilisation d'un certificat d'identité lors de la négociation

L'ASA doit utiliser un certificat d'identité lors de la négociation du tunnel IKEv2 avec Secure Client (services client sécurisés). Pour la configuration du point de confiance d'accès à distance IKEv2, utilisez les commandes suivantes

```
crypto ikev2 remote-access trustpoint <name> [line<number>]
```

L'utilisation de cette commande permet à Secure Client (services client sécurisés) de prendre en charge la sélection de groupe pour l'utilisateur final. Vous pouvez configurer deux points de confiance en même temps : deux RSA, deux ECDSA ou un de chaque. L'ASA analyse la liste des points de confiance configurés et choisit le premier pris en charge par le client. Si ECDSA est préféré, vous devez configurer ce point de confiance avant le point de confiance RSA.

L'option de numéro de ligne spécifie l'endroit dans la ligne où vous souhaitez insérer le point de confiance. En règle générale, cette option est utilisée pour insérer un point de confiance en haut sans supprimer et rajouter l'autre ligne. Si une ligne n'est pas spécifiée, l'ASA ajoute le point de confiance à la fin de la liste.

Si vous essayez d'ajouter un point de confiance qui existe déjà, vous recevez une erreur. Si vous utilisez la commande **no crypto ikev2 remote-access trustpoint** sans préciser le nom de point de confiance à supprimer, toute la configuration de point de confiance est supprimée.

Configurer le pool de cœurs de chiffrement

Vous pouvez modifier l'allocation des cœurs de chiffrement sur les plateformes de traitement multiprocesseur symétrique (SMP) afin d'augmenter le débit du trafic TLS/DTLS de Secure Client (services client sécurisés). Ces modifications peuvent accélérer le chemin de données du VPN SSL et offrir des gains de performance visibles par la clientèle dans Secure Client (services client sécurisés), les tunnels intelligents et le transfert de ports. Ces étapes décrivent la configuration de l'ensemble de cœurs de chiffrement en mode contexte unique ou multiple.

Procédure

Spécifiez comment allouer les processeurs accélérateurs de chiffrement :

crypto engine accelerator-bias

- **équilibré** : distribue également les ressources matérielles de chiffrement (cœurs Admin/SSL et IPsec).
- **ipsec** : alloue les ressources matérielles de chiffrement en vue d'IPsec (y compris le trafic vocal chiffré SRTP).
- **ssl** : alloue les ressources matérielles de chiffrement en faveur d'Admin/SSL. Utilisez ce biais lorsque vous prenez en charge les sessions VPN d'accès à distance Secure Client (services client sécurisés) basées sur SSL.

Exemple :

```
hostname(config)# crypto engine accelerator-bias ssl
```

Configurer la tunnellation fractionnée dynamique

Avec la tunnellation fractionnée dynamique, vous pouvez provisionner dynamiquement des exclusions de tunnellation fractionnée après l'établissement du tunnel, en fonction du nom de domaine DNS de l'hôte. La tunnellation dynamique fractionnée est configurée en créant un attribut personnalisé et en l'ajoutant à une politique de groupe.

Avant de commencer

Pour utiliser cette fonctionnalité, vous devez avoir AnyConnect version 4.5 (ou ultérieure). Consultez [À propos de la tunnellation fractionnée dynamique](#) pour obtenir plus d'explications.

Procédure

- Étape 1** Définissez le type d'attribut personnalisé dans le contexte WebVPN à l'aide de la commande suivante :
- ```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains
```
- Étape 2** Définissez les noms d'attribut personnalisés pour chaque service en nuage ou Web qui doit être accessible par le client en dehors du tunnel VPN. Par exemple, ajoutez Google\_domains pour représenter une liste de noms de domaine DNS relatifs aux services Web de Google. La valeur de l'attribut contient la liste des noms de domaine à exclure du tunnel VPN et doit être au format CSV (valeurs séparées par des virgules), comme suit :

```
anyconnect-custom-data dynamic-split-exclude-domains webex.com, webexconnect.com, tags.tiqcdn.com
```

**Étape 3**

Associez l'attribut personnalisé défini précédemment à une stratégie de groupe à l'aide de la commande suivante, exécutée dans le contexte des attributs de stratégie de groupe : `anyconnect-custom`

```
dynamic-split-exclude-domains value webex_service_domains
```

**Prochaine étape**

Si la tunnellation d'inclusion fractionnée est configurée, une exclusion de fractionnement dynamique est appliquée uniquement si au moins une des adresses IP de réponse DNS fait partie du réseau d'inclusion fractionnée. S'il n'y a aucun chevauchement entre les adresses IP des réponses DNS et les réseaux de la liste d'inclusion fractionnée, il n'est pas nécessaire d'appliquer l'exclusion dynamique, car le trafic correspondant à toutes les adresses IP renvoyées par DNS est déjà exclu de la tunnellation.

## Configuration du tunnel VPN de gestion

Un tunnel VPN de gestion assure la connectivité au réseau d'entreprise chaque fois que le système client est sous tension, pas seulement lorsqu'une connexion VPN est établie par l'utilisateur final. Vous pouvez effectuer la gestion des correctifs sur les terminaux hors du bureau, notamment les périphériques rarement connectés par l'utilisateur, via VPN, au réseau d'entreprise. Les scripts de connexion du système d'exploitation des terminaux qui nécessitent une connectivité au réseau d'entreprise en bénéficieront également.

Le tunnel VPN de gestion est censé être transparent pour l'utilisateur final ; par conséquent, le trafic réseau initié par les applications des utilisateurs n'est pas touché par défaut, mais est plutôt acheminé à l'extérieur du tunnel VPN de gestion.

Si un utilisateur se plaint de connexions lentes, cela peut indiquer que le tunnel de gestion n'a pas été configuré correctement. Consultez le [Guide d'administration de Cisco Secure Client](#) pour connaître les exigences supplémentaires, les incompatibilités, les limites et le dépannage du tunnel VPN de gestion.

**Avant de commencer**

Nécessite AnyConnect version 4.7 (ou ultérieure)

**Procédure****Étape 1**

Ajoutez le profil téléchargé (`profileMgmt`) à la stratégie de groupe (`MgmtTunGrpPolicy`) mappée au groupe de tunnels utilisé par la connexion du tunnel de gestion :

Pour indiquer que le profil est le profil VPN de gestion AnyConnect, incluez **type vpn-mgmt** dans la commande **anyconnect profiles**. Un profil VPN AnyConnect normal est de type utilisateur.

```
group-policy MgmtTunGrpPolicy attributes
 webvpn
 anyconnect profiles value profileMgmt type vpn-mgmt
```

**Étape 2**

Pour déployer le profil VPN de gestion par le biais de la connexion du tunnel de l'utilisateur, ajoutez le profil chargé (`profileMgmt`) à la stratégie de groupe (`DfltGrpPolicy`) mappée au groupe de tunnels utilisé par la connexion du tunnel de l'utilisateur :

```
group-policy DfltGrpPolicy attributes
```

```
webvpn
 anyconnect profiles value profileMgmt type vpn-mgmt
```

## Affichage des sessions VPN actives

Les rubriques suivantes expliquent comment afficher les informations de session VPN.

### Affichage des sessions actives Secure Client (services client sécurisés) par type d'adresse IP

Pour afficher les sessions Secure Client (services client sécurisés) actives à l'aide de l'interface de ligne de commande, saisissez la commande **show vpn-sessiondb anyconnect filter p-ipversion** ou **show vpn-sessiondb anyconnect filter a-ipversion** en mode d'exécution privilégié.

- Affichez les sessions actives Secure Client (services client sécurisés) qui sont filtrées en fonction de l'adresse publique IPv4 ou IPv6 du terminal. L'adresse publique est l'adresse attribuée au terminal par l'entreprise.

```
show vpn-sessiondb anyconnect filter p-ipversion {v4 | v6}
```

- Affichez les sessions actives Secure Client (services client sécurisés) qui sont filtrées en fonction de l'adresse IPv4 ou IPv6 attribuée au terminal. L'adresse attribuée est l'adresse attribuée au Secure Client (services client sécurisés) par l'ASA.

```
show vpn-sessiondb anyconnect filter a-ipversion {v4 | v6}
```

#### Exemple de sortie de la commande **show vpn-sessiondb anyconnect filter p-ipversion [v4 | v6]**

```
hostname(config)# show vpn-sessiondb anyconnect filter p-ipversion v4
```

```
Session Type: AnyConnect
```

```
Username : user1 Index : 40
Assigned IP : 192.168.17.10 Public IP : 198.51.100.1
Protocol : AnyConnect-Parent SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1
Bytes Tx : 10570 Bytes Rx : 8085
Group Policy : GroupPolicy_SSLACCLIENT
Tunnel Group : SSLACCLIENT
Login Time : 15:17:12 UTC Mon Oct 22 2012
Duration : 0h:00m:09s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

**Sortie de la commande `show vpn-sessiondb anyconnect filter a-ipversion [v4 | v6]`**

```
hostname(config)# show vpn-sessiondb anyconnect filter a-ipversion v6

Session Type: AnyConnect

Username : user1 Index : 45
Assigned IP : 192.168.17.10
Public IP : 2001:DB8:8:1:90eb:3fe5:9eea:fb29
Assigned IPv6 : 2001:DB8:9:1::24
Protocol : AnyConnect-Parent SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1
Bytes Tx : 10662 Bytes Rx : 17248
Group Policy : GroupPolicy_SSL_IPv6 Tunnel Group : SSL_IPv6
Login Time : 17:42:42 UTC Mon Oct 22 2012
Duration : 0h:00m:33s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

**Affichage des sessions VPN de site à site actives par type d'adresse IP**

Pour afficher les sessions VPN de site à site actives à l'aide de l'interface de ligne de commande, saisissez la commande **`show vpn-sessiondb l2l filter ipversion`** en mode d'exécution privilégié.

Cette commande affiche les sessions VPN de site à site actives filtrées en fonction de l'adresse publique IPv4 ou IPv6 de la connexion.

L'adresse publique est l'adresse attribuée au terminal par l'entreprise.

```
show vpn-sessiondb l2l filter ipversion {v4 | v6}
```

**À propos de l'application des politiques ISE :**

Cisco Identity Services Engine (ISE) est une plateforme de gestion et de contrôle des politiques de sécurité. Il automatise et simplifie le contrôle d'accès et la conformité de sécurité pour la connectivité filaire, sans fil et VPN. Cisco ISE est principalement utilisé pour fournir un accès sécurisé et l'accès des invités, prendre en charge les projets BYOD (Bring Your Own Device) et appliquer les politiques d'utilisation en collaboration avec Cisco TrustSec.

La fonctionnalité Change of Authorization (CoA) d'ISE fournit un mécanisme permettant de modifier les attributs d'une session d'authentification, d'autorisation et de comptabilité (AAA) après son établissement. Lorsqu'une politique est modifiée pour un utilisateur ou un groupe d'utilisateurs dans AAA, des paquets CoA peuvent être envoyés directement à l'ASA depuis l'ISE pour réinitialiser l'authentification et appliquer la nouvelle politique. Un point d'application de posture en ligne (IPEP) n'est pas nécessaire pour appliquer les listes de contrôle d'accès (ACL) à chaque session VPN établie avec l'ASA.

L'application des politiques ISE est prise en charge sur les clients VPN suivants :

- IPSec
- Secure Client (services client sécurisés)
- L2TP/IPSec

**Remarque**

Certains éléments de politique tels que l'ACL dynamique (dACL) et la balise de groupe de sécurité (SGT) sont pris en charge, alors que les éléments de politique tels que l'affectation de VLAN et l'affectation d'adresses IP ne sont pas pris en charge.

Le flux du système est le suivant :

1. Un utilisateur final demande une connexion VPN.
2. L'ASA authentifie l'utilisateur auprès de l'ISE et reçoit une liste de contrôle d'accès d'utilisateur qui fournit un accès limité au réseau.
3. Un message de début de comptabilité est envoyé à l'ISE pour enregistrer la session.
4. L'évaluation de la posture se produit directement entre l'agent NAC et l'ISE. Ce processus est transparent pour l'ASA.
5. L'ISE envoie une mise à jour de politique à l'ASA au moyen d'un « policy push » CoA. Cela identifie une nouvelle ACL utilisateur qui fournit des privilèges d'accès réseau accrus.

**Remarque**

Des évaluations de politiques supplémentaires peuvent se produire pendant la durée de vie de la connexion, de manière transparente pour l'ASA, par le biais des mises à jour ultérieures de CoA.

Ce modèle de flux diffère de la plupart des scénarios qui utilisent RADIUS CoA. Pour les authentifications 802.1x filaires ou sans fil, RADIUS CoA n'inclut aucun attribut. Il déclenche uniquement la deuxième authentification dans laquelle tous les attributs, tels que DACL, sont associés. Pour la posture VPN ASA, il n'y a pas de deuxième authentification. Tous les attributs sont retournés dans le RADIUS CoA. La session VPN est active et il est impossible de modifier la plupart des paramètres utilisateur VPN. Les seuls paramètres qui peuvent être modifiés par une activation CoA sont RedirectURL, RedirectACL et la balise de groupe de sécurité (SGT).

## Configurer les groupes de serveurs RADIUS pour l'application des politiques ISE

Pour permettre l'évaluation et l'application des politiques ISE, configurez un groupe de serveurs RADIUS AAA pour les serveurs ISE et ajoutez les serveurs au groupe. Lorsque vous configurez le groupe de tunnels pour le VPN, vous spécifiez ce groupe de serveurs pour les services AAA dans le groupe.

### Procédure

#### Étape 1

Créez le groupe de serveurs AAA RADIUS.

**aaa-server group\_name protocol radius**

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)#
```

**Étape 2** Activez les services d'autorisation dynamique RADIUS (CoA) pour le groupe de serveurs AAA.

**dynamic-authorization** [**port number**]

La définition d'un port est facultative. La valeur par défaut est 1700, la plage est comprise entre 1024 et 65535.

Lorsque vous utilisez le groupe de serveurs dans un tunnel VPN, le groupe de serveurs RADIUS sera enregistré pour la notification CoA et l'ASA écoutera le port pour détecter les mises à jour de politique CoA d'ISE.

```
hostname (config-aaa-server-group) # dynamic-authorization
```

**Étape 3** Si vous ne souhaitez pas utiliser ISE pour l'authentification, activez le mode d'autorisation seulement pour le groupe de serveurs RADIUS.

**authorize-only**

Cela indique que lorsque ce groupe de serveurs est utilisé pour l'autorisation, le message de demande d'accès RADIUS sera généré en tant que demande « Autorize Only » (Autorisation uniquement), par opposition aux méthodes de mot de passe configurées pour le serveur AAA. Si vous configurez un mot de passe commun à l'aide de la commande **radius-common-pw** pour le serveur RADIUS, il sera ignoré.

Par exemple, vous utiliserez le mode d'autorisation seulement si vous souhaitez utiliser des certificats pour l'authentification plutôt que ce groupe de serveurs. Vous utiliserez toujours ce groupe de serveurs pour l'autorisation et la gestion de comptes dans le tunnel VPN.

```
hostname (config-aaa-server-group) # authorize-only
```

**Étape 4** Activez la génération périodique de messages RADIUS interim-accounting-update.

**interim-accounting-update** [**periodic** [**hours**]]

ISE gère un répertoire des sessions actives en fonction des enregistrements de traçabilité qu'il reçoit des périphériques NAS comme l'ASA. Cependant, si ISE ne reçoit aucune indication que la session est toujours active (message de traçabilité ou transactions de posture) pendant une période de 5 jours, il supprimera l'enregistrement de session de sa base de données. Pour vous assurer que les connexions VPN de longue durée ne sont pas supprimées, configurez le groupe pour envoyer des messages interim-accounting-update périodiques à ISE pour toutes les sessions actives.

- **periodic** [**hours**] permet la génération et la transmission périodiques des enregistrements de comptabilité pour chaque session VPN configurée pour envoyer des enregistrements de comptabilité au groupe de serveurs en question. Vous pouvez éventuellement inclure l'intervalle, en heures, pour l'envoi de ces mises à jour. La valeur par défaut est de 24 heures, la plage est comprise entre 1 et 120.
- (Aucun paramètre.) Si vous utilisez cette commande sans le mot clé **periodic**, l'ASA envoie des messages interim-accounting-update uniquement lorsqu'une connexion de tunnel VPN est ajoutée à une session VPN sans client. Lorsque cela se produit, la mise à jour de comptabilité est générée afin d'informer le serveur RADIUS de la nouvelle adresse IP attribuée.

```
hostname (config-aaa-server-group) # interim-accounting-update periodic 12
```

**Étape 5** (Facultatif) Fusionnez une ACL téléchargeable avec l'ACL reçue dans la paire AV de Cisco à partir d'un paquet RADIUS.

**merge-dacl** {**before-avpair** | **after-avpair**}

Cette option s'applique uniquement aux connexions VPN. Pour les utilisateurs de VPN, les ACL peuvent prendre la forme d'ACL de paire attribut/valeur de Cisco, d'ACL téléchargeables et d'une ACL configurée sur l'ASA. Cette option détermine si l'ACL téléchargeable et l'ACL de la paire attribut/valeur sont fusionnées, et ne s'applique à aucune ACL configurée sur l'ASA.

Le paramètre par défaut est **no merge dacl**, ce qui indique que les ACL téléchargeables ne seront pas fusionnées avec les ACL de paire attribut/valeur de Cisco. Si une paire AV et une ACL téléchargeable sont reçues, la paire AV a la priorité et est utilisée.

L'option **before-avpair** signifie que les entrées d'ACL téléchargeables doivent être placées avant les entrées de la paire d'AV de Cisco.

L'option **after-avpair** signifie que les entrées d'ACL téléchargeables doivent être placées après les entrées de la paire d'AV de Cisco.

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)# merge-dacl before-avpair
```

## Étape 6

(Facultatif) Précisez le nombre maximum de demandes envoyées à un serveur RADIUS du groupe avant d'essayer le serveur suivant.

**max-failed-attempts** *nombre*

La plage se situe entre 1 et 5. La valeur par défaut est de 3.

Si vous avez configuré une méthode de secours à l'aide de la base de données locale (pour l'accès de gestion uniquement), et que tous les serveurs du groupe ne répondent pas, le groupe est considéré comme ne répondant pas et la méthode de secours est essayée. Le groupe de serveurs reste marqué comme ne répondant pas pendant une période de 10 minutes (par défaut), de sorte que les demandes AAA supplémentaires effectuées dans cette période ne résultent pas en une tentative d'entrer en contact avec le groupe de serveurs et que la méthode de secours est utilisée immédiatement. Pour modifier la période de non-réponse par défaut, consultez la commande **reactivation-mode** à l'étape suivante.

Si vous n'avez pas de méthode de secours, l'ASA continue de réessayer les serveurs du groupe.

```
hostname(config-aaa-server-group)# max-failed-attempts 2
```

## Étape 7

(Facultatif) Précisez la méthode (politique de réactivation) par laquelle les serveurs défaillants d'un groupe sont réactivés.

**reactivation-mode** {**depletion** [**deadtime** *minutes*] | **timed**}

Lieu :

- **depletion** [**deadtime** *minutes*] réactive les serveurs défaillants seulement après que tous les serveurs du groupe sont inactifs. Il s'agit du mode de réactivation par défaut. Vous pouvez préciser la durée, entre 0 et 1 440 minutes, qui s'écoule entre la désactivation du dernier serveur du groupe et la réactivation ultérieure de tous les serveurs. La valeur par défaut est 10 minutes.
- **timed** réactive les serveurs défaillants après 30 secondes de temps d'arrêt.

```
hostname(config-aaa-server-group)# reactivation-mode deadtime 20
```

## Étape 8

(Facultatif) Envoyez des messages de traçabilité à tous les serveurs du groupe.

**accounting-mode simultaneous**

Pour rétablir la valeur par défaut d'envoi de messages uniquement au serveur actif, saisissez la commande **accounting-mode single**.

```
hostname(config-aaa-server-group)# accounting-mode simultaneous
```

**Étape 9**

Ajoutez les serveurs ISE RADIUS au groupe.

```
aaa-server group_name [(interface_name)] host {server_ip | name} [key]
```

Lieu :

- *group\_name* est le nom du groupe de serveurs RADIUS.
- *(interface\_name)* est le nom de l'interface par laquelle le serveur est accessible. La valeur par défaut est (inside). Les parenthèses sont obligatoires.
- **host** {server\_ip | name} est l'adresse IP ou le nom d'hôte du serveur ISE RADIUS.
- *key* est la clé facultative pour chiffrer la connexion. Vous pouvez plus facilement saisir cette clé dans la commande **key** après être passé en mode **aaa-server-host**. Si vous ne configurez pas de clé, la connexion n'est pas chiffrée (texte en clair). La clé est une chaîne alphanumérique sensible à la casse pouvant comporter jusqu'à 127 caractères, ce qui correspond à la même valeur que la clé sur le serveur RADIUS.

Vous pouvez ajouter plusieurs serveurs au groupe.

```
hostname(config)# aaa-server servergroup1 (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key sharedsecret
hostname(config-aaa-server-host)# exit
```

## Exemples de configuration pour l'application de la politique ISE

### Configurer le tunnel VPN pour l'authentification dynamique ISE avec des mots de passe

L'exemple suivant montre comment configurer un groupe de serveurs ISE pour les mises à jour d'autorisation dynamique (CoA) et la comptabilité périodique horaire. La configuration du groupe de tunnels qui configure l'authentification par mot de passe avec ISE est incluse.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```



### Configurer le tunnel VPN pour l'autorisation ISE uniquement

L'exemple suivant montre comment configurer un groupe de tunnels pour la validation et l'autorisation des certificats locaux avec ISE. Incluez la commande `authorize-only` dans la configuration du groupe de serveurs, car le groupe de serveurs ne sera pas utilisé pour l'authentification.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

## Dépannage de l'application des politiques

Les commandes suivantes peuvent être utilisées pour le débogage.

Pour suivre l'activité CoA :

```
debug radius dynamic-authorization
```

Pour suivre la fonctionnalité d'URL de redirection :

```
debug aaa url-redirect
```

Pour afficher les règles de classification NP correspondant à la fonctionnalité de redirection d'URL :

```
show asp table classify domain url-redirect
```

## Configurer les paramètres avancés SSL

L'ASA utilise le protocole SSL (Secure Sockets Layer) et le protocole TLS (Transport Layer Security) pour prendre en charge la transmission sécurisée des messages pour ASDM, Clientless SSL VPN, VPN et les sessions basées sur le navigateur. L'ASA prend en charge les protocoles SSLv3, TLSv1, TLSv1.1, TLSv1.2, et TLSv1.3 pour les connexions VPN et de gestion basées sur SSL. En outre, DTLS est utilisé pour les connexions du client VPN AnyConnect

Les suites de chiffrement suivantes sont prises en charge, comme indiqué :

| Chiffre                      | TLSv1.1 / DTLS V1 | TLSv1.2 / DTLSV 1.2 | TLSv1.3 |
|------------------------------|-------------------|---------------------|---------|
| TLS_AES_128_GCM_SHA256       | Non               | Non                 | Oui     |
| TLS_CHACHA20_POLY1305_SHA256 | Non               | Non                 | Oui     |

| Chiffre                       | TLSv1.1 / DTLS V1 | TLSv1.2 / DTLSV 1.2 | TLSv1.3 |
|-------------------------------|-------------------|---------------------|---------|
| TLS_AES_256_GCM_SHA384        | Non               | Non                 | Oui     |
| AES128-GCM-SHA256             | Non               | Oui                 | Non     |
| AES128-SHA                    | Oui               | oui                 | Non     |
| AES128-SHA256                 | Non               | Oui                 | Non     |
| AES256-GCM-SHA384             | Non               | Oui                 | Non     |
| AES256-SHA                    | Oui               | oui                 | Non     |
| AES256-SHA256                 | Non               | Oui                 | Non     |
| DESR-CBC-SHA                  | Non               | Non                 | Non     |
| DES-CBC-SHA                   | Oui               | oui                 | Non     |
| DHE-RSA-AES128-GCM-SHA256     | Non               | Oui                 | Non     |
| DHE-RSA-AES128-SHA            | Oui               | oui                 | Non     |
| DHE-RSA-AES128-SHA256         | Non               | Oui                 | Non     |
| DHE-RSA-AES256-GCM-SHA384     | Non               | l                   | Non     |
| DHE-RSA-AES256-SHA            | Oui               | oui                 | Non     |
| ECDHE-ECDSA-AES128-GCM-SHA256 | Non               | Oui                 | Non     |
| ECDHE-ECDSA-AES128-SHA256     | Non               | Oui                 | Non     |
| ECDHE-ECDSA-AES256-GCM-SHA384 | Non               | Oui                 | Non     |
| ECDHE-ECDSA-AES256-SHA384     | Non               | Oui                 | Non     |
| ECDHE-RSA-AES128-GCM-SHA256   | Oui               | oui                 | Non     |
| ECDHE-RSA-AES128-SHA256       | Non               | Oui                 | Non     |
| ECDHE-RSA-AES256-GCM-SHA384   | Non               | Oui                 | Non     |
| ECDHE-RSA-AES256-SHA384       | Non               | Oui                 | Non     |
| NULL-SHA                      | Non               | Non                 | Non     |
| RC4-MD5                       | Non               | Non                 | Non     |
| RC4-SHA                       | Non               | Non                 | Non     |

**Remarque**

Pour la version 9.4(1), tous les mots-clés SSLv3 ont été supprimés de la configuration ASA et la prise en charge SSLv3 a été supprimée de l'ASA. Si SSLv3 est activé, une erreur de démarrage s'affichera à partir de la commande avec l'option SSLv3. L'ASA reviendra ensuite à l'utilisation par défaut de TLSv1.

Le récepteur mobile Citrix peut ne pas prendre en charge les protocoles TLS 1.1/1.2 ; consultez [https://www.citrix.com/content/dam/citrix/en\\_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf](https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf) pour la compatibilité

Pour spécifier la version minimale du protocole pour laquelle l'ASA négociera les connexions SSL/TLS et DTLS, procédez comme suit :

**Procédure****Étape 1**

Définissez la version de protocole minimale pour laquelle l'ASA négociera une connexion.

**ssl server-version** [tlsv1 | tlsv1.1 | tlsv1.2 | tlsv1.3] [dtls1 | dtls1.2]

Lieu :

- **tlsv1** : saisissez ce mot-clé pour accepter les ClientHellos SSLv2 et négocier TLSv1 (ou supérieur)
- **tlsv1.1** : saisissez ce mot-clé pour accepter les ClientHellos SSLv2 et négocier TLSv1.1 (ou supérieur)
- **tlsv1.2** : saisissez ce mot-clé pour accepter les ClientHellos SSLv2 et négocier TLSv1.2 (ou supérieur)
- **tlsv1.3** : saisissez ce mot-clé pour accepter les ClientHellos SSLv2 et négocier TLSv1.3 (ou supérieur)
- **dtls1** : saisissez ce mot-clé pour accepter les ClientHellos DTLSv1 et négocier DTLSv1 (ou supérieur)
- **dtls1.2** : saisissez ce mot-clé pour accepter les messages client hello DTLSv1.2 et négocier DTLSv1.2 (ou version supérieure)

**Remarque**

La configuration et l'utilisation de DTLS s'appliquent uniquement aux connexions d'accès à distance Secure Client (services client sécurisés).

Assurez-vous que la session TLS est aussi sécurisée ou plus sécurisée que la session DTLS en utilisant une version de TLS égale ou supérieure à DTLS. Compte tenu de cela, tlsv1.2 est la seule version TLS acceptable lors du choix de dtls1.2 ; et toute version TLS peut être utilisée avec dtls1, car elles sont toutes égales ou supérieures à DTLS 1.0.

**Exemple :**

Exemples :

```
hostname(config)# ssl server-version tlsv1.1
```

```
hostname(config)# ssl server-version tlsv1.2 dtls1.2
```

**Étape 2**

Spécifiez la version maximale du protocole SSL/TLS que l'ASA utilise lorsqu'il agit comme serveur.

**ssl server-max-version** [tlsv1 | tlsv1.1 | tlsv1.2 | tlsv1.3]

Si `server-max-version` est configuré à TLSV1.2, vous ne pourrez pas configurer TLSV1.3 comme `server-version`.

### Étape 3

Spécifiez la version du protocole SSL/TLS que l'ASA utilise lorsqu'il agit comme client.

**ssl client-version** [ `tlsv1` | `tlsv1.1` | `tlsv1.2` | `tlsv1.3` ]

Lieu :

- **tlsv1** : saisissez ce mot-clé pour spécifier que l'ASA transmet les messages client hello TLSv1 et négocie TLSv1 (ou version supérieure).
- **tlsv1.1** : saisissez ce mot-clé pour spécifier que l'ASA transmet les messages client hello TLSv1.1 et négocie TLSv1.1 (ou version supérieure).
- **tlsv1.2** : saisissez ce mot-clé pour spécifier que l'ASA transmet les messages client hello TLSv1.2 et négocie TLSv1.2 (ou version supérieure).
- **tlsv1.3** : saisissez ce mot-clé pour spécifier que l'ASA transmet les messages client hello TLSv1.3 et négocie TLSv1.3 (ou version supérieure).

DTLS n'est pas disponible pour le rôle de client SSL.

#### Exemple :

Exemples :

```
hostname(config)# ssl client-version tlsv1
```

### Étape 4

Spécifiez la version maximale du protocole SSL/TLS que l'ASA utilise lorsqu'il agit comme client.

**ssl client-max-version** [ `tlsv1` | `tlsv1.1` | `tlsv1.2` | `tlsv1.3` ]

Si `client-max-version` est configuré à TLSV1.2, vous ne pourrez pas configurer TLSV1.3 comme `client-version`.

### Étape 5

Précisez les algorithmes des suites de chiffrement pour les protocoles SSL, DTLS et TLS.

**ssl cipher version** [ `level` | `custom string` ]

Lieu :

- L'argument *version* spécifie la version du protocole SSL, DTLS ou TLS. Versions prises en charge :
  - `default` : ensemble des suites de chiffrement pour les connexions sortantes.
  - `dtlsv1` : suites de chiffrement pour les connexions entrantes DTLSv1.
  - `dtlsv1.2` : suites de chiffrement pour les connexions entrantes DTLSv1.2.
  - `tlsv1` : suites de chiffrement pour les connexions entrantes TLSv1.
  - `tlsv1.1` : suites de chiffrement pour les connexions entrantes TLSv1.1.
  - `tlsv1.2` : suites de chiffrement pour les connexions entrantes TLSv1.2.
  - `tlsv1.3` : suites de chiffrement pour les connexions entrantes TLSv1.3.
- L'argument *level* précise la robustesse des suites de chiffrement et indique le niveau minimal configuré. Les valeurs valides, par ordre croissant de robustesse, sont les suivantes :
  - `all` : comprend toutes les suites de chiffrement.

- **low** : comprend toutes les suites de chiffrement, sauf NULL-SHA.
  - **medium** (il s'agit du paramètre par défaut pour toutes les versions de protocole) : comprend toutes les suites de chiffrement (sauf NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA, et DES-CBC3-SHA).
  - **fips** : comprend toutes les suites de chiffrement conformes à FIPS (sauf NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA, et DES-CBC3-SHA).
  - **high** (s'applique uniquement à TLSv1.2 et TLSv1.3) : comprend uniquement AES-256 avec chiffrements SHA-2 pour TLSv1.2. La robustesse de toutes les suites de chiffrement TLSv1.3 est élevée.
- Le fait de spécifier l'option **customstring** vous permet d'exercer un contrôle total sur la suite de chiffrement à l'aide des chaînes de définition de chiffrement OpenSSL. Pour en savoir plus, consultez <https://www.openssl.org/docs/apps/ciphers.html>.

Le paramètre recommandé est **medium**. L'utilisation de **high** peut limiter la connectivité. L'utilisation de **custom** peut limiter les fonctionnalités si seulement quelques suites de chiffrement sont configurées. Le fait de restreindre la valeur **custom** par défaut limite la connectivité sortante, y compris la mise en grappe.

L'ASA spécifie l'ordre de priorité des chiffrements pris en charge. Consultez la référence de commande pour en savoir plus.

Cette commande remplace la commande `ssl encryption`, qui est déconseillée depuis la version 9.3(2).

## Étape 6

Autorisez plusieurs points de confiance sur une seule interface.

**ssl trust-point name** [ [**interface** *vpnlb-ip* ] | [ **domain** *domain-name* ]

```
hostname(config)# ssl trust-point www-cert domain www.example.com
```

L'argument **name** spécifie le nom du point de confiance. L'argument **interface** spécifie le nom de l'interface sur laquelle un point de confiance est configuré. Le mot-clé `vpnlb-ip` s'applique uniquement aux interfaces et associe ce point de confiance à l'adresse IP du cluster d'équilibrage de charge VPN sur cette interface. La paire mot-clé-argument **domain***domain-name* spécifie un point de confiance associé à un nom de domaine particulier utilisé pour accéder à l'interface.

Vous pouvez configurer jusqu'à 16 points de confiance par interface.

Si vous ne précisez ni interface ni domaine, cette commande crée le point de confiance de secours pour toutes les interfaces qui n'ont pas de point de confiance configuré.

Si vous saisissez la commande **ssl trustpoint ?**, les points de confiance configurés disponibles s'affichent. Si vous saisissez la commande **ssl trust-point name ?** (par exemple, **ssl trust-point mysslcert ?**), les interfaces configurées disponibles pour l'association entre le point de confiance et le certificat SSL s'affichent.

Suivez ces consignes lorsque vous utilisez cette commande :

- La valeur du point de confiance doit être le nom du point de confiance de l'autorité de certification tel qu'il est configuré dans la commande **crypto ca trustpoint name**.
- La valeur de interface doit être le nom `nameif` d'une interface préalablement configurée.
- La suppression d'un point de confiance supprime également toutes les entrées **ssl trust-point** qui font référence à ce point de confiance.

- Vous pouvez avoir une entrée `ssl trust-point` pour chaque interface et une entrée qui ne spécifie aucune interface.
- Vous pouvez réutiliser le même point de confiance pour plusieurs entrées.
- Un point de confiance configuré avec le mot-clé `domain` peut s'appliquer à plusieurs interfaces (selon la façon dont vous vous connectez).
- Vous ne pouvez avoir qu'un seul **ssl trust-point** par valeur *domain-name*.
- Si l'erreur suivante s'affiche après avoir saisi cette commande :

```
error:0B080074:x509 certificate routines:X509_check_private_key:key values
mismatch@x509_cmp.c:339
```

Cela signifie qu'un utilisateur a configuré un nouveau certificat pour remplacer un certificat précédemment configuré. Vous n'avez rien à faire.

- Les certificats sont choisis dans l'ordre suivant :
  - Si une connexion correspond à la valeur du mot-clé **domain**, ce certificat est choisi en premier. (commande **ssl trust-point name domain domain-name**)
  - Si une connexion est établie à l'adresse d'équilibrage de charge, le certificat `vpn-lb-ip` est choisi. (**ssl trust-point name interface vpn-lb-ip** command)
  - Le certificat configuré pour l'interface. (**ssl trust-point name interface** command)
  - Le certificat par défaut n'est pas associé à une interface. **ssl trust-point name**
  - Le certificat autosigné et autogénéré de l'ASA.

**Étape 7** Précisez le groupe DH à utiliser avec les suites de chiffrement DHE-RSA utilisées par TLS.

```
ssl dh-group [group14 | group15]
hostname(config)# ssl dh-group group14
```

Le mot-clé `group14` et `group15` configure le groupe DH 14 (module de 2 048 bits, sous-groupe d'ordre premier de 224 bits).

Le groupe 14 n'est pas compatible avec Java 7. Tous les groupes sont compatibles avec Java 8. Le groupe 14 est conforme à la norme FIPS. La valeur par défaut est `ssl dh-group group14`.

**Étape 8** Précisez le groupe à utiliser avec les suites de chiffrement ECDHE-ECDSA utilisées par TLS.

```
ssl ecdh-group [group19 | group20 | group21]
hostname(config)# ssl ecdh-group group20
```

Le mot-clé `group19` configure le groupe 19 (EC 256 bits). Le mot-clé `group20` configure le groupe 20 (EC de 384 bits). Le mot-clé `group21` configure le groupe 21 (EC 521 bits).

La valeur par défaut est `ssl ecdh-group group19`.

#### Remarque

Les chiffrements ECDSA et DHE ont la priorité la plus élevée.

### Prochaine étape

Vous pouvez utiliser les commandes suivantes pour afficher la configuration TLS/DTLS :

- **show run ssl** s'il ne s'agit pas de la version TLS/DTLS par défaut.
- **show run ssl all** s'il s'agit de la version TLS/DTLS par défaut.

## Flux persistants tunnelisés IPsec

Dans les réseaux exécutant une version du logiciel ASA antérieure à la version 8.0.4, les flux de trafic IPsec LAN à LAN ou TCP d'accès à distance traversant un tunnel IPsec sont abandonnés lorsque le tunnel tombe. Les flux sont recréés au besoin lorsque et si le tunnel est de nouveau disponible. Cette politique fonctionne bien du point de vue de la gestion des ressources et de la sécurité. Cependant, dans certains cas, ce comportement peut poser problème pour les utilisateurs, en particulier pour ceux qui migrent d'environnements PIX vers des environnements ASA uniquement et pour les applications TCP héritées qui ne redémarrent pas facilement, ou dans les réseaux comprenant des passerelles qui ont tendance à interrompre fréquemment les tunnels. (Consultez CSCsj40681 et CSCsi47630 pour en savoir plus.)

La fonctionnalité de flux de tunnel IPsec persistant résout ce problème. Avec cette fonctionnalité activée, l'ASA conserve et reprend les flux tunnelisés avec état (TCP). Tous les autres flux sont abandonnés lorsque le tunnel tombe et doivent se rétablir lorsqu'un nouveau tunnel apparaît.

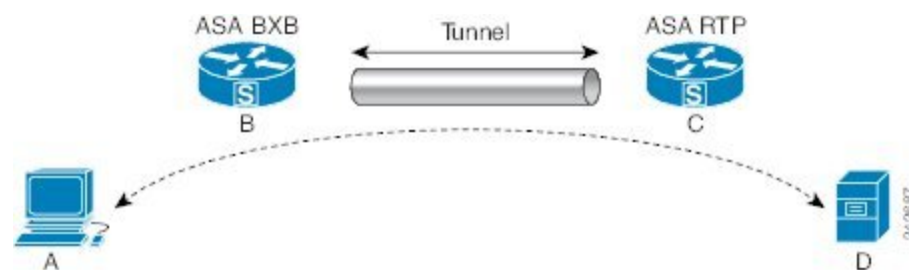


#### Remarque

Cette fonctionnalité prend en charge les tunnels IPsec LAN à LAN et les tunnels d'accès à distance IPsec fonctionnant en mode Network-Extension. Il ne prend pas en charge les tunnels d'accès à distance IPsec ou AnyConnect/SSL.

L'exemple suivant montre le fonctionnement de la fonctionnalité de flux persistants de tunnellation IPsec.

**Illustration 5 : Scénario de réseau**



Dans cet exemple, les réseaux BXB et RTP sont connectés via un tunnel sécurisé LAN à LAN par une paire d'équipements de sécurité. Un ordinateur dans le réseau BXB exécute un transfert FTP à partir d'un serveur dans le réseau RTP par l'intermédiaire du tunnel sécurisé. Dans ce scénario, supposons que, pour une raison quelconque, le tunnel soit abandonné après que le PC se soit connecté au serveur et ait lancé le transfert. Bien que le tunnel soit rétabli puisque les données tentent toujours de circuler, le transfert FTP ne se termine pas. L'utilisateur doit mettre fin au transfert et recommencer en se connectant au serveur. Toutefois, si la

fonctionnalité de flux de tunnel IPsec persistants est activée, tant que le tunnel est recréé dans l'intervalle de temporisation, les données continuent de circuler correctement dans le nouveau tunnel, car les équipements de sécurité conservent l'état de ce flux.

### Scénario

Les sections suivantes décrivent les situations de flux de données pour un tunnel abandonné et récupéré, d'abord avec la fonctionnalité des flux persistants de tunnellation IPsec désactivée, puis avec la fonctionnalité activée. Dans les deux cas, reportez-vous à la figure précédente pour une illustration du réseau. Dans cette illustration :

- Le flux B-C définit le tunnel [et transporte les données ESP chiffrées](#).
- Le flux A-D est la connexion TCP du transfert FTP et traverse le tunnel défini par le flux B-C. Ce flux contient également des informations d'état utilisées par le pare-feu pour inspecter ce flux TCP/FTP. Les informations sur l'état sont essentielles et sont constamment mises à jour par le pare-feu à mesure que le transfert progresse.



#### Remarque

Les flux inverses dans chaque direction sont omis pour des raisons de simplicité.

### Flux persistants de tunnellation IPsec désactivés

Lorsque le tunnel LAN à LAN tombe, le flux A-D et le flux B-C et toutes les informations d'état leur appartenant sont supprimées. Par la suite, le tunnel est rétabli et le flux B-C est recréé et peut reprendre le transport des données tunnelisées. Mais le flux TCP/FTP A-D rencontre des problèmes. Comme les informations d'état décrivant le flux jusqu'à ce stade du transfert FTP ont été supprimées, le pare-feu avec état bloque les données FTP en transit et rejette la création du flux A-D. Ayant perdu l'historique de l'existence même de ce flux, le pare-feu traite le transfert FTP comme des paquets TCP parasites et les abandonne. Il s'agit du comportement par défaut.

### Flux de tunnel IPsec persistants activés

Avec la fonctionnalité de flux persistants de tunnellation IPsec activée, tant que le tunnel est recréé dans la fenêtre de délai d'expiration, les données continuent de circuler correctement, car l'ASA a toujours accès aux informations d'état du flux A-D.

Avec cette fonctionnalité activée, l'ASA traite les flux de manière indépendante. Cela signifie que le flux A-D n'est pas supprimé lorsque le tunnel défini par le flux B-C est abandonné. L'ASA conserve et reprend les flux tunnelisés avec état (TCP). Tous les autres flux sont abandonnés et doivent être rétablis sur le nouveau tunnel. Cela n'affecte pas la politique de sécurité pour les flux tunnelisés, car l'ASA abandonne tous les paquets entrants sur le flux A-D lorsque le tunnel est en panne.

Les flux TCP tunnelisés ne sont pas abandonnés, ils reposent donc sur le délai d'expiration TCP pour le nettoyage. Toutefois, si le délai d'expiration est désactivé pour un flux tunnelisé particulier, ce flux reste dans le système jusqu'à ce qu'il soit effacé manuellement ou par d'autres moyens (par exemple, par un TCP RST de l'homologue).



# Configurer les flux de tunnel IPsec persistants à l'aide de l'interface de ligne de commande

Exemple de configuration

## Dépannage des flux persistants tunnelisés IPsec

Les commandes **show asp table** et **show conn** peuvent être utiles pour résoudre les problèmes liés aux flux IPsec tunnelisés persistants.

### La fonctionnalité des flux de tunnel IPsec persistants est-elle activée ?

Pour voir si cette fonctionnalité est activée dans un tunnel particulier, consultez le contexte VPN associé au tunnel à l'aide de la commande **show asp table**. La commande **show asp table vpn-context** affiche un indicateur « +PRESERVE » pour chaque contexte qui maintient les flux avec état après l'interruption du tunnel, comme illustré dans l'exemple suivant (gras ajoutés pour la lisibilité) :

```
hostname(config)# show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
```

```

hostname(config)# show asp table vpn-context detail
```

```
VPN CTX = 0x0005FF54

Peer IP = ASA_Private
Pointer = 0x6DE62DA0
State = UP
Flags = DECR+ESP+PRESERVE
SA = 0x001659BF
SPI = 0xB326496C
Group = 0
Pkts = 0
Bad Pkts = 0
Bad SPI = 0
Spoof = 0
Bad Crypto = 0
Rekey Pkt = 0
Rekey Call = 0
```

```
VPN CTX = 0x0005B234

Peer IP = ASA_Private
Pointer = 0x6DE635E0
State = UP
Flags = ENCR+ESP+PRESERVE
SA = 0x0017988D
SPI = 0x9AA50F43
Group = 0
Pkts = 0
Bad Pkts = 0
Bad SPI = 0
Spoof = 0
Bad Crypto = 0
```

```

Rekey Pkt = 0
Rekey Call = 0
hostname(config)#
Configuration and Restrictions
This configuration option is subject to the same CLI configuration restrictions as other
sysopt VPN CLI.

```

## Localisation des flux orphelins

Si un tunnel LAN à LAN / Network-Extension Mode tombe et ne se rétablit pas avant l'expiration du délai, il peut subsister un certain nombre de flux de tunnel orphelins. Ces flux ne sont pas interrompus en raison de la panne du tunnel, mais toutes les données qui tentent de les traverser sont abandonnées. Pour voir ces flux, utilisez la commande **show conn**, comme dans les exemples suivants (le gras est ajouté pour mettre en évidence les entrées utilisateur) :

```

asa2(config)# show conn detail
9 in use, 14 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
 B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
 E - outside back connection, F - outside FIN, f - inside FIN,
 G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
 i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
 k - Skinny media, M - SMTP data, m - SIP media, n - GUP
 O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
 q - SQL*Net data, R - outside acknowledged FIN,
 R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
 s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
 V - VPN orphan, W - WAAS,
 X - inspected by service module

```

L'exemple suivant montre un exemple de sortie de la commande **show conn** lorsqu'un flux orphelin existe, comme indiqué par l'indicateur **V** :

```

hostname# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00 bytes 1048 flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle bytes 1048 flags UIOB

```

Pour limiter le rapport aux connexions comportant des flux orphelins, ajoutez l'option **vpn\_orphan** à la commande **show conn state**, comme dans l'exemple suivant :

```

hostname# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013 idle 0:00:00 bytes 2841019 flags UOVB

```

## Effacer les configurations WebVPN de l'ASA

Lorsque vous utilisez les commandes **no webvpn** et **clear configure webvpn**, les configurations WebVPN par défaut ne sont pas supprimées. Les compteurs **http\_in** et **http\_out** sont conservés pour recueillir des statistiques de compression.

Pour effacer les configurations WebVPN de l'ASA, effectuez l'une des opérations suivantes :

- Désactivez les statistiques de compression après un démarrage à l'aide de la commande **no compression all**.
- Effacez les compteurs de statistiques de compression à l'aide de la commande **clear compression all**.



## CHAPITRE 5

# Profils de connexion, stratégies de groupe et utilisateurs

Ce chapitre décrit comment configurer les profils de connexion VPN (anciennement appelés « groupes de tunnels »), les stratégies de groupe et les utilisateurs. Ce chapitre comprend les sections suivantes :

- [Aperçu des profils de connexion, des stratégies de groupe et des utilisateurs, à la page 99](#)
- [Profils de connexion, à la page 101](#)
- [Configurer les profils de connexion, à la page 105](#)
- [Stratégies de groupe, à la page 132](#)
- [Utiliser un serveur Zone Labs Integrity., à la page 175](#)
- [Configurer les attributs d'utilisateur, à la page 181](#)
- [Bonnes pratiques pour la configuration et l'ajustement de l'ACL du filtre de VPN, à la page 190](#)

## Aperçu des profils de connexion, des stratégies de groupe et des utilisateurs

Les groupes et les utilisateurs sont des concepts centraux dans la gestion de la sécurité des réseaux privés virtuels (VPN) et dans la configuration de l'ASA. Ils précisent les attributs qui déterminent l'accès de l'utilisateur et l'utilisation du VPN. Un *groupe* est un ensemble d'utilisateurs traités comme une seule entité. *Les utilisateurs* obtiennent leurs attributs des *stratégies de groupe*. Un *profil de connexion* identifie la stratégie de groupe pour une connexion spécifique. Si vous n'affectez pas de stratégie de groupe particulière à un utilisateur, la stratégie de groupe par défaut pour la connexion s'applique.

En résumé, vous configurez d'abord les profils de connexion pour définir les valeurs de la connexion. Ensuite, vous configurez les stratégies de groupe. Celles-ci définissent des valeurs pour les utilisateurs dans l'agrégation. Vous configurez ensuite les utilisateurs, qui peuvent hériter des valeurs des groupes et configurer certaines valeurs sur la base d'un utilisateur individuel. Ce chapitre décrit comment et pourquoi configurer ces entités.



### Remarque

Vous configurez les profils de connexion à l'aide des commandes **tunnel-group**. Dans ce chapitre, les termes « connection profile » (profil de connexion) et « tunnel group » (groupe de tunnels) sont souvent utilisés de manière interchangeable.

Les profils de connexion et les stratégies de groupe simplifient la gestion du système. Pour simplifier la tâche de configuration, l'ASA fournit un profil de connexion par défaut de réseau local (LAN) (DefaultL2Lgroup), un profil de connexion d'accès à distance par défaut pour le VPN IKEv2 (DefaultRAGroup), un profil de connexion par défaut pour les connexions SSL sans client et Secure Client (services client sécurisés) SSL (DefaultWEBVPNgroup) et une stratégie de groupe par défaut (DfltGrpPolicy). Les profils de connexion par défaut et la stratégie de groupe fournissent des paramètres qui sont susceptibles d'être communs à de nombreux utilisateurs. Lorsque vous ajoutez des utilisateurs, vous pouvez préciser qu'ils « héritent » des paramètres d'une stratégie de groupe. Ainsi, vous pouvez configurer rapidement l'accès VPN pour un grand nombre d'utilisateurs.

Si vous décidez d'accorder des droits identiques à tous les utilisateurs VPN, vous n'avez pas besoin de configurer des profils de connexion ou des stratégies de groupe spécifiques, mais les VPN fonctionnent rarement de cette manière. Par exemple, vous pourriez permettre à un groupe des finances d'accéder à une partie d'un réseau privé, à un groupe de service à la clientèle d'accéder à une autre partie et à un groupe MIS d'accéder aux autres parties. En outre, vous pouvez autoriser des utilisateurs spécifiques du groupe MIS à accéder à des systèmes auxquels d'autres utilisateurs du groupe MIS n'ont pas accès. Les profils de connexion et les stratégies de groupe offrent la possibilité de le faire de manière sécurisée.



#### Remarque

L'ASA comprend également le concept de groupes d'objets, qui est un surensemble de listes de réseaux. Les groupes d'objets vous permettent de définir l'accès VPN aux ports ainsi qu'aux réseaux. Les groupes d'objets sont liés aux listes de contrôle d'accès plutôt qu'aux stratégies de groupe et aux profils de connexion. Pour en savoir plus sur l'utilisation des groupes d'objets, consultez le chapitre 20, « Objets » dans le guide de configuration sur les opérations générales.

L'appareil de sécurité peut appliquer des valeurs d'attribut à partir d'une variété de sources. Il les applique selon la hiérarchie suivante :

1. enregistrement Dynamic Access Policy (DAP)
2. Nom de l'utilisateur
3. Stratégie de groupe
4. Stratégie de groupe pour le profil de connexion
5. Stratégie de groupe par défaut

Par conséquent, les valeurs DAP d'un attribut ont une priorité plus élevée que celles configurées pour un utilisateur, une stratégie de groupe ou un profil de connexion.

Lorsque vous activez ou désactivez un attribut pour un enregistrement DAP, l'ASA applique cette valeur et l'impose. Par exemple, lorsque vous désactivez le serveur proxy HTTP en mode de configuration `dap webvpn`, l'ASA ne cherche aucune autre valeur. Lorsque vous utilisez à la place le mot-clé `no` pour la commande `http-proxy`, l'attribut n'est pas présent dans l'enregistrement DAP, de sorte que l'appareil de sécurité remonte à l'attribut AAA dans le nom d'utilisateur et, si nécessaire, à la stratégie de groupe pour trouver une valeur à appliquer. La configuration VPN SSL sans client ASA ne prend en charge qu'une seule commande **http-proxy** et une seule commande **https-proxy**. Nous vous recommandons d'utiliser ASDM pour configurer DAP.

# Profils de connexion

Un profil de connexion comprend un ensemble d'enregistrements qui déterminent les politiques de connexion du tunnel. Ces enregistrements identifient les serveurs sur lesquels l'utilisateur du tunnel est authentifié, ainsi que les serveurs de comptabilité, le cas échéant, auxquels les informations de connexion sont envoyées. Ils identifient également une stratégie de groupe par défaut pour la connexion et contiennent des paramètres de connexion spécifiques au protocole. Les profils de connexion comprennent un petit nombre d'attributs qui concernent la création du tunnel lui-même. Les profils de connexion comprennent un pointeur vers une stratégie de groupe qui définit les attributs axés sur l'utilisateur.

L'ASA fournit les profils de connexion par défaut suivants : DefaultL2Lgroup pour les connexions de réseau local (LAN à réseau local), DefaultRAGroup pour les connexions d'accès à distance IPSEC et DefaultWEBVPNGroup pour les connexions VPN SSL (basées sur le navigateur et Secure Client (services client sécurisés)). Vous pouvez modifier ces profils de connexion par défaut, mais vous ne pouvez pas les supprimer. Vous pouvez également créer un ou plusieurs profils de connexion spécifiques à votre environnement. Les profils de connexion sont locaux à l'ASA et ne peuvent pas être configurés sur des serveurs externes.



## Remarque

Certains profils (comme IKEv1 en phase 1) peuvent ne pas être en mesure de déterminer si un terminal est d'accès à distance ou de réseau local (LAN). S'il ne peut pas déterminer le groupe de tunnels, il utilise la valeur par défaut

```
tunnel-group-map default-group <tunnel-group-name>
```

(la valeur par défaut est *DefaultRAGroup*).

## Paramètres de connexion du profil de connexion général

Les paramètres généraux sont communs à toutes les connexions VPN. Les paramètres généraux incluent les éléments suivants :

- Nom du profil de connexion : vous spécifiez un nom de profil de connexion lorsque vous ajoutez ou modifiez un profil de connexion. Les considérations suivantes s'appliquent :
  - Pour les clients qui utilisent des clés prépartagées pour s'authentifier, le nom de profil de connexion est le même que le nom de groupe qu'un client transmet à l'ASA.
  - Les clients qui utilisent des certificats pour s'authentifier transmettent ce nom dans le cadre du certificat, et l'ASA extrait le nom du certificat.
- Type de connexion : les types de connexion comprennent l'accès à distance IKEv1, IPsec de LAN à LAN et AnyConnect (SSL/IKEv2). Un profil de connexion ne peut avoir qu'un seul type de connexion.
- Serveurs d'authentification, d'autorisation et de comptabilité : ces paramètres identifient les groupes ou les listes de serveurs que l'ASA utilise aux fins suivantes :
  - Authentification des utilisateurs
  - Obtention de renseignements sur les services auxquels les utilisateurs sont autorisés à accéder
  - Stockage des enregistrements comptables

Un groupe de serveurs peut comprendre un ou plusieurs serveurs.

- Stratégie de groupe par défaut pour la connexion : une stratégie de groupe est un ensemble d'attributs axés sur l'utilisateur. La stratégie de groupe par défaut est la stratégie de groupe dont l'ASA utilise les attributs par défaut lors de l'authentification ou de l'autorisation d'un utilisateur de tunnel.
- Méthode d'affectation d'adresse client : cette méthode comprend des valeurs pour un ou plusieurs serveurs DHCP ou ensembles d'adresses que l'ASA affecte aux clients.
- Gestion des mots de passe : ce paramètre vous permet d'alerter un utilisateur que le mot de passe actuel doit expirer dans un nombre spécifié de jours (la valeur par défaut est de 14 jours), puis d'offrir à l'utilisateur la possibilité de modifier le mot de passe.
- Suppression de groupe et de domaine : ces paramètres dirigent la façon dont l'ASA traite les noms d'utilisateurs qu'il reçoit. Ils s'appliquent uniquement aux noms d'utilisateurs reçus sous la forme `user@realm`.

Un domaine est un domaine administratif ajouté à un nom d'utilisateur avec le délimiteur `@` (`user@abc`). Si vous supprimez le domaine, l'ASA utilise le nom d'utilisateur et le groupe (le cas échéant) pour l'authentification. Si vous supprimez le groupe, l'ASA utilise le nom d'utilisateur et le domaine (le cas échéant) pour l'authentification.

Saisissez la commande `strip-realm` pour supprimer le qualificatif de domaine, et saisissez la commande `strip-group` pour supprimer le qualificatif de groupe du nom d'utilisateur lors de l'authentification. Si vous supprimez les deux qualificatifs, l'authentification est basée sur le *nom d'utilisateur* uniquement. Sinon, l'authentification est basée sur la chaîne complète `username@realm` ou `username<delimiter>group`. Vous devez préciser `strip-realm` si votre serveur ne peut pas analyser les délimiteurs.

En outre, pour les clients L2TP/IPsec uniquement, lorsque vous spécifiez la commande `strip-group`, l'ASA sélectionne le profil de connexion (groupe de tunnels) pour les connexions utilisateur en obtenant le nom de groupe à partir du nom d'utilisateur présenté par le client VPN.

- Autorisation requise : ce paramètre vous permet d'exiger une autorisation avant qu'un utilisateur ne puisse se connecter ou de désactiver cette exigence.
- Attributs DN d'autorisation : ce paramètre spécifie les attributs de nom distinctif à utiliser lors de l'autorisation.

## Paramètres de connexion de groupe de tunnels IPsec

Les paramètres IPsec comprennent les éléments suivants :

- Une méthode d'authentification du client : clés prépartagées, certificats ou les deux.
  - Pour les connexions IKE basées sur des clés prépartagées, il s'agit de la clé alphanumérique elle-même (jusqu'à 128 caractères de long), associée à la politique de connexion.
  - Exigence de validation de l'identifiant de l'homologue : ce paramètre spécifie s'il faut valider l'identité de l'homologue à l'aide du certificat d'homologue.
  - Si vous spécifiez des certificats ou les deux pour la méthode d'authentification, l'utilisateur final doit fournir un certificat valide afin de s'authentifier.
- Une méthode d'authentification hybride étendue : XAUTH et XAUTH hybride.

Vous utilisez la commande **isakmp ikev1-user-authentication** pour mettre en œuvre l'authentification hybride XAUTH lorsque vous devez utiliser des certificats numériques pour l'authentification ASA et une méthode existante différente pour l'authentification des utilisateurs VPN distants, comme RADIUS, TACACS+ ou SecurID.

- Paramètres keepalive d'ISAKMP (IKE). Cette fonctionnalité permet à l'ASA de surveiller la présence continue d'un homologue distant et de signaler sa propre présence à cet homologue. Si l'homologue ne répond pas, l'ASA supprime la connexion. L'activation des messages keepalive IKE empêche les connexions bloquées lorsque l'homologue IKE perd la connectivité.

Il existe différentes formes de messages keepalive IKE. Pour que cette fonctionnalité fonctionne, l'ASA et son homologue distant doivent prendre en charge une forme commune. Cette fonctionnalité fonctionne avec les homologues suivants :

- Cisco AnyConnect VPN Client
- logiciel Cisco IOS<sup>®</sup>
- Cisco Secure PIX Firewall

Les clients VPN autres que Cisco ne prennent pas en charge les IKE keepalives.

Si vous configurez un groupe d'homologues mixtes et que certains de ces homologues prennent en charge les IKE keepalives et d'autres ne le font pas, activez les IKE keepalives pour l'ensemble du groupe. La fonctionnalité n'affecte pas les homologues qui ne la prennent pas en charge.

Si vous désactivez les IKE keepalives, les connexions avec des homologues qui ne répondent pas restent actives jusqu'à leur expiration. Nous vous recommandons donc de maintenir votre délai d'inactivité court. Pour modifier votre délai d'inactivité, consultez [Configurer les stratégies de groupe](#), à la page 136.



#### Remarque

Pour réduire les coûts de connectivité, désactivez les IKE keepalives si ce groupe comprend des clients se connectant par l'intermédiaire des lignes ISDN. Les connexions ISDN se déconnectent normalement si elles sont inactives, mais le mécanisme IKE keepalive empêche les connexions d'être inactives et donc de se déconnecter.

Si vous désactivez les IKE keepalives, le client se déconnecte uniquement lorsque ses clés IKE ou IPsec expirent. Le trafic en échec ne déconnecte pas le tunnel avec les valeurs du profil de délai d'expiration d'homologue comme il le fait lorsque les IKE keepalives sont activés.

Si vous avez une configuration LAN à LAN en utilisant le mode principal IKE, assurez-vous que les deux homologues ont la même configuration IKE keepalive. Les deux homologues doivent avoir activé les IKE keepalives ou les deux homologues doivent l'avoir désactivé.

- Si vous configurez l'authentification à l'aide de certificats numériques, vous pouvez préciser s'il faut envoyer l'ensemble de la chaîne de certificats (qui envoie à l'homologue le certificat d'identité et tous les certificats émis) ou uniquement les certificats d'autorité émettrice (y compris le certificat racine et tous les certificats d'autorité de certification subordonnés).

- Vous pouvez informer les utilisateurs qui utilisent des versions obsolètes du logiciel client Windows qu'ils doivent mettre à jour leur client, et vous pouvez fournir un mécanisme pour qu'ils obtiennent la version client mise à jour. Vous pouvez configurer et modifier la mise à jour client, soit pour tous les profils de connexion, soit pour des profils de connexion particuliers.
- Si vous configurez l'authentification à l'aide de certificats numériques, vous pouvez spécifier le nom du point de confiance qui identifie le certificat à envoyer à l'homologue IKE.

## Paramètres de connexion de profil de connexion pour les sessions VPN SSL

Le tableau ci-dessous fournit une liste des attributs de profil de connexion qui sont spécifiques aux connexions VPN SSL (Secure Client (services client sécurisés) et sans client). En plus de ces attributs, vous configurez les attributs de profil de connexion généraux communs à toutes les connexions VPN.



### Remarque

Dans les versions antérieures, les « profils de connexion » étaient appelés « groupes de tunnels ». Vous configurez un profil de connexion avec des commandes de groupe de tunnels. Ce chapitre utilise souvent ces termes de manière interchangeable.

**Tableau 7 : Attributs de profil de connexion pour le VPN SSL**

|                       | Fonction                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>authentication</b> | Définit la méthode d'authentification AAA ou Certificat.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>customization</b>  | Identifie le nom d'une personnalisation définie précédemment à appliquer. Les personnalisations déterminent l'apparence des fenêtres que l'utilisateur voit à l'ouverture de session. Vous configurez les paramètres de personnalisation dans le cadre de la configuration du VPN SSL sans client.                                                                                                                                                                                                                              |
| <b>nbns-server</b>    | Identifie le nom du serveur de service de nom NetBIOS (nbns-server) à utiliser pour la résolution de nom CIFS.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>group-alias</b>    | Spécifie un ou plusieurs autres noms par lesquels le serveur peut faire référence à un profil de connexion. Lors de la connexion, l'utilisateur sélectionne le nom du groupe dans un menu déroulant.                                                                                                                                                                                                                                                                                                                            |
| <b>group-url</b>      | Identifie une ou plusieurs URL de groupe. Si vous configurez cet attribut, les utilisateurs entrant sur une URL spécifiée n'ont pas besoin de sélectionner de groupe à la connexion.<br><br>Un déploiement d'équilibrage de charge qui utilise des URL de groupe pour la connectivité Secure Client (services client sécurisés), nécessite que chaque nœud ASA de la grappe configure une URL de groupe pour l'adresse de grappe virtuelle, ainsi qu'une URL de groupe pour l'adresse publique d'équilibrage de charge du nœud. |
| <b>dns-group</b>      | Identifie le groupe de serveurs DNS qui spécifie le nom du serveur DNS, le nom de domaine, le serveur de noms, le nombre de tentatives et les valeurs de délai d'expiration d'un serveur DNS à utiliser pour un profil de connexion.                                                                                                                                                                                                                                                                                            |



|                              | Fonction                                                                                                                                                                                                                                             |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>hic-fail-group-policy</b> | Spécifie une politique de fonctionnalité VPN si vous utilisez Cisco Secure Desktop Manager pour définir l'attribut de politique basée sur un groupe sur « Use Failure Group-Policy » ou « Use Success Group-Policy, si les critères correspondent ». |
| <b>override-svc-download</b> | Remplace le téléchargement des attributs de stratégie de groupe ou de nom d'utilisateur configurés pour le téléchargement du client VPN AnyConnect vers l'utilisateur distant.                                                                       |
| <b>radius-reject-message</b> | Active l'affichage du message de rejet RADIUS sur l'écran de connexion lorsque l'authentification est rejetée.                                                                                                                                       |

## Configurer les profils de connexion

Cette section décrit le contenu et la configuration des profils de connexion, tant en mode contexte unique qu'en mode contexte multiple.



### Remarque

Le mode contexte multiple s'applique uniquement aux VPN de site à site IKEv2 et IKEv1 et ne s'applique pas à Secure Client (services client sécurisés), au VPN SSL sans client, à l'ancien client VPN Cisco, au client VPN natif d'Apple, au client VPN natif de Microsoft ni à cTCP pour IKEv1 IPsec.

Vous pouvez modifier les profils de connexion par défaut et vous pouvez configurer un nouveau profil de connexion pour l'un des trois types de groupe de tunnels. Si vous ne configurez pas explicitement un attribut dans un profil de connexion, cet attribut reçoit sa valeur du profil de connexion par défaut. Le type de profil de connexion par défaut est l'accès à distance. Les paramètres suivants dépendent de votre choix de type de tunnel. Pour voir la configuration actuelle et la configuration par défaut de tous vos profils de connexion, y compris le profil de connexion par défaut, saisissez la commande **show running-config all tunnel-group**.

## Profils de connexion

Le nombre maximal de profils de connexion (groupes de tunnels) qu'un ASA peut prendre en charge est une fonction du nombre maximal de sessions VPN simultanées pour la plateforme + 5. La tentative d'ajout d'un groupe de tunnels supplémentaire au-delà de la limite entraîne l'affichage du message suivant : « ERREUR : la limite de 30 groupes de tunnels configurés a été atteinte ».

## Configuration par défaut du profil de connexion IPsec d'accès à distance

Le contenu du profil de connexion d'accès à distance par défaut est le suivant :

```
tunnel-group DefaultRAGroup type remote-access
tunnel-group DefaultRAGroup general-attributes
no address-pool
no ipv6-address-pool
authentication-server-group LOCAL
accounting-server-group RADIUS
default-group-policy DfltGrpPolicy
```

```

no dhcp-server
no strip-realm
no password-management
no override-account-disable
no strip-group
no authorization-required
authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup webvpn-attributes
 hic-fail-group-policy DfltGrpPolicy
 customization DfltCustomization
 authentication aaa
 no override-svc-download
 no radius-reject-message
 dns-group DefaultDNS
tunnel-group DefaultRAGroup ipsec-attributes
 no pre-shared-key
 peer-id-validate req
 no chain
 no trust-point
 isakmp keepalive threshold 1500 retry 2
 no radius-sdi-xauth
 isakmp ikev1-user-authentication xauth
tunnel-group DefaultRAGroup ppp-attributes
 no authentication pap
 authentication chap
 authentication ms-chap-v1
 no authentication ms-chap-v2
 no authentication eap-proxy

tunnel-group DefaultRAGroup type remote-access
tunnel-group DefaultRAGroup general-attributes
 no address-pool
 no ipv6-address-pool
 authentication-server-group LOCAL
 accounting-server-group RADIUS
 default-group-policy DfltGrpPolicy
 no dhcp-server
 no strip-realm
 no password-management
 no strip-group
 no authorization-required
 authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup webvpn-attributes
 hic-fail-group-policy DfltGrpPolicy
 customization DfltCustomization
 authentication aaa
 no override-svc-download
 no radius-reject-message
 dns-group DefaultDNS
tunnel-group DefaultRAGroup ipsec-attributes
 no pre-shared-key
 peer-id-validate req
 no chain
 no trust-point
 isakmp keepalive threshold 1500 retry 2
 no radius-sdi-xauth
 isakmp ikev1-user-authentication xauth
tunnel-group DefaultRAGroup ppp-attributes
 no authentication pap
 authentication chap
 authentication ms-chap-v1
 no authentication ms-chap-v2
 no authentication eap-proxy

```

## Attributs généraux du groupe de tunnels IPsec

Les attributs généraux sont communs à plus d'un type de groupe de tunnels. Les tunnels d'accès à distance IPsec et de VPN SSL sans client partagent la plupart des mêmes attributs généraux. Les tunnels IPsec de réseau LAN à LAN utilisent un sous-ensemble. Reportez-vous à la *Référence des commandes de la série Cisco Secure Firewall ASA* pour obtenir une description complète de toutes les commandes. Cette section décrit, dans l'ordre, comment configurer les profils d'accès à distance et de connexion LAN à LAN.

## Configurer les profils de connexion d'accès à distance.

Utilisez un profil de connexion d'accès à distance lors de la configuration d'une connexion entre les clients distants suivants et un ASA de site central :

- Secure Client (connexion avec SSL ou IPsec/IKEv2)
- VPN SSL sans client (connexion par navigateur avec SSL)
- Client matériel VPN Cisco ASA 5500 Easy (connexion avec IPsec/IKEv1)

Nous fournissons également une stratégie de groupe par défaut nommée DfltGrpPolicy.

Pour configurer un profil de connexion d'accès à distance, configurez d'abord les attributs généraux du groupe de tunnels, puis les attributs d'accès à distance. Consultez les sections suivantes :

- [Préciser un nom et un type pour le profil de connexion d'accès à distance, à la page 107.](#)
- [Configurer les attributs généraux du profil de connexion d'accès à distance, à la page 108.](#)
- [Configurer de la double authentification, à la page 112](#)
- [Configurer les attributs IPsec IKEv1 du profil de connexion d'accès à distance, à la page 114.](#)
- [Configurer les attributs PPP du profil de connexion à distance IPsec, à la page 116](#)

## Préciser un nom et un type pour le profil de connexion d'accès à distance

### Procédure

---

Créez le profil de connexion en précisant son nom et son type, en saisissant la commande **tunnel-group**.

Pour un tunnel d'accès à distance, le type est **remote-access**.

**tunnel-group** *tunnel\_group\_name* **type remote-access**

#### Exemple :

Par exemple, pour créer un profil de connexion d'accès à distance nommé TunnelGroup1, entrez la commande suivante :

```
hostname(config)# tunnel-group TunnelGroup1 type remote-access
hostname(config)#
```

---

## Configurer les attributs généraux du profil de connexion d'accès à distance

Pour configurer ou modifier les attributs généraux du profil de connexion, précisez les paramètres selon les étapes suivantes.

### Procédure

#### Étape 1

Pour configurer les attributs généraux, exécutez la tâche **tunnel-group general-attributes** en mode contexte unique ou multiple, ce qui vous place en mode de configuration tunnel-group general-attributes. L'invite change pour indiquer le changement de mode.

```
hostname(config)# tunnel-group tunnel_group_name general-attributes
hostname(config-tunnel-general)#
```

#### Étape 2

Précisez le nom du groupe de serveurs d'authentification, le cas échéant. Si vous souhaitez utiliser la base de données LOCAL pour l'authentification en cas d'échec du groupe de serveurs spécifié, ajoutez le mot-clé **LOCAL** :

```
hostname(config-tunnel-general)# authentication-server-group [(interface_name)] groupname
[LOCAL]
hostname(config-tunnel-general)#
```

Le nom du groupe de serveurs d'authentification peut comporter jusqu'à 16 caractères.

Vous pouvez éventuellement configurer une authentification spécifique à une interface en ajoutant le nom de l'interface après celui du groupe. Le nom de l'interface, qui indique où le tunnel se termine, doit être placé entre parenthèses. La commande suivante configure une authentification spécifique à l'interface pour l'interface nommée test, en utilisant le groupe de serveurs servergroup1 pour l'authentification :

```
hostname(config-tunnel-general)# authentication-server-group (test) servergroup1
hostname(config-tunnel-general)#
```

#### Étape 3

Précisez le nom du groupe de serveurs d'autorisation à utiliser, le cas échéant. Lorsque vous configurez cette valeur, les utilisateurs doivent exister dans la base de données des autorisations pour la connexion :

```
hostname(config-tunnel-general)# authorization-server-group groupname
hostname(config-tunnel-general)#
```

Le nom du groupe de serveurs d'autorisation peut comporter jusqu'à 16 caractères. Par exemple, la commande suivante précise l'utilisation du groupe de serveurs d'autorisation FinGroup :

```
hostname(config-tunnel-general)# authorization-server-group FinGroup
hostname(config-tunnel-general)#
```

#### Étape 4

Précisez le nom du groupe de serveurs de comptabilité à utiliser, le cas échéant :

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

Le nom du groupe de serveurs de comptabilité peut comporter jusqu'à 16 caractères. Par exemple, la commande suivante spécifie l'utilisation du groupe de serveurs de comptabilité nommé comptroller :

```
hostname(config-tunnel-general) # accounting-server-group comptroller
hostname(config-tunnel-general) #
```

### Étape 5

Précisez le nom de la stratégie de groupe par défaut :

```
hostname(config-tunnel-general) # default-group-policy policynome
hostname(config-tunnel-general) #
```

Le nom de la stratégie de groupe peut comporter jusqu'à 64 caractères. L'exemple suivant définit DfltGrpPolicy comme nom de la stratégie de groupe par défaut :

```
hostname(config-tunnel-general) # default-group-policy DfltGrpPolicy
hostname(config-tunnel-general) #
```

### Étape 6

Précisez les noms ou les adresses IP des serveurs DHCP (jusqu'à 10 serveurs), ainsi que les noms des ensembles d'adresses DHCP (jusqu'à 6 ensembles). Les valeurs par défaut sont aucun serveur DHCP et aucun ensemble d'adresses. La commande **dhcp-server** permet de configurer l'ASA pour qu'il envoie des options supplémentaires aux serveurs DHCP spécifiés lorsqu'il tente d'attribuer des adresses IP aux clients VPN. Pour en savoir plus sur la commande **dhcp-server**, consultez le guide de référence des commandes Cisco Secure Firewall ASA.

```
hostname(config-tunnel-general) # dhcp-server server1 [...server10]
hostname(config-tunnel-general) # address-pool [(interface name)] address_pool1
[...address_pool6]
hostname(config-tunnel-general) #
```

#### Remarque

Si vous spécifiez un nom d'interface, vous devez le mettre entre parenthèses.

Vous configurez les ensembles d'adresses à l'aide de la commande **ip local pool** en mode de configuration globale.

### Étape 7

Précisez le nom du groupe de serveurs d'authentification NAC, si vous utilisez le contrôle d'admission au réseau, afin d'identifier le groupe de serveurs utilisé pour la validation de posture NAC. Configurez au moins un serveur de contrôle d'accès pour prendre en charge la NAC. Utilisez la commande **aaa-server** pour nommer le groupe ACS. Utilisez ensuite la commande **nac-authentication-server-group** en reprenant le même nom de groupe.

L'exemple suivant identifie acs-group1 comme groupe de serveurs d'authentification utilisé pour la validation de posture NAC :

```
hostname(config-group-policy) # nac-authentication-server-group acs-group1
hostname(config-group-policy) #
```

L'exemple suivant montre l'héritage du groupe de serveurs d'authentification à partir du groupe d'accès à distance par défaut :

```
hostname(config-group-policy) # no nac-authentication-server-group
```

```
hostname (config-group-policy)
```

#### Remarque

La NAC nécessite la présence de Cisco Trust Agent sur l'hôte distant.

### Étape 8

Précisez s'il faut supprimer le groupe ou le domaine du nom d'utilisateur avant de le transmettre au serveur AAA. La valeur par défaut est de ne pas supprimer le nom de groupe ou le domaine :

```
hostname (config-tunnel-general) # strip-group
hostname (config-tunnel-general) # strip-realm
hostname (config-tunnel-general) #
```

Un domaine est un domaine administratif. Si vous supprimez le domaine, l'ASA utilise le nom d'utilisateur et le groupe (le cas échéant) pour l'authentification. Si vous supprimez le groupe, l'ASA utilise le nom d'utilisateur et le domaine (le cas échéant) pour l'authentification. Saisissez la commande **strip-realm** pour supprimer le qualificatif de domaine, et utilisez la commande **strip-group** pour supprimer le qualificatif de groupe du nom d'utilisateur lors de l'authentification. Si vous supprimez les deux qualificatifs, l'authentification est basée sur le *username* uniquement. Sinon, l'authentification est basée sur la chaîne complète *username@realm* ou *username<delimiter> group*. Vous devez préciser **strip-realm** si votre serveur ne peut pas analyser les délimiteurs.

### Étape 9

En option, si votre serveur est un serveur RADIUS, RADIUS avec NT ou LDAP, vous pouvez également activer la gestion des mots de passe.

#### Remarque

Si vous utilisez un serveur de répertoire LDAP pour l'authentification, la gestion des mots de passe est prise en charge avec le Sun Microsystems JAVA System Directory Server (anciennement nommé Sun ONE Directory Server) et Microsoft Active Directory.

Le DN configuré sur l'ASA pour accéder à un serveur de répertoire Sun doit pouvoir accéder à la politique de mot de passe par défaut sur ce serveur. Nous vous conseillons d'utiliser l'administrateur de répertoire ou un utilisateur disposant des privilèges d'administrateur de répertoire, comme DN. Vous pouvez également placer une ACI sur la politique de mot de passe par défaut.

Microsoft : vous devez configurer LDAP sur SSL pour activer la gestion des mots de passe avec Microsoft Active Directory.

Cette fonctionnalité, qui est désactivée par défaut, avertit un utilisateur lorsque le mot de passe actuel est sur le point d'expirer. La valeur par défaut est de commencer à avertir l'utilisateur 14 jours avant l'expiration :

```
hostname (config-tunnel-general) # password-management
hostname (config-tunnel-general) #
```

Si le serveur est un serveur LDAP, vous pouvez préciser le nombre de jours (de 0 à 180) avant l'expiration pour commencer à avertir l'utilisateur de l'expiration en attente :

```
hostname (config-tunnel-general) # password-management [password-expire in days n]
hostname (config-tunnel-general) #
```

#### Remarque

La commande **password-management**, saisie en mode de configuration des attributs généraux du groupe de tunnel, remplace la commande **radius-with-expiry** abandonnée qui était précédemment saisie en mode des attributs ipsec du groupe de tunnel.

Lorsque vous configurez cette commande **password-management**, l'ASA informe l'utilisateur distant lors de la connexion que le mot de passe actuel de l'utilisateur est sur le point d'expirer ou a expiré. L'ASA offre ensuite à l'utilisateur la possibilité de modifier le mot de passe. Si le mot de passe actuel n'a pas encore expiré, l'utilisateur peut toujours se connecter en utilisant ce mot de passe. L'ASA ignore cette commande si l'authentification RADIUS ou LDAP n'a pas été configurée.

Notez que cela ne modifie pas le nombre de jours avant l'expiration du mot de passe, mais plutôt le nombre de jours précédant l'expiration à partir duquel l'ASA commence à avertir l'utilisateur que le mot de passe est sur le point d'expirer.

Si vous spécifiez le mot-clé **password-expire-in-days**, vous devez également préciser le nombre de jours.

Le fait de préciser cette commande avec le nombre de jours défini à 0 désactive cette commande. L'ASA n'informe pas l'utilisateur de l'expiration en attente, mais l'utilisateur peut modifier le mot de passe après son expiration.

Consultez [Configurer les paramètres de Microsoft Active Directory pour la gestion des mots de passe, à la page 128](#) pour de plus amples renseignements.

La version 7.1 de l'ASA et les versions ultérieures prennent généralement en charge la gestion des mots de passe pour le client VPN AnyConnect, le client VPN Cisco IPsec, le client de tunnellation complète VPN SSL et les connexions sans client lors de l'authentification avec LDAP ou avec toute connexion RADIUS prenant en charge MS-CHAPv2. La gestion des mots de passe *n'est pas prise en charge* pour aucun de ces types de connexion pour Kerberos/AD (mot de passe Windows) ou le domaine NT 4.0.

Certains serveurs RADIUS qui prennent en charge MS-CHAP ne prennent actuellement pas en charge MS-CHAPv2. La commande **password-management** nécessite MS-CHAPv2, veuillez donc vérifier auprès de votre fournisseur.

#### Remarque

Le serveur RADIUS (par exemple, Cisco ACS) peut transmettre la demande d'authentification à un autre serveur d'authentification. Cependant, du point de vue de l'ASA, il ne communique qu'avec un serveur RADIUS.

Pour LDAP, la méthode de modification de mot de passe est propriétaire des différents serveurs LDAP du marché. Actuellement, l'ASA met en œuvre la logique de gestion des mots de passe propriétaire uniquement pour les serveurs Microsoft Active Directory et Sun LDAP. LDAP natif nécessite une connexion SSL. Vous devez activer LDAP sur SSL avant de tenter d'effectuer la gestion des mots de passe pour LDAP. Par défaut, LDAP utilise le port 636.

## Étape 10

## Étape 11

Précisez l'attribut ou les attributs à utiliser pour obtenir un nom pour une requête d'autorisation à partir d'un certificat. Cet attribut précise quelle partie du champ DN du sujet utiliser comme nom d'utilisateur pour l'autorisation :

```
hostname(config-tunnel-general)# authorization-dn-attributes {primary-attribute
[secondary-attribute] | use-entire-name}
```

Par exemple, la commande suivante spécifie l'utilisation de l'attribut CN comme nom d'utilisateur pour l'autorisation :

```
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(config-tunnel-general)#
```

Les attributs de authorization-dn-attributes sont **C** (Country), **CN** (Common Name), **DNQ** (DN qualifier), **EA** (E-mail Address), **GENQ** (Generational qualifier), **GN** (Given Name), **I** (Initials), **L** (Locality), **N** (Name), **O** (Organization), **OU** (Organizational Unit), **SER** (Serial Number), **SN** (Surname), **SP** (State/Province), **T** (Title), **UID** (User ID), et **UPN** (User Principal Name).

## Étape 12

Précisez s'il faut exiger une autorisation réussie avant de permettre à un utilisateur de se connecter. Par défaut, aucune autorisation n'est exigée.

```
hostname(config-tunnel-general)# authorization-required
hostname(config-tunnel-general)#
```

## Configurer de la double authentification

La double authentification est une fonctionnalité facultative qui oblige un utilisateur à saisir des informations d'authentification supplémentaires, telles qu'un deuxième nom d'utilisateur et un deuxième mot de passe, à l'écran de connexion. Précisez les commandes suivantes pour configurer la double authentification.

### Procédure

## Étape 1

Spécifiez le groupe de serveurs d'authentification secondaire. Cette commande spécifie le groupe de serveurs AAA à utiliser comme serveur AAA secondaire.

### Remarque

Cette commande s'applique uniquement aux connexions VPN AnyConnect.

Le groupe de serveurs secondaires ne peut pas préciser un groupe de serveurs SDI. Par défaut, l'authentification secondaire n'est pas requise.

```
hostname(config-tunnel-general)# secondary-authentication-server-group [interface_name]
{none | LOCAL | groupname [LOCAL]} [use-primary-name]
```

Si vous utilisez le mot-clé none (aucun), aucune authentification secondaire n'est requise. La valeur *groupname* spécifie le nom du groupe de serveurs AAA. Local spécifie l'utilisation de la base de données du serveur interne et, lorsqu'il est utilisé avec la valeur groupname, LOCAL spécifie le repli.

Par exemple, pour définir le groupe de serveurs d'authentification principal sur sdi\_group et le groupe de serveurs d'authentification secondaire sur ldap\_server, entrez les commandes suivantes :

```
hostname(config-tunnel-general)# authentication-server-group
hostname(config-tunnel-general)# secondary-authentication-server-group
```

### Remarque



Si vous utilisez le mot-clé **use-primary-name**, la boîte de dialogue de connexion ne demande qu'un seul nom d'utilisateur. En outre, si les noms d'utilisateurs sont extraits d'un certificat numérique, seul le nom d'utilisateur principal est utilisé pour l'authentification.

## Étape 2

Si vous obtenez le nom d'utilisateur secondaire à partir d'un certificat, saisissez **secondary-username-from-certificate** :

```
hostname(config-tunnel-general) # secondary-username-from-certificate C | CN | ... | use-script
```

Les valeurs des champs DN à extraire du certificat pour utilisation comme nom d'utilisateur secondaire sont les mêmes que pour la commande **username-from-certificate** principale. Vous pouvez également spécifier le mot-clé **use-script**, qui ordonne à l'ASA d'utiliser un fichier de script généré par ASDM.

Par exemple, pour spécifier le nom commun comme champ de nom d'utilisateur principal et l'unité organisationnelle comme champ de nom d'utilisateur secondaire, saisissez les commandes suivantes :

```
hostname(config-tunnel-general) # tunnel-group test1 general-attributes
hostname(config-tunnel-general) # username-from-certificate cn
hostname(config-tunnel-general) # secondary-username-from-certificate ou
```

## Étape 3

Utilisez la commande **secondary-pre-fill-username** en mode tunnel-group webvpn-attributes pour activer l'extraction d'un nom d'utilisateur secondaire d'un certificat client à utiliser dans l'authentification. Utilisez les mots-clés pour préciser si cette commande s'applique à une connexion sans client ou à une connexion de client VPN SSL (AnyConnect) et si vous souhaitez masquer le nom d'utilisateur extrait de l'utilisateur final. Par défaut, cette fonction est désactivée. Les options sans client et client SSL peuvent toutes deux exister en même temps, mais vous devez les configurer dans des commandes distinctes.

```
hostname(config-tunnel-general) # secondary-pre-fill-username-from-certificate
{clientless | client} [hide]
```

Par exemple, pour spécifier l'utilisation de **pre-fill-username** pour l'authentification principale et secondaire d'une connexion, entrez les commandes suivantes :

```
hostname(config-tunnel-general) # tunnel-group test1 general-attributes
hostname(config-tunnel-general) # pre-fill-username client
hostname(config-tunnel-general) # secondary-pre-fill-username client
```

## Étape 4

Précisez le serveur d'authentification à utiliser pour obtenir les attributs d'autorisation à appliquer à la connexion. Le serveur d'authentification principal est la sélection par défaut. Cette commande n'est significative que pour la double authentification.

```
hostname(config-tunnel-general) # authentication-attr-from-server {primary | secondary}
```

Par exemple, pour spécifier l'utilisation du serveur d'authentification secondaire, entrez les commandes suivantes :

```
hostname(config-tunnel-general) # tunnel-group test1 general-attributes
hostname(config-tunnel-general) # authentication-attr-from-server secondary
```

- Étape 5** Précisez le nom d'utilisateur d'authentification, principal ou secondaire, à associer à la session. La valeur par défaut est `primary` (principale). Lorsque la double authentification est activée, il est possible que deux noms d'utilisateur distincts soient authentifiés pour la session. L'administrateur doit désigner l'un des noms d'utilisateurs authentifiés comme nom d'utilisateur de la session. Le nom d'utilisateur de session est le nom d'utilisateur fourni pour la comptabilité, la base de données de session, les journaux système et la sortie de débogage.

```
hostname(config-tunnel-general)# authenticated-session-username {primary | secondary}
```

Par exemple, pour spécifier que le nom d'utilisateur d'authentification associé à la session doit provenir du serveur d'authentification secondaire, entrez les commandes suivantes :

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# authenticated-session-username secondary
```

## Configurer les attributs IPsec IKEv1 du profil de connexion d'accès à distance

Pour configurer les attributs IPsec IKEv1 d'un profil de connexion d'accès à distance, procédez comme suit. La description suivante suppose que vous avez déjà créé le profil de connexion d'accès à distance. Les profils de connexion d'accès à distance ont plus d'attributs que les profils de connexion LAN à LAN.

### Procédure

- Étape 1** Pour préciser les attributs IPsec d'un tunnel-group (groupe de tunnels) d'accès à distance, passez en mode `tunnel-group ipsec-attributes` en saisissant la commande suivante en mode de contexte unique ou multiple. L'invite change pour indiquer le changement de mode.

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

Cette commande passe en mode de configuration `tunnel-group ipsec-attributes`, dans lequel vous configurez les attributs IPsec du tunnel-group d'accès à distance en mode de contexte unique ou multiple.

Par exemple, la commande suivante indique que les commandes en mode `tunnel-group ipsec-attributes` qui suivent s'appliquent au profil de connexion nommé `TG1`. Remarquez que l'invite change pour indiquer que vous êtes maintenant en mode `ipsec-attributes` de groupe de tunnels :

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

- Étape 2** Précisez la clé prépartagée pour prendre en charge les connexions IKEv1 basées sur des clés prépartagées. Par exemple, la commande suivante spécifie la clé prépartagée `xyzx` pour prendre en charge les connexions IKEv1 pour un profil de connexion d'accès à distance IPsec IKEv1 :

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
```

```
hostname(config-tunnel-ipsec)#
```

**Étape 3** Précisez s'il faut valider l'identité de l'homologue à l'aide du certificat d'homologue :

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

Les valeurs *d'option* possibles sont **req** (required) (obligatoire), **cert** ((if supported by certificate) (si pris en charge par certificat) et **nocheck** (do not check) (ne pas vérifier). La valeur par défaut est **req**.

Par exemple, la commande suivante indique que la validation du peer-id (identifiant de l'homologue) est requise :

```
hostname(config-tunnel-ipsec)# peer-id-validate req
hostname(config-tunnel-ipsec)#
```

**Étape 4** Précisez s'il faut activer l'envoi d'une chaîne de certificats. La commande suivante inclut le certificat racine et tous les certificats d'autorité de certification subordonnés dans la transmission :

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

Cet attribut s'applique à tous les types de groupes de tunnels IPsec.

**Étape 5** Précisez le nom d'un point de confiance qui identifie le certificat à envoyer à l'homologue IKE :

```
hostname(config-tunnel-ipsec)# ikev1 trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

La commande suivante spécifie mytrustpoint comme nom du certificat à envoyer à l'homologue IKE :

```
hostname(config-ipsec)# ikev1 trust-point mytrustpoint
```

**Étape 6** Précisez le seuil des messages keepalive ISAKMP et le nombre de tentatives autorisées :

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

Le paramètre **threshold** spécifie le nombre de secondes (10 à 3600) pendant lesquelles l'homologue est autorisé à passer en inactivité avant de commencer la surveillance des messages keepalive. Le paramètre **retry** est l'intervalle (de 2 à 10 secondes) entre les tentatives après qu'une réponse keepalive n'a pas été reçue. Les messages keepalive IKE sont activés par défaut. Pour désactiver les messages keepalive ISAKMP, saisissez **isakmp keepalive disable**.

Par exemple, la commande suivante définit la valeur de seuil IKE keepalive à 15 secondes et définit l'intervalle de nouvelle tentative à 10 secondes :

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

La valeur par défaut du paramètre **threshold** est de 300 pour l'accès à distance et de 10 pour LAN à LAN, et la valeur par défaut du paramètre de nouvelle tentative est 2.

Pour spécifier que le site central (passerelle sécurisée) ne doit jamais lancer la surveillance ISAKMP, entrez la commande suivante :

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

### Étape 7 Précisez la méthode d'authentification hybride ISAKMP, XAUTH ou XAUTH hybride.

Vous utilisez la commande **isakmp ikev1-user-authentication** pour mettre en œuvre l'authentification hybride XAUTH lorsque vous devez utiliser des certificats numériques pour l'authentification ASA et une méthode existante différente pour l'authentification des utilisateurs VPN distants, comme RADIUS, TACACS+ ou SecurID. Hybrid XAUTH décompose la phase 1 d'IKE en deux étapes suivantes, ensemble appelées authentification hybride :

- L'ASA s'authentifie auprès de l'utilisateur VPN distant à l'aide des techniques de clé publique standard. Cela établit une association de sécurité IKE qui est authentifiée de manière unidirectionnelle.
- Un échange XAUTH authentifie ensuite l'utilisateur VPN distant. Cette authentification étendue peut utiliser l'une des méthodes d'authentification existantes prises en charge.

#### Remarque

Avant de pouvoir définir le type d'authentification sur hybride, vous devez configurer le serveur d'authentification, créer une clé prépartagée et configurer un point de confiance.

Vous pouvez utiliser la commande **isakmp ikev1-user-authentication** avec le paramètre interface facultatif pour spécifier une interface particulière. Lorsque vous omettez le paramètre d'interface, la commande s'applique à toutes les interfaces et sert de valeur de secours lorsque la commande par interface n'est pas spécifiée. Lorsque deux commandes **isakmp ikev1-user-authentication** sont spécifiées pour un profil de connexion et que l'une utilise le paramètre **d'interface** et l'autre ne le fait pas, celle qui spécifie l'interface a priorité pour cette interface particulière.

Par exemple, les commandes suivantes activent XAUTH hybride sur l'interface interne pour un profil de connexion appelé example-group :

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication (inside) hybrid
hostname(config-tunnel-ipsec)#
```

## Configurer les attributs PPP du profil de connexion à distance IPsec

Pour configurer les attributs du protocole de point à point d'un profil de connexion d'accès à distance, procédez comme suit. Les attributs PPP s'appliquent *uniquement* aux profils de connexion d'accès à distance IPsec. La description suivante suppose que vous ayez déjà créé le profil de connexion d'accès à distance IPsec.

## Procédure

**Étape 1** Entrez en mode de configuration tunnel-group ppp-attributes, dans lequel vous configurez les attributs PPP du groupe de tunnels d'accès à distance, en entrant la commande suivante. L'invite change pour indiquer le changement de mode :

```
hostname(config)# tunnel-group tunnel-group-name type remote-access
hostname(config)# tunnel-group tunnel-group-name ppp-attributes
hostname(config-tunnel-ppp)#
```

Par exemple, la commande suivante désigne que les commandes de mode ppp-attributes du groupe de tunnels qui suivent concernent le profil de connexion nommé TG1. Remarquez que l'invite change pour indiquer que vous êtes maintenant en mode tunnel-group ppp-attributes :

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ppp-attributes
hostname(config-tunnel-ppp)#
```

**Étape 2** Précisez s'il faut activer l'authentification à l'aide de protocoles spécifiques pour la connexion PPP. La valeur du protocole peut être l'une des suivantes :

- **pap** : active l'utilisation du Protocole d'authentification par mot de passe pour la connexion PPP.
- **chap** : active l'utilisation du Protocole d'authentification par défi pour la connexion PPP.
- **ms-chap-v1** ou **ms-chap-v2** : active l'utilisation du Protocole Microsoft d'authentification par défi, version 1 ou version 2 pour la connexion PPP.
- **eap** : active l'utilisation du protocole d'authentification extensible (EAP) pour la connexion PPP.

CHAP et MSCHAPv1 sont activés par défaut.

Voici la syntaxe de la commande :

```
hostname(config-tunnel-ppp)# authentication protocol
hostname(config-tunnel-ppp)#
```

Pour désactiver l'authentification pour un protocole en particulier, utilisez la forme **no** de la commande :

```
hostname(config-tunnel-ppp)# no authentication protocol
hostname(config-tunnel-ppp)#
```

Par exemple, la commande suivante active l'utilisation du protocole PAP pour une connexion PPP :

```
hostname(config-tunnel-ppp)# authentication pap
hostname(config-tunnel-ppp)#
```

La commande suivante permet l'utilisation du protocole MS-CHAP, version 2 pour une connexion PPP :

```
hostname(config-tunnel-ppp)# authentication ms-chap-v2
```

```
hostname (config-tunnel-ppp) #
```

La commande suivante permet l'utilisation du protocole EAP-PROXY pour une connexion PPP :

```
hostname (config-tunnel-ppp) # authentication pap
hostname (config-tunnel-ppp) #
```

La commande suivante désactive l'utilisation du protocole MS-CHAP, version 1 pour une connexion PPP :

```
hostname (config-tunnel-ppp) # no authentication ms-chap-v1
hostname (config-tunnel-ppp) #
```

## Configurer les profils de connexion LAN-à-LAN

Un profil de connexion VPN IPsec LAN à LAN s'applique uniquement aux connexions client IPsec LAN à LAN. Alors que de nombreux paramètres que vous configurez sont les mêmes que pour les profils de connexion d'accès à distance IPsec, les tunnels LAN à LAN ont moins de paramètres. Les sections suivantes vous montrent comment configurer un profil de connexion LAN à LAN :

- [Préciser un nom et un type pour un profil de connexion LAN à LAN, à la page 118](#)
- [Configurer les attributs généraux du profil de connexion LAN-à-LAN, à la page 119](#)
- [Configurer les attributs IPsec IKEv1 de site à site \(LAN à LAN\), à la page 119](#)

### Configurer le profil de connexion LAN à LAN par défaut

Le contenu du profil de connexion LAN à LAN par défaut est le suivant :

```
tunnel-group DefaultL2LGroup type ipsec-l2l
tunnel-group DefaultL2LGroup general-attributes
 default-group-policy DfltGrpPolicy
tunnel-group DefaultL2LGroup ipsec-attributes
 no ikev1 pre-shared-key
 peer-id-validate req
 no chain
 no ikev1 trust-point
 isakmp keepalive threshold 10 retry 2
```

Les profils de connexion de réseau local (LAN à réseau local) ont moins de paramètres que les profils de connexion d'accès à distance, et la plupart de ces paramètres sont les mêmes pour les deux groupes. Pour faciliter la configuration de la connexion, elles sont répertoriées séparément ici. Tous les paramètres que vous ne configurez pas explicitement héritent de leurs valeurs du profil de connexion par défaut.

### Préciser un nom et un type pour un profil de connexion LAN à LAN

Pour spécifier un nom et un type pour un profil de connexion, entrez la commande **tunnel-group**, comme suit :

```
hostname(config)# tunnel-group tunnel_group_name type tunnel_type
```

Pour un tunnel LAN à LAN, le type est **ipsec-l2l** ; par exemple, pour créer le profil de connexion LAN à LAN nommé docs, saisissez la commande suivante :

```
hostname(config)# tunnel-group docs type ipsec-l2l
hostname(config)#
```

## Configurer les attributs généraux du profil de connexion LAN-à-LAN

Pour configurer les attributs généraux du profil de connexion, procédez comme suit :

### Procédure

- Étape 1** Entrez en mode tunnel-group general-attributes en précisant le mot-clé general-attributes en mode contexte unique ou multiple :

```
tunnel-group tunnel-group-name general-attributes
```

**Exemple :**

Pour le profil de connexion nommé docs, entrez la commande suivante :

```
hostname(config)# tunnel-group docs general-attributes
hostname(config-tunnel-general)#
```

L'invite change pour indiquer que vous êtes maintenant en mode config-general, dans lequel vous configurez les attributs généraux du groupe de tunnels.

- Étape 2** Précisez le nom de la stratégie de groupe par défaut :

```
default-group-policy policynome
```

**Exemple :**

La commande suivante spécifie que le nom de la stratégie de groupe par défaut est MyPolicy :

```
hostname(config-tunnel-general)# default-group-policy MyPolicy
hostname(config-tunnel-general)#
```

## Configurer les attributs IPsec IKEv1 de site à site (LAN à LAN)

Pour configurer les attributs IPsec IKEv1, procédez comme suit :

## Procédure

- Étape 1** Pour configurer les attributs IPsec IKEv1 du groupe de tunnels, entrez en mode de configuration tunnel-group ipsec-attributes en utilisant la commande tunnel-group avec le mot-clé ipsec-attributes, en mode de contexte unique ou multiple.

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

Par exemple, la commande suivante passe en mode config-ipsec afin que vous puissiez configurer les paramètres du profil de connexion nommé TG1 :

```
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

L'invite change pour indiquer que vous êtes maintenant en mode de configuration ipsec-attributes de groupe de tunnels.

- Étape 2** Précisez la clé prépartagée pour prendre en charge les connexions IKEv1 basées sur des clés prépartagées.

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key key
hostname(config-tunnel-ipsec)#
```

Par exemple, la commande suivante spécifie la clé prépartagée XYZX pour prendre en charge les connexions IKEv1 pour un profil de connexion LAN-à-LAN :

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
hostname(config-tunnel-general)#
```

- Étape 3** Précisez s'il faut valider l'identité de l'homologue à l'aide du certificat d'homologue :

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

Les options disponibles sont **req** required (obligatoire), **cert** (if-supported (si pris en charge par certificat) et **nocheck** (do-not-check (ne pas vérifier). La valeur par défaut est **req**. Par exemple, la commande suivante définit l'option peer-id-validate à **nocheck** :

```
hostname(config-tunnel-ipsec)# peer-id-validate nocheck
hostname(config-tunnel-ipsec)#
```

- Étape 4** Précisez s'il faut activer l'envoi d'une chaîne de certificats. Cette action inclut le certificat racine et tous les certificats d'autorité de certification subordonnés dans la transmission :

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```



Vous pouvez appliquer cet attribut à tous les types de groupes de tunnels.

#### Étape 5

Précisez le nom d'un point de confiance qui identifie le certificat à envoyer à l'homologue IKE :

```
hostname(config-tunnel-ipsec)# trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

Par exemple, la commande suivante définit le nom du point de confiance comme mytrustpoint :

```
hostname(config-tunnel-ipsec)# trust-point mytrustpoint
hostname(config-tunnel-ipsec)#
```

Vous pouvez appliquer cet attribut à tous les types de groupes de tunnels.

#### Étape 6

Précisez le seuil keepalive d'ISAKMP (IKE) et le nombre de tentatives autorisées. Le paramètre **threshold** spécifie le nombre de secondes (10 à 3 600) pendant lesquelles l'homologue est autorisé à passer en inactivité avant de commencer la surveillance des messages keepalive. Le paramètre **retry** est l'intervalle (de 2 à 10 secondes) entre les tentatives après qu'une réponse keepalive n'a pas été reçue. Les messages keepalive IKE sont activés par défaut. Pour désactiver les messages keepalive IKE, saisissez la forme **no** de la commande **isakmp** :

```
hostname(config)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

Par exemple, la commande suivante définit le seuil ISAKMP keepalive à 15 secondes et définit l'intervalle de nouvelle tentative à 10 secondes :

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

La valeur par défaut du paramètre **threshold** pour LAN à LAN est 10 et la valeur par défaut du paramètre de nouvelle tentative est 2.

Pour spécifier que le site central (passerelle sécurisée) ne doit jamais lancer la surveillance ISAKMP, entrez la commande suivante :

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

#### Étape 7

Précisez la méthode d'authentification hybride ISAKMP, XAUTH ou XAUTH hybride.

Vous utilisez la commande **isakmp ikev1-user-authentication** pour mettre en œuvre l'authentification hybride XAUTH lorsque vous devez utiliser des certificats numériques pour l'authentification ASA et une méthode existante différente pour l'authentification des utilisateurs VPN distants, comme RADIUS, TACACS+ ou SecurID. Hybrid XAUTH décompose la phase 1 d'IKE en deux étapes suivantes, ensemble appelées authentification hybride :

- L'ASA s'authentifie auprès de l'utilisateur VPN distant à l'aide des techniques de clé publique standard. Cela établit une association de sécurité IKE qui est authentifiée de manière unidirectionnelle.
- Un échange XAUTH authentifie ensuite l'utilisateur VPN distant. Cette authentification étendue peut utiliser l'une des méthodes d'authentification existantes prises en charge.

**Remarque**

Avant de pouvoir définir le type d'authentification sur hybride, vous devez configurer le serveur d'authentification, créer une clé prépartagée et configurer un point de confiance.

Par exemple, les commandes suivantes activent XAUTH hybride pour un profil de connexion appelé example-group :

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication hybrid
hostname(config-tunnel-ipsec)#
```

## À propos des groupes de tunnels pour les clients IKEv2 basés sur les normes

Un groupe de tunnels est un ensemble d'enregistrements qui contiennent des politiques de connexion de tunnel. Vous configurez un groupe de tunnels pour identifier les serveurs AAA, préciser les paramètres de connexion et définir une stratégie de groupe par défaut. L'ASA stocke les groupes de tunnels en interne.

Le groupe de tunnels par défaut pour l'accès à distance IPsec est DefaultRAGroup. Vous pouvez modifier le groupe de tunnels par défaut, mais pas le supprimer.

IKEv2 permet la configuration de méthodes d'authentification asymétriques (c'est-à-dire l'authentification par clé prépartagée pour l'initiateur, mais l'authentification par certificat ou l'authentification EAP pour le répondeur) à l'aide d'interfaces de ligne de commande d'authentification locale et distante distinctes. Par conséquent, avec IKEv2, vous avez une authentification asymétrique, dans laquelle un côté s'authentifie avec un identifiant et l'autre côté utilise un autre identifiant (une clé prépartagée, un certificat ou un EAP).

Le groupe DefaultRAGroup doit être configuré pour l'authentification EAP, car ces connexions client ne peuvent pas être mappées à un groupe de tunnels spécifique, sauf si l'authentification par certificat est utilisée avec la correspondance du DN du certificat.

## Prise en charge des attributs IKEv2 basée sur les normes

L'ASA prend en charge les attributs IKEv2 suivants :

- INTERNAL\_IP4\_ADDRESS / INTERNAL\_IP6\_ADDRESS : adresse IPv4 ou IPv6

**Remarque**

La double pile (affectation d'une adresse IPv4 et IPv6) n'est pas prise en charge pour IKEv2. Si une adresse IPv4 et une adresse IPv6 sont demandées et que les deux adresses peuvent être attribuées, seule une adresse IPv4 est attribuée.

- INTERNAL\_IP4\_NETMASK : masque réseau d'adresses IPv4
- INTERNAL\_IP4\_DNS/INTERNAL\_IP6\_DNS : adresse DNS principale/secondaire
- INTERNAL\_IP4\_NBNS : adresse WINS principale/secondaire
- INTERNAL\_IP4\_SUBNET/INTERNAL\_IP6\_SUBNET : listes de tunnellation fractionnée

- `APPLICATION_VERSION` : ignoré. Aucune réponse n'est envoyée pour éviter de communiquer des informations de version sur l'ASA pour des raisons de sécurité. Cependant, la demande de charge utile de configuration du client peut inclure cet attribut, et la chaîne apparaît sur l'ASA dans la sortie de commande `vpn-sessiondb` et dans le journal système.

## Prise en charge DAP

Pour autoriser la configuration de politiques DAP par type de connexion, un nouveau type de client, IPsec-IKEv2-Generic-RA, peut être utilisé pour appliquer une politique propre à ce type de connexion.

## Sélection de groupe de tunnels pour les clients d'accès à distance

Le tableau suivant fournit une liste des clients d'accès à distance et des options de groupe de tunnels disponibles :

| Client d'accès à distance                 | Liste des groupes de tunnels | URL du groupe | Mise en correspondance du nom distinctif du certificat                                                                                                                            | Groupe par défaut (Groupe de RA par défaut)                                        | Autre |
|-------------------------------------------|------------------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|-------|
| Cisco AnyConnect VPN Client               | Oui                          | Oui           | Oui                                                                                                                                                                               | Oui                                                                                | S. O. |
| Windows L2TP/IPsec (Mode principal IKEv1) | Non                          | Non           | <ul style="list-style-type: none"> <li>• Oui (lors de l'utilisation de certificats de machine locale)</li> <li>• Non (lors de l'utilisation d'un protocole PSK)</li> </ul>        | Oui                                                                                | S. O. |
| IKEv2 basé sur les normes                 | Non                          | Non           | <ul style="list-style-type: none"> <li>• Oui (lors de l'utilisation de certificats de machine locale)</li> <li>• Non (lors de l'utilisation de l'authentification EAP)</li> </ul> | Oui<br><b>Remarque</b><br>Vous devez utiliser le groupe de tunnels DefaultRAGroup. | s.o.  |

## Prise en charge de l'authentification pour les clients IKEv2 basés sur les normes

Le tableau suivant fournit une liste des clients IKEv2 basés sur les normes et les méthodes d'authentification prises en charge :



### Remarque

Les limites de la méthode d'authentification sont basées sur le manque de prise en charge sur le client, et non sur l'ASA. Toute l'authentification EAP est relayée par l'ASA en tant que proxy entre le client et le serveur EAP. La prise en charge des méthodes EAP dépend du client et du serveur EAP pour la méthode EAP.

| Type de client/Méthode d'authentification | EAP-TLS                                                                                                                                           | EAP-MSCHAPv2                                                                                                                                      | EAP-MD5                                                                                                                                           | Certificat uniquement | PSK  |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|------|
| StrongSwan sur Linux                      | S. O.                                                                                                                                             | <ul style="list-style-type: none"> <li>• ISE : oui</li> <li>• ACS : oui</li> <li>• FreeRadius : oui</li> <li>• AD via FreeRadius : oui</li> </ul> | <ul style="list-style-type: none"> <li>• ISE : oui</li> <li>• ACS : oui</li> <li>• FreeRadius : oui</li> <li>• AD via FreeRadius : oui</li> </ul> | Oui                   | Oui  |
| StrongSwan sur Android                    | S. O.                                                                                                                                             | <ul style="list-style-type: none"> <li>• ISE : oui</li> <li>• ACS : oui</li> <li>• FreeRadius : oui</li> <li>• AD via FreeRadius : oui</li> </ul> | Non                                                                                                                                               | Oui                   | S.O. |
| Windows 7/8/8.1                           | <ul style="list-style-type: none"> <li>• ISE : oui</li> <li>• ACS : oui</li> <li>• FreeRadius : oui</li> <li>• AD via FreeRadius : oui</li> </ul> | <ul style="list-style-type: none"> <li>• ISE : oui</li> <li>• ACS : oui</li> <li>• FreeRadius : oui</li> <li>• AD via FreeRadius : oui</li> </ul> | s.o.                                                                                                                                              | Oui                   | S.O. |
| Windows Phone                             | <ul style="list-style-type: none"> <li>• ISE : oui</li> <li>• ACS : oui</li> <li>• FreeRadius : oui</li> <li>• AD via FreeRadius : oui</li> </ul> | <ul style="list-style-type: none"> <li>• ISE : oui</li> <li>• ACS : oui</li> <li>• FreeRadius : oui</li> <li>• AD via FreeRadius - Oui</li> </ul> | s.o.                                                                                                                                              | s.o.                  | s.o. |

| Type de client/Méthode d'authentification | EAP-TLS                                                                                                                                           | EAP-MSCHAPv2                                                                                                                                      | EAP-MD5                                                                                                                                           | Certificat uniquement | PSK   |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-------|
| Samsung Knox                              | S. O.                                                                                                                                             | <ul style="list-style-type: none"> <li>• ISE : oui</li> <li>• ACS : oui</li> <li>• FreeRadius : oui</li> <li>• AD via FreeRadius - Oui</li> </ul> | <ul style="list-style-type: none"> <li>• ISE : oui</li> <li>• ACS : oui</li> <li>• FreeRadius : oui</li> <li>• AD via FreeRadius - Oui</li> </ul> | Oui                   | S. O. |
| iOS 8                                     | <ul style="list-style-type: none"> <li>• ISE : oui</li> <li>• ACS : oui</li> <li>• FreeRadius : oui</li> <li>• AD via FreeRadius - Oui</li> </ul> | <ul style="list-style-type: none"> <li>• ISE : oui</li> <li>• ACS : oui</li> <li>• FreeRadius : oui</li> <li>• AD via FreeRadius : oui</li> </ul> | S. O.                                                                                                                                             | Oui                   | Oui   |
| Client natif Android                      | S. O.                                                                                                                                             | <ul style="list-style-type: none"> <li>• ISE : oui</li> <li>• ACS : oui</li> <li>• FreeRadius : oui</li> <li>• AD via FreeRadius</li> </ul>       | S. O.                                                                                                                                             | Oui                   | Oui   |

## Authentification de plusieurs certificats

Le protocole d'authentification agrégé a été étendu pour définir l'échange de protocole pour l'authentification à certificats multiples et l'utiliser pour les deux types de sessions. Une fois que le client a établi une connexion SSL et est entré dans l'authentification agrégée, une autre connexion SSL est établie et l'ASA voit que le client nécessite une authentification par certificat et demande le certificat client.

L'ASA configure l'authentification requise pour une connexion Secure Client (services client sécurisés) d'un groupe de tunnels de type accès à distance. Un mappage de groupe de tunnels est effectué avec les méthodes existantes telles que le mappage de règle de certificat, l'URL de groupe, etc., mais les méthodes d'authentification requises sont négociées avec le client.

### Exemple

groupe de tunnels <name> attributs-webvpn

```
authentication {aaa [certificat | certificat multiple] | certificat multiple [aaa | saml] | saml [certificat | certificat multiple]}
```

Les options d'authentification sont AAA uniquement, certificat uniquement, certificats multiples uniquement, AAA et certificat, AAA et certificats multiples, SAML, SAML et certificat, ou certificats multiples et SAML.

```
ASA(config)# tunnel-group AnyConnect webvpn-attributes
ASA(config-tunnel-webvpn)# authentication?
tunnel-group-webvpn mode commands/options:
aaa Use username and password for authentication
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
saml Use SAML for authentication
ASA(config-tunnel-webvpn)# authentication multiple-certificate?

tunnel-group-webvpn mode commands/options:
aaa Use username and password for authentication
saml Use SAML for authentication
<cr>

ASA(config-tunnel-webvpn)# authentication aaa?

tunnel-group-webvpn mode commands/options:
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
<cr>ASA(config-tunnel-webvpn)# authentication aaa?

ASA(config-tunnel-webvpn)# authentication saml?
tunnel-group-webvpn mode commands/options:
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
<cr>
```

## Configurer l'option query-identity pour la récupération de l'identité EAP

Le client Microsoft Windows 7 IKEv2 envoie une adresse IP comme identité Internet Key Exchange (IKE), ce qui empêche le serveur Cisco ASA de l'utiliser efficacement pour la recherche du groupe de tunnels. L'ASA doit être configuré avec l'option **query-identity** pour l'authentification EAP afin de permettre à l'ASA de récupérer une identité EAP valide du client.

Pour l'authentification basée sur les certificats, le serveur ASA et les certificats client Microsoft Windows 7 doivent comporter un champ Extended Key Usage (EKU) comme suit :

- Pour le certificat client, champ EKU = certificat d'authentification du client.
- Pour le certificat de serveur, champ EKU = certificat d'authentification du serveur.

Vous pouvez obtenir les certificats auprès du serveur de certificats Microsoft ou d'un autre serveur d'autorité de certification.

Pour l'authentification EAP, le client Microsoft Windows 7 IKEv2 attend une demande d'identité EAP avant toute autre demande EAP. Assurez-vous de configurer le mot-clé **query-identity** dans le profil de groupe de tunnels sur le serveur ASA IKEv2 afin d'envoyer au client une demande d'identité EAP.



### Remarque

L'interception DHCP est prise en charge pour IKEv2 afin de permettre à Windows d'effectuer la tunnellation fractionnée. Cette fonctionnalité ne fonctionne qu'avec les attributs de tunnellation fractionnée IPv4.

## Procédure

**Étape 1** Pour définir le type de connexion sur l'accès à distance IPsec, saisissez la commande **tunnel-group**. La syntaxe est **tunnel-group nom type**, où nom est le nom que vous attribuez au groupe de tunnels, et type est le type de tunnel.

Dans l'exemple suivant, la clé prépartagée IKEv2 est configurée comme suit : 44kkaol59636jnfx

```
hostname(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 44kkaol59636jnfx
```

### Remarque

Vous devez configurer la commande **ikev2 remote-authentication pre-shared-key** ou la commande **ikev2 remote-authentication certificate** pour terminer l'authentification.

**Étape 2** Pour préciser le protocole EAP (Extensible Authentication Protocol) comme méthode prenant en charge l'authentification des utilisateurs avec des clients tiers d'accès à distance IKEv2 conformes aux normes, utilisez la commande **ikev2 remote-authentication eap [query-identity]**.

### Remarque

Avant de pouvoir activer EAP pour l'authentification à distance, vous devez configurer l'authentification locale à l'aide d'un certificat et configurer un point de confiance valide à l'aide de la commande **ikev2 local-authentication {certificate trustpoint}**. Sinon, la demande d'authentification EAP est rejetée.

Vous pouvez configurer plusieurs options qui permettent au client d'utiliser n'importe laquelle des options configurées, mais non pas toutes, pour l'authentification à distance.

Pour les connexions IKEv2, le mappage du groupe de tunnels doit déterminer quelles méthodes d'authentification autoriser pour l'authentification à distance (PSK, certificat et EAP) et pour l'authentification locale (PSK et certificat), ainsi que le point de confiance à utiliser pour l'authentification locale. Actuellement, le mappage est effectué à l'aide de l'ID IKE, extrait de la valeur du champ de l'homologue ou du certificat homologue au moyen de la carte de certificats. Si les deux options échouent, la connexion entrante est mappée au groupe de tunnels d'accès à distance par défaut, DefaultRAGroup. Une carte de certificats est une option applicable uniquement lorsque l'homologue distant est authentifié par un certificat. Cette carte permet le mappage vers différents groupes de tunnels. Pour l'authentification par certificat uniquement, la recherche de groupe de tunnels est effectuée à l'aide de règles ou à l'aide du paramètre par défaut. Pour l'authentification EAP et PSK, la recherche du groupe de tunnels est effectuée à l'aide de l'ID IKE sur le client, lequel correspond au nom du groupe de tunnels, ou à l'aide du paramètre par défaut.

Pour l'authentification EAP, vous devez utiliser le groupe de tunnels DefaultRAGroup, sauf si le client autorise la configuration indépendante de l'identifiant IKE et du nom d'utilisateur.

L'exemple suivant montre le refus d'une demande EAP d'authentification :

```
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 12345678
ERROR: The local-authentication method is required to be certificate based
if remote-authentication allows EAP
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

**Étape 3** Enregistrez vos modifications.

```
hostname(config)# write memory
hostname(config)#
```

Pour vérifier que le tunnel est établi et fonctionnel, utilisez la commande **show vpn-sessiondb summary** ou **show crypto ipsec sa**.

## Configurer les paramètres de Microsoft Active Directory pour la gestion des mots de passe

Si vous utilisez un serveur de répertoire LDAP pour l'authentification, la gestion des mots de passe est prise en charge avec le Sun Microsystems JAVA System Directory Server (anciennement nommé Sun ONE Directory Server) et Microsoft Active Directory.

- Sun : le DN configuré sur l'ASA pour accéder à un serveur de répertoire Sun doit pouvoir accéder à la politique de mot de passe par défaut sur ce serveur. Nous vous conseillons d'utiliser l'administrateur de répertoire ou un utilisateur disposant des privilèges d'administrateur de répertoire, comme DN. Vous pouvez également placer une ACI sur la politique de mot de passe par défaut.
- Microsoft : vous devez configurer LDAP sur SSL pour activer la gestion des mots de passe avec Microsoft Active Directory.

Pour utiliser la gestion des mots de passe avec Microsoft Active Directory, vous devez définir certains paramètres Active Directory et configurer également la gestion des mots de passe sur l'ASA. Cette section décrit les paramètres Active Directory associés à diverses actions de gestion de mots de passe. Ces descriptions supposent que vous ayez également activé la gestion des mots de passe sur l'ASA et configuré les attributs correspondants de gestion des mots de passe. Les étapes précises de cette section renvoient à la terminologie Active Directory sous Windows 2000. Cette section suppose que vous utilisez un serveur de répertoire LDAP pour l'authentification.

## Utiliser Active Directory pour forcer l'utilisateur à modifier le mot de passe lors de la prochaine connexion

Pour forcer un utilisateur à modifier le mot de passe d'utilisateur lors de la connexion suivante, spécifiez la commande **password-management** en mode de configuration des attributs généraux du groupe de tunnels sur l'ASA et effectuez les étapes suivantes sous Active Directory :

### Procédure

- |                |                                                                                                                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Étape 1</b> | Choisissez <b>Start (Démarrer) &gt; Programs (Programmes) &gt; Administrative Tools (Outils d'administration) &gt; Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory)</b> . |
| <b>Étape 2</b> | Cliquez avec le bouton droit pour choisir <b>Username (Nom d'utilisateur) &gt; Username (Nom d'utilisateur) &gt; Account (Compte)</b> .                                                                      |
| <b>Étape 3</b> | Cochez la case <b>User must change password at next logon</b> (L'utilisateur doit changer le mot de passe à la prochaine connexion).                                                                         |



Lors de la prochaine connexion de cet utilisateur, l'ASA affiche l'invite suivante : « New password required (Nouveau mot de passe requis). Changement de mot de passe requis You must enter a new password with a minimum length  $n$  to continue ». (Vous devez saisir un nouveau mot de passe d'une longueur minimale de  $n$  pour continuer.) Vous pouvez définir la longueur minimale de mot de passe requise,  $n$ , dans le cadre de la configuration Active Directory en accédant à Start (Démarrer) > Programs (Programmes) > Administrative Tools (Outils d'administration) > Domain Security Policy (Politique de sécurité de domaine) > Windows Settings (Paramètres Windows) > Security Settings (Paramètres de sécurité) > Account Policies (Politiques de compte) > Password Policy (Politique de mot de passe). Sélectionnez **Minimum password length** (Longueur minimale du mot de passe).

## Utiliser Active Directory pour préciser l'ancienneté maximale du mot de passe

Pour renforcer la sécurité, vous pouvez spécifier que les mots de passe expirent après un certain nombre de jours. Pour spécifier un âge de mot de passe maximal pour un mot de passe d'utilisateur, spécifiez la commande **password-management** en mode de configuration d'attributs généraux de groupe de tunnel sur l'ASA et effectuez les étapes suivantes sous Active Directory :



### Remarque

La commande **radius-with-expiry**, précédemment configurée dans le cadre de la configuration tunnel-group remote-access pour gérer l'âge du mot de passe, est obsolète. La commande **password-management**, saisie en mode tunnel-group general-attributes, la remplace.

### Procédure

- Étape 1** Choisissez Start (Démarrer) > Programs (Programmes) > Administrative Tools (Outils d'administration) , > Domain Security Policy (Politique de sécurité du domaine) > Windows Settings (Paramètres Windows) , > Security Settings (Paramètres de sécurité) , > Account Policies (Politiques de compte) , > Password Policy (Politique de mot de passe).
- Étape 2** Double-cliquez sur Âge maximal du mot de passe.
- Étape 3** Cochez la case **Define this policy setting** (Définir ce paramètre de politique) et précisez l'âge maximal du mot de passe, en jours, que vous souhaitez autoriser.

## Utiliser Active Directory pour appliquer la longueur minimale du mot de passe

Pour appliquer une longueur minimale pour les mots de passe, spécifiez la commande **password-management** en mode de configuration d'attributs généraux de groupe de tunnels sur l'ASA et effectuez les étapes suivantes sous Active Directory :

### Procédure

- Étape 1** Choisissez Start (Démarrer) > Programs (Programmes) > Administrative Tools (Outils administratifs) > Domain Security Policy (Stratégie de sécurité du domaine).

- Étape 2** Choisissez **Paramètres de Windows > Paramètres de sécurité > Politiques de compte > Politique de mot de passe**.
- Étape 3** Double-cliquez sur **Minimum Password Length** (Longueur minimale du mot de passe).
- Étape 4** Cochez la case **Define this policy setting** (Définir ce paramètre de politique), puis indiquez le nombre minimal de caractères requis pour le mot de passe.

## Utiliser Active Directory pour appliquer la complexité du mot de passe

Pour appliquer des mots de passe complexes, par exemple, pour exiger qu'un mot de passe contienne des lettres majuscules et minuscules, des chiffres et des caractères spéciaux, saisissez la commande **password-management** en mode de configuration des attributs généraux du groupe de tunnels sur l'ASA et effectuez les étapes suivantes sous Active Directory :

### Procédure

- Étape 1** Choisissez **Start (Démarrer) > Programs (Programmes) > Administrative Tools (Outils d'administration) > Domain Security Policy (Politique de sécurité du domaine)**. Sélectionnez **Windows Settings (Paramètres Windows) > Security Settings (Paramètres de sécurité) > Account Policies (Politiques de compte) > Password Policy (Politique de mot de passe)**.
- Étape 2** Double-cliquez sur **Password must meet complexity requirements** (Le mot de passe doit respecter les exigences de complexité) pour ouvrir la boîte de dialogue **Security Policy Setting** (Paramètre de stratégie de sécurité).
- Étape 3** Cochez la case **Define this policy setting** (Définir ce paramètre de politique) et sélectionnez **Enable** (Activer).

L'application de la complexité des mots de passe ne prend effet que lorsque l'utilisateur modifie son mot de passe ; par exemple, lorsque vous avez configuré **Enforce password change at next login** (Forcer le changement de mot de passe à la prochaine ouverture de session) ou **Password expires in *n* days** (Le mot de passe expire dans *n* jours). Au moment de la connexion, l'utilisateur reçoit un message pour saisir un nouveau mot de passe, et le système n'acceptera qu'un mot de passe complexe.

## Configurer le profil de connexion pour la prise en charge des messages RADIUS/SDI pour Secure Client (services client sécurisés)

Cette section décrit les procédures pour s'assurer que le client VPN AnyConnect utilisant des jetons du logiciel RSA SecureID peut répondre correctement aux invites d'utilisateur fournies au client par l'intermédiaire d'un proxy RADIUS vers un ou plusieurs serveurs SDI.



### Remarque

Si vous avez configuré la fonctionnalité de double authentification, l'authentification SDI est prise en charge uniquement sur le serveur d'authentification principal.

Lorsqu'un utilisateur distant se connecte à l'ASA avec le client VPN AnyConnect et tente de s'authentifier à l'aide d'un jeton RSA SecurID, l'ASA communique avec le serveur RADIUS, qui à son tour, communique avec le serveur SDI au sujet de l'authentification.

Lors de l'authentification, le serveur RADIUS présente des messages de défi d'accès à l'ASA. Ces messages de défi comprennent des messages de réponse contenant du texte du serveur SDI. Le texte du message est différent lorsque l'ASA communique directement avec un serveur SDI que lorsqu'il communique par l'intermédiaire du proxy RADIUS. Par conséquent, afin d'apparaître en tant que serveur SDI natif auprès du Secure Client (services client sécurisés), l'ASA doit interpréter les messages du serveur RADIUS.

De plus, comme les messages SDI sont configurables sur le serveur SDI, le texte du message sur l'ASA doit correspondre (en tout ou en partie) au texte du message sur le serveur SDI. Sinon, les invites affichées à l'utilisateur du client distant peuvent ne pas être appropriées pour l'action requise lors de l'authentification. Le Secure Client (services client sécurisés) peut ne pas répondre et l'authentification peut échouer.

[Configurer l'appareil de sécurité pour prendre en charge les messages RADIUS/SDI, à la page 131](#) décrit comment configurer l'ASA pour assurer une authentification réussie entre le client et le serveur SDI.

## Configurer l'appareil de sécurité pour prendre en charge les messages RADIUS/SDI

Pour configurer l'ASA afin qu'il interprète les messages de réponse RADIUS propres à SDI et invite l'utilisateur Secure Client (services client sécurisés) à prendre la mesure appropriée, procédez comme suit :

### Procédure

#### Étape 1

Configurez un profil de connexion (groupe de tunnels) pour transférer les messages de réponse RADIUS de manière à simuler une communication directe avec un serveur SDI à l'aide de la commande **proxy-auth sdi**, en mode de configuration tunnel-group webvpn. Les utilisateurs s'authentifiant auprès du serveur SDI doivent se connecter sur ce profil de connexion.

#### Exemple :

```
hostname(config)# tunnel-group sales webvpn attributes
hostname(tunnel-group-webvpn)# proxy-auth sdi
```

#### Étape 2

Configurez sur l'ASA le texte du message de réponse RADIUS pour qu'il corresponde, en tout ou en partie, au texte du message envoyé par le serveur RADIUS à l'aide de la commande **proxy-auth\_map sdi**, en mode de configuration tunnel-group webvpn.

Le texte du message par défaut utilisé par l'ASA est le texte du message par défaut utilisé par le serveur Cisco Secure Access Control Server (ACS). Si vous utilisez Cisco Secure ACS et qu'il utilise le texte de message par défaut, vous n'avez pas besoin de configurer le texte de message sur l'ASA. Sinon, utilisez la commande **proxy-auth\_map sdi** pour vous assurer que le texte du message correspond.

Le tableau ci-dessous présente le code de message, le texte du message de réponse RADIUS par défaut et la fonction de chaque message. Comme l'appareil de sécurité recherche les chaînes dans l'ordre où elles apparaissent dans le tableau, vous devez vous assurer que la chaîne utilisée pour le texte du message n'est pas un sous-ensemble d'une autre chaîne.

Par exemple, « nouveau NIP » est un sous-ensemble du texte de message par défaut pour new-pin-sup et next-ccode-and-reauth. Si vous configurez new-pin-sup comme « nouveau NIP », lorsque l'appareil de sécurité reçoit « nouveau NIP avec le code de carte suivant » du serveur RADIUS, il fera correspondre le texte au code new-pin-sup plutôt qu'au code next-ccode-and-reauth.

Codes d'opération SDI, texte du message par défaut et fonction du message

| Code de message      | Texte du message de réponse RADIUS par défaut | Fonction                                                                                                                                                                           |
|----------------------|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| code suivant         | Veuillez entrer le code d'accès suivant       | Indique que l'utilisateur doit saisir le NEXT tokencode sans le NIP.                                                                                                               |
| new-pin-sup          | N'oubliez pas votre nouveau NIP               | Indique que le nouveau NIP système a été fourni et affiche ce NIP pour l'utilisateur.                                                                                              |
| new-pin-meth         | Voulez-vous saisir votre propre code NIP      | Demande à l'utilisateur quelle nouvelle méthode de code NIP utiliser pour créer un nouveau NIP.                                                                                    |
| new-pin-req          | Entrez votre nouveau NIP alphanumérique       | Indique un NIP généré par l'utilisateur et demande à l'utilisateur de saisir le NIP.                                                                                               |
| new-pin-reenter      | Saisir de nouveau le NIP :                    | Utilisé en interne par l'ASA pour la confirmation du NIP fourni par l'utilisateur. Le client confirme le NIP sans demander à l'utilisateur de le saisir.                           |
| new-pin-sys-ok       | Nouveau NIP accepté                           | Indique que le NIP fourni par l'utilisateur a été accepté.                                                                                                                         |
| next-code-and-reauth | nouveau NIP avec le code de carte suivant     | Fait suite à une opération de NIP et indique que l'utilisateur doit attendre le prochain tokencode et saisir à la fois le nouveau NIP et le tokencode suivant pour s'authentifier. |
| ready-for-sys-pin    | Accepter un NIP généré par le système         | Utilisé en interne par l'ASA pour indiquer que l'utilisateur est prêt à recevoir le NIP généré par le système.                                                                     |

L'exemple suivant passe en mode `aaa-server-host` et modifie le texte du message de réponse RADIUS `new-pin-sup` :

```
hostname(config)# aaa-server radius_sales host 10.10.10.1
hostname(config-aaa-server-host)# proxy-auth_map sdi new-pin-sup "This is your new PIN"
```

## Stratégies de groupe

Cette section décrit les stratégies de groupe et comment les configurer.

Une stratégie de groupe est un ensemble de paires d'attributs/valeurs orientées utilisateur pour les connexions IPsec qui sont stockées en interne (localement) sur le périphérique ou en externe sur un serveur RADIUS. Le profil de connexion utilise une politique de groupe qui définit les conditions de connexions des utilisateurs après l'établissement du tunnel. Les stratégies de groupe vous permettent d'appliquer des ensembles complets d'attributs à un utilisateur ou à un groupe d'utilisateurs, plutôt que d'avoir à spécifier chaque attribut individuellement pour chaque utilisateur.

Saisissez les commandes **group-policy** en mode de configuration globale pour affecter une stratégie de groupe aux utilisateurs ou pour modifier une stratégie de groupe pour des utilisateurs spécifiques.

L'ASA comprend une stratégie de groupe par défaut. En plus de la stratégie de groupe par défaut, que vous pouvez modifier mais pas supprimer, vous pouvez créer une ou plusieurs stratégies de groupe spécifiques à votre environnement.

Vous pouvez configurer des stratégies de groupe internes et externes. Les groupes internes sont configurés sur la base de données interne de l'ASA. Les groupes externes sont configurés sur un serveur d'authentification externe, tel que RADIUS. Les stratégies de groupe comprennent les attributs suivants :

- Identité
- Définitions de serveur
- Paramètres de pare-feu client
- Protocoles de tunnelisation
- Paramètres IPsec
- Paramètres matériels
- Filtres
- Paramètres de configuration client
- Paramètres de connexion

## Modifier la stratégie de groupe par défaut

L'ASA fournit une stratégie de groupe par défaut. Vous pouvez modifier cette stratégie de groupe par défaut, mais vous ne pouvez pas la supprimer. Une stratégie de groupe par défaut, nommée `DfltGrpPolicy`, existe toujours sur l'ASA, mais cette stratégie de groupe par défaut ne prend effet que si vous configurez l'ASA pour l'utiliser. Lorsque vous configurez d'autres stratégies de groupe, tout attribut que vous ne spécifiez pas explicitement hérite de sa valeur de la stratégie de groupe par défaut.



### Remarque

Les profils Secure Client (services client sécurisés), y compris tout ou tous les types de profils Secure Client (services client sécurisés) (comme Network Access Manager, Umbrella, etc.) configurés sur `DfltGrpPolicy` (et qui lui sont affectés) ne sont pas hérités par d'autres stratégies de groupe, sauf si les autres stratégies de groupe sont explicitement configurées pour hériter de `DfltGrpPolicy`. En d'autres termes, les profils Secure Client (services client sécurisés) associés à `DfltGrpPolicy` ne sont pas hérités lorsque des profils Secure Client (services client sécurisés) spécifiques sont configurés dans une stratégie de groupe.

Pour afficher la stratégie de groupe par défaut, saisissez la commande suivante :

```
hostname(config)# show running-config all group-policy DfltGrpPolicy
hostname(config)#
```

Pour configurer la stratégie de groupe par défaut, saisissez la commande suivante :

```
hostname(config)# group-policy DfltGrpPolicy internal
hostname(config)#
```



**Remarque** La stratégie de groupe par défaut est toujours interne. Malgré le fait que la syntaxe de la commande est `hostname(config)# group-policy DfltGrpPolicy {internal | external}`, vous ne pouvez pas modifier son type en externe.

Pour modifier l'un des attributs de la stratégie de groupe par défaut, utilisez la commande **group-policy attributes** pour passer en mode attributs, puis précisez les commandes pour modifier les attributs souhaités :

```
hostname(config)# group-policy DfltGrpPolicy attributes
```



**Remarque** Le mode d'attributs s'applique uniquement aux stratégies de groupe internes.

La stratégie de groupe par défaut, DfltGrpPolicy, que fournit l'ASA est la suivante :

```
hostname# show run all group-policy DfltGrpPolicy
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 wins-server none
 dns-server value 10.10.10.1.1
 dhcp-network-scope none
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-idle-timeout alert-interval 1
 vpn-session-timeout none
 vpn-session-timeout alert-interval 1
 vpn-filter none
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client

password-storage disable
ip-comp disable
re-xauth disable
group-lock none
pfs disable
ipsec-udp disable
ipsec-udp-port 10000
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain value cisco.com
split-dns none
split-tunnel-all-dns disable
intercept-dhcp 255.255.255.255 disable
secure-unit-authentication disable
user-authentication disable
user-authentication-idle-timeout 30
ip-phone-bypass disable
client-bypass-protocol disable
gateway-fqdn none
leap-bypass disable
nem disable
backup-servers keep-client-config
msie-proxy server none
msie-proxy method no-modify
```

```

msie-proxy except-list none
msie-proxy local-bypass disable
msie-proxy pac-url none
msie-proxy lockdown enable
vlan none
nac-settings none
address-pools none
ipv6-address-pools none
smartcard-removal-disconnect enable
scep-forwarding-url none
client-firewall none
client-access-rule none
webvpn
 url-list none
 filter none
 homepage none
 html-content-filter none

http-proxy disable

anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface private none
anyconnect firewall-rule client-interface public none
anyconnect keep-installer installed
anyconnect ssl keepalive 20
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression lzs
anyconnect modules none
anyconnect profiles none
anyconnect ask none
customization none
keep-alive-ignore 4
http-comp gzip
download-max-size 2147483647
upload-max-size 2147483647
post-max-size 2147483647
user-storage none
storage-objects value cookies,credentials
storage-key none
hidden-shares none

activex-relay enable
unix-auth-uid 65534
unix-auth-gid 65534
file-entry enable
file-browsing enable
url-entry enable
deny-message value Login was successful, but because certain criteria have not been met
or due to some specific group policy, you do not have permission to use any of the VPN
features. Contact your IT administrator for more information

anyconnect ssl df-bit-ignore disable
anyconnect routing-filtering-ignore disable

always-on-vpn profile-setting

```

Vous pouvez modifier la stratégie de groupe par défaut et vous pouvez également créer une ou plusieurs stratégies de groupe spécifiques à votre environnement.

## Configurer les stratégies de groupe

Une stratégie de groupe peut s'appliquer à tout type de tunnel. Dans chaque cas, si vous ne définissez pas explicitement de paramètre, le groupe prend la valeur de la stratégie de groupe par défaut.

Vous pouvez effectuer ces tâches de configuration en mode contexte unique ou en mode multi-contexte :



### Remarque

Le mode multi-contexte s'applique uniquement aux connexions site à site IKEv2 et IKEv1 et ne s'applique pas à AnyConnect, au VPN SSL sans client, au client VPN natif Apple, au client VPN natif Microsoft ou à cTCP pour IKEv1 IPsec.

## Configurer une stratégie de groupe externe

Les stratégies de groupe externes tirent leurs valeurs d'attribut du serveur externe que vous spécifiez. Pour une stratégie de groupe externe, vous devez identifier le groupe de serveurs AAA que l'ASA peut interroger pour les attributs et préciser le mot de passe à utiliser lors de la récupération des attributs du groupe de serveurs AAA externe. Si vous utilisez un serveur d'authentification externe et si vos attributs de stratégie de groupe externes existent dans le même serveur RADIUS que les utilisateurs que vous prévoyez d'authentifier, vous devez vous assurer qu'il n'y a pas de duplication de nom entre eux.



### Remarque

Les noms de groupes externes sur l'ASA font référence aux noms d'utilisateur sur le serveur RADIUS. En d'autres termes, si vous configurez le groupe externe X sur l'ASA, le serveur RADIUS voit la requête comme une demande d'authentification pour l'utilisateur X. Ainsi, les groupes externes ne sont en fait que des comptes d'utilisateurs sur le serveur RADIUS qui ont une signification particulière pour l'ASA. Si vos attributs de groupe externe existent dans le même serveur RADIUS que les utilisateurs que vous prévoyez d'authentifier, il ne doit y avoir aucune duplication de nom entre eux.

L'ASA prend en charge l'autorisation utilisateur sur un serveur LDAP ou RADIUS externe. Avant de configurer l'ASA pour utiliser un serveur externe, vous devez configurer le serveur avec les attributs d'autorisation ASA appropriés et, à partir d'un sous-ensemble de ces attributs, attribuer des autorisations spécifiques aux utilisateurs individuels. Suivez les instructions dans [Configurer un serveur AAA externe pour le VPN](#), à la page 295 pour configurer votre serveur externe.

## Procédure

Pour configurer une stratégie de groupe externe, effectuez l'étape suivante et spécifiez un nom et un type pour la stratégie de groupe, ainsi que le nom du groupe de serveurs et un mot de passe :

```
hostname(config)# group-policy group_policy_name type server-group server_group_name password
server_password
hostname(config)#
```

### Remarque

Pour une stratégie de groupe externe, RADIUS est le seul type de serveur AAA pris en charge.



Par exemple, la commande suivante crée une stratégie de groupe externe nommée ExtGroup qui obtient ses attributs d'un serveur RADIUS externe nommé ExtRAD et spécifie que le mot de passe à utiliser lors de la récupération des attributs est newpassword :

```
hostname(config)# group-policy ExtGroup external server-group ExtRAD password newpassword
hostname(config)#
```

#### Remarque

Vous pouvez configurer plusieurs attributs spécifiques au fournisseur (VSA), comme décrit dans [Configurer un serveur AAA externe pour le VPN, à la page 295](#). Si un serveur RADIUS est configuré pour renvoyer l'attribut de classe (n° 25), l'ASA utilise cet attribut pour authentifier le nom de groupe. Sur le serveur RADIUS, l'attribut doit être formaté comme suit : OU=*groupname* ; où le *nom de groupe* est identique au nom de groupe configuré sur l'ASA — par exemple, OU=Finance.

## Créer une stratégie de groupe interne

Pour configurer une stratégie de groupe interne, passez en mode de configuration, utilisez la commande group-policy, spécifiez un nom et le type **internal** pour la stratégie de groupe :

```
hostname(config)# group-policy group_policy_name internal
hostname(config)#
```

Par exemple, la commande suivante crée la stratégie de groupe interne nommée GroupPolicy1 :

```
hostname(config)# group-policy GroupPolicy1 internal
hostname(config)#
```



**Remarque** Vous ne pouvez pas modifier le nom d'une stratégie de groupe après sa création.

Vous pouvez configurer les attributs d'une stratégie de groupe interne en copiant les valeurs d'une stratégie de groupe préexistante, en ajoutant le mot-clé **from** et en précisant le nom de la stratégie existante :

```
hostname(config)# group-policy group_policy_name internal from group_policy_name
hostname(config-group-policy)#
```

Par exemple, la commande suivante crée la stratégie de groupe interne nommée GroupPolicy2 en copiant les attributs de GroupPolicy1 :

```
hostname(config)# group-policy GroupPolicy2 internal from GroupPolicy1
hostname(config-group-policy)#
```

## Configurer les attributs généraux de la stratégie de groupe interne

### Nom de la stratégie de groupe

Le nom de la stratégie de groupe a été choisi lors de la création de la stratégie de groupe interne. Vous ne pouvez pas modifier le nom d'une stratégie de groupe une fois qu'elle a été créée. Consultez [Créer une stratégie de groupe interne](#), à la page 137 pour de plus amples renseignements.

### Configurer la bannière de message de stratégie de groupe

Précisez la bannière ou le message de bienvenue, le cas échéant, que vous souhaitez afficher. La valeur par défaut est Sans bannière. Le message que vous spécifiez s'affiche sur les clients distants lorsqu'ils se connectent. Pour spécifier une bannière, saisissez la commande **banner** en mode de configuration de la stratégie de groupe. Le texte de la bannière peut comporter jusqu'à 500 caractères.



**Remarque** Assurez-vous d'utiliser des sauts de ligne normaux dans la boîte de dialogue de la bannière et non « \n ».

La longueur totale de la bannière, qui s'affiche après l'ouverture de session sur le client VPN distant, est passée de 510 à 4 000 caractères dans la version 9.5.1 de l'ASA.



**Remarque** Un retour chariot et un saut de ligne inclus dans la bannière comptent comme deux caractères.

Pour supprimer une bannière existante, utilisez la forme **no** de cette commande. Sachez que l'utilisation de la version **no** de la commande supprime toutes les bannières de la stratégie de groupe.

Une stratégie de groupe peut hériter de cette valeur d'une autre stratégie de groupe. Pour éviter d'hériter d'une valeur, saisissez le mot-clé **none** au lieu de spécifier une valeur pour la chaîne de bannière, comme suit :

```
hostname(config-group-policy)# banner {value banner_string | none}
```

L'exemple suivant montre comment créer une bannière pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems ASA 9.0.
```

### Préciser les ensembles d'adresses pour les connexions d'accès à distance

Lorsque les clients d'accès à distance se connectent à l'ASA, celui-ci peut attribuer au client une adresse IPv4 ou IPv6 en fonction de la stratégie de groupe spécifiée pour la connexion.

Vous pouvez spécifier une liste de six ensembles d'adresses maximum à utiliser pour l'attribution d'adresses locales. L'ordre dans lequel vous spécifiez les ensembles est important. L'ASA attribue les adresses de ces ensembles d'adresses dans l'ordre dans lequel ces ensembles d'adresses apparaissent dans cette commande.

## Attribuer un ensemble d'adresses IPv4 à une stratégie de groupe interne

### Avant de commencer

Créez l'ensemble d'adresses IPv4.

### Procédure

- 
- Étape 1** Entrez en mode de configuration de la stratégie de groupe.
- group-policy value attributes**
- Exemple :**
- ```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```
- Étape 2** Attribuez l'ensemble d'adresses nommé ipv4-pool1, ipv4-pool2 et ipv4-pool3 à la stratégie de groupe FirstGroup. Vous êtes autorisé à spécifier jusqu'à 6 ensembles d'adresses pour la stratégie de groupe.
- address-pools value pool-name1 pool-name2 pool-name6**
- Exemple :**
- ```
asa4(config-group-policy)# address-pools value ipv4-pool1 ipv4-pool2 ipv4-pool3
asa4(config-group-policy)#
```
- Étape 3** (Facultatif) Utilisez la commande **no address-pools value pool-name** pour supprimer les ensembles d'adresses de la configuration de la stratégie de groupe et rétablir l'héritage des informations d'ensemble d'adresses à partir d'autres sources, telles que DfltGrpPolicy.
- no address-pools value pool-name1 pool-name2 pool-name6**
- Exemple :**
- ```
hostname(config-group-policy)# no address-pools value ipv4-pool1 ipv4-pool2 ipv4-pool3
hostname(config-group-policy)#
```
- Étape 4** (Facultatif) La commande **address-pools none** désactive cet attribut afin qu'il ne soit pas hérité d'autres sources de politique, telles que DfltGrpPolicy.
- ```
hostname(config-group-policy)# address-pools none
hostname(config-group-policy)#
```
- Étape 5** (Facultatif) La commande **no address pools none** supprime la commande **address-pools none** de la stratégie de groupe, en restaurant la valeur par défaut, qui est d'autoriser l'hérité.
- ```
hostname(config-group-policy)# no address-pools none
```

```
hostname (config-group-policy) #
```

Attribuer un ensemble d'adresses IPv6 à une stratégie de groupe interne

Avant de commencer

Créez l'ensemble d'adresses IPv6. Consultez [Adresses IP pour les VPN](#), à la page 191.

Procédure

Étape 1

Entrez en mode de configuration de la stratégie de groupe.

group-policy value attributes

Exemple :

```
hostname> en
hostname# config t
hostname (config) # group-policy FirstGroup attributes
hostname (config-group-policy) #
```

Étape 2

Attribuez l'ensemble d'adresses nommé ipv6-pool à la stratégie de groupe FirstGroup. Vous pouvez affecter jusqu'à six ensembles d'adresses IPv6 à une stratégie de groupe.

Exemple :

Cet exemple montre ipv6-pool1, ipv6-pool2 et ipv6-pool3 affectés à la stratégie de groupe FirstGroup.

```
hostname (config-group-policy) # ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3
hostname (config-group-policy) #
```

Étape 3

(Facultatif) Utilisez la commande **no ipv6-address-pools value pool-name** pour supprimer les ensembles d'adresses de la configuration de la stratégie de groupe et rétablir l'héritage des informations d'ensemble d'adresses à partir d'autres sources telles que DfltGroupPolicy.

no ipv6-address-pools value pool-name1 pool-name2 pool-name6

Exemple :

```
hostname (config-group-policy) # no ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3
hostname (config-group-policy) #
```

Étape 4

(Facultatif) Utilisez la commande **ipv6-address-pools none** pour désactiver cet attribut afin qu'il ne soit pas hérité d'autres sources de politique, telles que DfltGrpPolicy.

```
hostname (config-group-policy) # ipv6-address-pools none
hostname (config-group-policy) #
```

Étape 5

(Facultatif) Utilisez la commande **no ipv6-address pools none** pour supprimer la commande **ipv6-address-pools none** de la stratégie de groupe et rétablir la valeur par défaut, qui est d'autoriser l'héritage.

```
hostname(config-group-policy)# no ipv6-address-pools none
hostname(config-group-policy)#
```

Préciser le protocole de tunnelisation pour la stratégie de groupe

Précisez le type de tunnel VPN pour cette stratégie de groupe en saisissant la commande **vpn-tunnel-protocol { IKEv1 | IKEv2 | l2tp-ipsec | ssl-client }** en mode de configuration de stratégie de groupe.

La valeur par défaut consiste à hériter des attributs de la stratégie de groupe par défaut. Pour supprimer l'attribut de la configuration en cours d'exécution, saisissez la forme **no** de cette commande.

Les valeurs des paramètres pour cette commande sont les suivantes :

- **IKEv1** : négocie un tunnel IPsec IKEv1 entre deux homologues (le client VPN Cisco ou une autre passerelle sécurisée). Crée des associations de sécurité qui régissent l'authentification, le chiffrement, l'encapsulation et la gestion des clés.
- **IKEv2** : négocie un tunnel IPsec IKEv2 entre deux homologues (Secure Client (services client sécurisés) ou une autre passerelle sécurisée). Crée des associations de sécurité qui régissent l'authentification, le chiffrement, l'encapsulation et la gestion des clés.
- **l2tp-ipsec** : négocie un tunnel IPsec pour une connexion L2TP.
- **ssl-client** : négocie un tunnel SSL en utilisant TLS ou DTLS avec Secure Client (services client sécurisés).

Entrez cette commande pour configurer un ou plusieurs modes de tunnellation. Au moins un mode de tunnellation doit être configuré pour que les utilisateurs puissent se connecter sur un tunnel VPN.

L'exemple suivant montre comment configurer le mode de tunnellation IPsec IKEv1 pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol ikev1
hostname(config-group-policy)#
```

Préciser un réseau VLAN pour l'accès à distance ou appliquer une règle de contrôle d'accès unifiée à la stratégie de groupe

Les filtres consistent en des règles qui déterminent s'il faut autoriser ou rejeter les paquets de données tunnellenés en fonction de critères comme l'adresse source, l'adresse de destination et le protocole. Vous pouvez spécifier une liste de contrôle d'accès unifiée IPv4 ou IPv6 pour votre stratégie de groupe ou lui permettre d'hériter des listes de contrôle d'accès spécifiées dans la stratégie de groupe par défaut.

Choisissez l'une des options suivantes pour spécifier un VLAN de sortie (également appelé « mappage VLAN ») pour l'accès à distance ou spécifier une liste de contrôle d'accès pour filtrer le trafic :

**Remarque**

Lors du mappage du VLAN avec IPv6, l'adresse externe (destination) doit être unique pour chacun des VLAN afin que le trafic déchiffré soit acheminé vers les réseaux internes. Vous ne pouvez pas avoir le même réseau de destination avec des VLAN et des mesures de routage différents.

- Entrez la commande suivante en mode de configuration de stratégie de groupe pour préciser le VLAN de sortie pour les sessions VPN d'accès à distance attribuées à cette stratégie de groupe ou à une stratégie de groupe qui hérite de cette stratégie de groupe :

[no] vlan {vlan_id | none}

no vlan supprime *vlan_id* de la stratégie de groupe. La stratégie de groupe hérite de la valeur *vlan* de la stratégie de groupe par défaut.

none supprime *vlan_id* de la stratégie de groupe et désactive le mappage VLAN pour cette stratégie de groupe. La stratégie de groupe n'hérite pas de la valeur *vlan* de la stratégie de groupe par défaut.

vlan_id est le numéro de VLAN, au format décimal, à affecter aux sessions VPN d'accès à distance qui utilisent cette stratégie de groupe. Le VLAN doit être configuré sur cet ASA conformément aux instructions de la section « Configuration des sous-interfaces VLAN et de la liaison 802.1Q » dans le guide de configuration des opérations générales.

**Remarque**

Pour les connexions VPN sans client, la fonctionnalité VLAN de sortie fonctionne uniquement pour le protocole HTTP.

- Précisez le nom de la règle de contrôle d'accès (ACL) à appliquer à la session VPN en utilisant la commande **vpn-filter** en mode de stratégie de groupe. Vous pouvez spécifier une liste de contrôle d'accès IPv4 ou IPv6 à l'aide de la commande *vpn-filter*.

**Remarque**

Vous pouvez également configurer cet attribut en mode nom d'utilisateur, auquel cas la valeur configurée sous nom d'utilisateur remplace la valeur de stratégie de groupe.

```
hostname(config-group-policy)# vpn-filter {value ACL name | none}
hostname(config-group-policy)#
```

Vous configurez les listes de contrôle d'accès pour autoriser ou refuser différents types de trafic pour cette stratégie de groupe. Vous saisissez ensuite la commande **vpn-filter** pour appliquer ces listes de contrôle d'accès.

Pour supprimer la liste de contrôle d'accès, y compris une valeur nulle créée en entrant la commande **vpn-filter none**, saisissez la forme **no** de cette commande. L'option **no** permet l'hérité d'une valeur d'une autre stratégie de groupe.

Une stratégie de groupe peut hériter de cette valeur d'une autre stratégie de groupe. Pour éviter d'hériter d'une valeur, saisissez le mot-clé **none** au lieu de spécifier un nom d'ACL. Le mot-clé **none** indique qu'il n'y a pas d'ACL et définit une valeur nulle, interdisant ainsi une ACL.

L'exemple suivant montre comment définir un filtre qui invoque une liste de contrôle d'accès nommée `acl_vpn` pour la stratégie de groupe nommée `FirstGroup` :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter acl_vpn
hostname(config-group-policy)#
```

La commande **vpn-filter** s'applique au trafic post-déchiffré après sa sortie du tunnel et au trafic préchiffré avant son entrée dans le tunnel. Une liste de contrôle d'accès utilisée pour un `vpn-filter` ne doit pas également être utilisée pour un `access-group` d'interface. Lorsqu'une commande **vpn-filter** est appliquée à une stratégie de groupe qui régit les connexions des clients VPN d'accès à distance, l'ACL doit être configurée avec les adresses IP attribuées au client dans la position **src_ip** de l'ACL et le réseau local dans la position **dest_ip** de l'ACL.

Lorsqu'une commande **vpn-filter** est appliquée à une stratégie de groupe qui régit une connexion LAN à LAN, l'ACL doit être configurée avec le réseau distant dans la position **src_ip** de l'ACL et le réseau local dans la position **dest_ip** de l'ACL.

La prudence doit être utilisée lors de la construction des listes de contrôle d'accès à utiliser avec la fonctionnalité `vpn-filter`. Les listes de contrôle d'accès sont bâties en gardant à l'esprit le trafic post-déchiffré. Cependant, les listes de contrôle d'accès sont également appliquées au trafic dans le sens opposé. Pour ce trafic préchiffré qui est destiné au tunnel, les listes de contrôle d'accès sont bâties avec les positions **src_ip** et **dest_ip** permutées.

Notez que le filtre VPN s'applique aux connexions initiales uniquement. Il ne s'applique pas aux connexions secondaires, comme une connexion de support SIP, qui sont ouvertes en raison de l'action de l'inspection d'application.

Dans l'exemple suivant : le `vpn-filter` est utilisé avec un client VPN d'accès à distance. Cet exemple suppose que l'adresse IP attribuée au client est 10.10.10.1/24 et que le réseau local est 192.168.1.0/24.

L'ACE suivant permet au client VPN d'accès à distance d'établir une connexion Telnet vers le réseau local :

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255
192.168.1.0 255.255.255.0 eq 23
```

L'ACE suivant permet au réseau local d'établir une connexion Telnet vers le client d'accès à distance :

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq
23 192.168.1.0 255.255.255.0
```



Remarque

L'ACE **access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23** permet au réseau local d'établir une connexion avec le client d'accès à distance sur n'importe quel port TCP s'il utilise un port source de 23. L'ACE **access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq 23 192.168.1.0 255.255.255.0** permet au client d'accès à distance d'établir une connexion au réseau local sur n'importe quel port TCP s'il utilise un port source de 23.

Dans l'exemple suivant, le `vpn-filter` est utilisé avec une connexion VPN de site à site. Cet exemple suppose que le réseau distant est 10.0.0.0/24 et que le réseau local est 192.168.1.0/24. L'ACE suivant permet au réseau distant de communiquer avec le réseau local :

```
hostname(config-group-policy)# access-list vpnfilt-121 permit 10.0.0.0 255.255.255.0
192.168.1.0 255.255.255.0 eq 23
```

L'ACE suivant permet au réseau local d'établir une connexion Telnet vers le réseau distant :

```
hostname(config-group-policy)# access-list vpnfilt-121 permit 10.0.0.0 255.255.255.0 eq 23
192.168.1.0 255.255.255.0
```



Remarque

L'ACE **access-list vpnfilt-121 permit 10.0.0.0 255.255.255.0 192.168.1.0 255.255.255.0 eq 23** permet au réseau local d'établir une connexion avec le réseau distant sur n'importe quel port TCP s'il utilise un port source de 23. L'ACE **access-list vpnfilt-121 permit 10.0.0.0 255.255.255.0 eq 23 192.168.1.0 255.255.255.0** permet au réseau distant d'établir une connexion avec le réseau local sur n'importe quel port TCP s'il utilise un port source de 23.

Préciser les heures d'accès au VPN pour une stratégie de groupe

Avant de commencer

Créer une plage horaire Consultez le guide de configuration sur les opérations générales ASA pour plus d'informations.

Procédure

Étape 1

Entrez en mode de configuration de la stratégie de groupe.

group-policy value attributes

Exemple :

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

Étape 2

Vous pouvez définir les heures d'accès VPN en associant une politique de plage temporelle configurée à une stratégie de groupe à l'aide de la commande **vpn-access-hours** en mode de configuration de stratégie de groupe. Cette commande attribue une plage horaire d'accès VPN nommée heures de travail à la stratégie de groupe nommée FirstGroup.

Une stratégie de groupe peut hériter d'une valeur de plage temporelle d'une stratégie de groupe par défaut ou d'une stratégie de groupe spécifiée. Pour éviter cet héritage, saisissez le mot-clé **none** au lieu du nom d'une plage temporelle dans cette commande. Ce mot-clé définit les heures d'accès VPN à une valeur nulle, ce qui n'autorise aucune politique de plage temporelle.

vpn-access-hours value {time-range-name | none}

Exemple :


```
hostname(config-group-policy)# vpn-access-hours value business-hours
hostname(config-group-policy)#
```

Préciser les connexions VPN simultanées pour une stratégie de groupe

Vous pouvez définir une limite au nombre de sessions simultanées qu'un utilisateur donné peut maintenir pour une stratégie de groupe. La valeur par défaut est de 3 sessions simultanées.

Les sessions périmées Secure Client (services client sécurisés), client IPsec ou sans client (sessions terminées de manière anormale) peuvent rester dans la base de données des sessions, même si une « nouvelle » session a été établie avec le même nom d'utilisateur.

Si le nombre autorisé de sessions simultanées est de 1 et que le même utilisateur se connecte à nouveau après une interruption anormale, la session périmée est supprimée de la base de données et une nouvelle session est établie. Si, toutefois, la session existante est toujours une connexion active et que le même utilisateur se connecte à nouveau, peut-être à partir d'un autre ordinateur, la première session est déconnectée et supprimée de la base de données, et une nouvelle session est établie.

Si le nombre de sessions simultanées autorisées est supérieur à 1, puis, lorsque l'utilisateur a atteint ce nombre maximal et tente de se connecter à nouveau, la session avec le temps d'inactivité le plus long est déconnectée. Si toutes les sessions actuelles sont inactives depuis une durée égale, la session la plus ancienne est déconnectée. Cette action libère une session et permet la nouvelle connexion.

Une fois que la limite maximale de sessions est atteinte, il faut un certain temps au système pour supprimer la session la plus ancienne. Ainsi, un utilisateur pourrait ne pas être en mesure de se connecter immédiatement et pourrait devoir réessayer la nouvelle connexion avant qu'elle ne se termine avec succès. Cela ne devrait pas être un problème si les utilisateurs déconnectent leurs sessions comme prévu. Vous pouvez éventuellement supprimer le retard en configurant le système pour ne pas attendre que la suppression soit terminée et autoriser immédiatement la connexion du nouvel utilisateur.

Procédure

	Commande ou action	Objectif
Étape 1	Précisez le nombre de connexions simultanées autorisées pour un utilisateur, à l'aide de la commande vpn-simultaneous-logins <i>nombre entier</i> en mode de configuration de stratégie de groupe.	vpn-simultaneous-logins <i>integer</i> La valeur par défaut est 3. La plage est un nombre entier compris entre 0 et 2147483647. Une stratégie de groupe peut hériter de cette valeur d'une autre stratégie de groupe. Saisissez 0 pour désactiver la connexion et empêcher l'accès de l'utilisateur. L'exemple suivant montre comment autoriser un maximum de 4 connexions simultanées pour la stratégie de groupe nommée FirstGroup : <pre>hostname(config)# group-policy FirstGroup attributes hostname(config-group-policy)# vpn-simultaneous-logins 4</pre> Remarque

	Commande ou action	Objectif
		• Bien que la limite maximale du nombre de connexions simultanées soit très élevée, autoriser plusieurs connexions simultanées peut compromettre la sécurité et affecter les performances. • Lorsque vous vous connectez à différents groupes de tunnels avec des stratégies de groupe différentes, vpn-simultaneous-logins supprime les sessions d'utilisateur même si les sessions existantes utilisent une stratégie de groupe différente.
Étape 2	(Facultatif) Lorsque la limite de connexions simultanées est atteinte, configurez le système pour établir de nouvelles sessions sans attendre que la session la plus ancienne soit supprimée.	vpn-simultaneous-login-delete-no-delay Cette option est désactivée par défaut. <pre>hostname(config)# group-policy FirstGroup attributes hostname(config-group-policy)# vpn-simultaneous-login-delete-no-delay</pre>

Restreindre l'accès à un profil de connexion précis

Précisez s'il faut restreindre les utilisateurs distants afin qu'ils accèdent uniquement par le profil de connexion, à l'aide de la commande **group-lock** en mode de configuration group-policy.

```
hostname(config-group-policy)# group-lock {value tunnel-grp-name | none}
hostname(config-group-policy)# no group-lock
hostname(config-group-policy)#
```

La variable *tunnel-grp-name* précise le nom d'un profil de connexion existant que l'ASA exige pour que l'utilisateur puisse se connecter. Le verrouillage de groupe restreint les utilisateurs en vérifiant si le groupe configuré dans le client VPN est le même que le profil de connexion auquel l'utilisateur est affecté. Si ce n'est pas le cas, l'ASA empêche l'utilisateur de se connecter. Si vous ne configurez pas group-lock, l'ASA authentifie les utilisateurs sans tenir compte du groupe attribué. Le verrouillage de groupe est désactivé par défaut.

Pour supprimer l'attribut **group-lock** de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cette option permet d'hériter d'une valeur provenant d'une autre stratégie de groupe.

Pour désactiver le verrouillage de groupe, saisissez la commande **group-lock** avec le mot-clé **none**. Le mot-clé none définit group-lock à une valeur nulle, de sorte qu'aucune restriction de verrouillage de groupe n'est appliquée. Cela empêche également d'hériter d'une valeur de verrouillage de groupe d'une stratégie de groupe par défaut ou précisée.

Préciser le délai de connexion VPN maximal dans une stratégie de groupe

Procédure

Étape 1

(Facultatif) Configurez une durée maximale pour les connexions VPN en utilisant la commande **vpn-session-timeout** {minutes} dans le mode de configuration de stratégie de groupe ou dans le mode de configuration du nom d'utilisateur.

La durée minimale est de 1 minute et la durée maximale est de 35 791 394 minutes. Il n'y a pas de valeur par défaut. À la fin de cette période, l'ASA met fin à la connexion.

L'exemple suivant montre comment définir un délai d'expiration de session VPN de 180 minutes pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

L'exemple suivant montre comment définir un délai d'expiration de session VPN de 180 minutes pour l'utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-session-timeout 180
hostname(config-username)#
```

Autres actions utilisant la commande **[no] vpn-session-timeout** {minutes | none} :

- Pour supprimer l'attribut de cette stratégie et autoriser l'héritage, saisissez la forme **no vpn-session-timeout** de cette commande.
- Pour autoriser un délai d'expiration illimité et ainsi empêcher l'héritage d'une valeur de délai d'expiration, saisissez **vpn-session-timeout none**.

Étape 2

Configurez le moment où un message d'alerte d'expiration de session s'affiche à l'utilisateur au moyen de la commande **vpn-session-timeout alert-interval** {minutes | } .

Ce message d'alerte indique aux utilisateurs le nombre de minutes restantes avant la déconnexion automatique de leur session VPN. L'exemple suivant montre comment spécifier que les utilisateurs seront informés 20 minutes avant la déconnexion de leur session VPN. Vous pouvez spécifier une plage de 1 à 30 minutes.

```
hostname(config-webvpn)# vpn-session-timeout alert-interval 20
```

Autres actions utilisant la commande **[no] vpn-session-timeout alert-interval** {minutes | none} :

- Utilisez la forme **no** de la commande pour indiquer que l'attribut d'intervalle d'alerte du délai d'expiration de la session VPN sera hérité de la stratégie de groupe par défaut :

```
hostname(config-webvpn)# no vpn-session-timeout alert-interval
```

- Le **vpn-session-timeout alert-interval none** indique que les utilisateurs ne recevront pas d'alerte.

Préciser un délai d'inactivité de session VPN pour une stratégie de groupe

Procédure

Étape 1

(Facultatif) Pour configurer un délai d'inactivité du VPN, utilisez la commande **vpn-idle-timeout** *minutes* en mode de configuration de stratégie de groupe ou en mode de configuration de nom d'utilisateur.

S'il n'y a aucune activité de communication sur la connexion pendant cette période, l'ASA arrête la connexion. La durée minimale est de 1 minute, la durée maximale est de 35 791 394 minutes et la valeur par défaut est de 30 minutes.

L'exemple suivant montre comment définir un délai d'inactivité VPN de 15 minutes pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
hostname(config-group-policy)#
```

Autres actions utilisant la commande **[no] vpn-idle-timeout** {*minutes* | **none**} :

- Saisissez **vpn-idle-timeout none** pour désactiver le délai d'inactivité du VPN et empêcher l'héritage d'une valeur de délai d'expiration.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout none
hostname(config-group-policy)#
```

Il en résulte Secure Client (services client sécurisés) (SSL et IPsec/IKEv2) et un VPN sans client utilisant la valeur globale **default-idle-timeout** *secondes* webvpn. Cette commande est saisie en mode webvpn-config, par exemple : `hostname(config-webvpn)# default-idle-timeout 300`. La valeur par défaut est de 1800 secondes (30 min), la plage est comprise entre 60 et 86400 secondes.

Pour toutes les connexions webvpn, la valeur **default-idle-timeout** est appliquée uniquement si **vpn-idle-timeout none** est défini dans l'attribut de stratégie de groupe/de nom d'utilisateur. Une valeur de délai d'inactivité non nulle est requise par l'ASA pour toutes les connexions Secure Client (services client sécurisés).

Pour les VPN de site à site (IKEv1, IKEv2) et VPN d'accès à distance IKEv1, nous vous recommandons de désactiver le délai d'expiration et d'autoriser une période d'inactivité illimitée.

- Pour désactiver le délai d'inactivité pour cette stratégie de groupe ou cette politique d'utilisateur, saisissez **no vpn-idle-timeout**. La valeur sera héritée.
- Si vous ne définissez pas du tout **vpn-idle-timeout**, de toute façon, la valeur est héritée, qui est par défaut de 30 minutes.

Remarque

vpn-idle-timeout contrôle uniquement la durée maximale d'une session parente. Les sessions enfants (SSL/DTLS) sont terminées de manière dynamique beaucoup plus tôt par un délai d'inactivité TCP de 5 minutes codé en dur ou en cas d'échec de la vérification Dead Peer Detection (DPD) (3 tentatives). Pour plus de détails, consultez la note dans [Configurer la détection d'homologue mort](#). Pour plus de détails sur les attributs DPD, keepalive et de temporisation, consultez [Answer AnyConnect FAQ - Tunnels, DPD et minuterie d'inactivité](#).

Étape 2

(Facultatif) Vous pouvez éventuellement configurer l'heure à laquelle un message d'alerte de délai d'inactivité s'affiche à l'utilisateur à l'aide de la commande **vpn-idle-timeout alert-interval** {minutes}.

Ce message d'alerte indique aux utilisateurs le nombre de minutes qu'il leur reste jusqu'à ce que leur session VPN soit déconnectée pour cause d'inactivité. L'intervalle d'alerte par défaut est d'une minute.

L'exemple suivant montre comment définir un intervalle d'alerte de délai d'inactivité du VPN de 3 minutes pour l'utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout alert-interval 3
hostname(config-username)#
```

Autres actions utilisant la commande **[no] vpn-idle-timeout alert-interval** {minutes | none} :

- Le paramètre **none** indique que les utilisateurs ne recevront pas d'alerte.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout none
hostname(config-username)#
```

- Pour supprimer l'intervalle d'alerte de cette stratégie de groupe ou d'utilisateur, saisissez **no vpn-idle-timeout alert-interval**. La valeur sera héritée.
- Si vous ne définissez pas ce paramètre du tout, l'intervalle d'alerte par défaut est d'une minute.

Configurer les serveurs WINS et DNS pour une stratégie de groupe

Vous pouvez spécifier des serveurs WINS et des serveurs DNS principaux et secondaires. La valeur par défaut dans chaque cas est aucune. Pour spécifier ces serveurs, procédez comme suit :

Procédure**Étape 1**

Précisez les serveurs WINS principal et secondaire :

```
hostname(config-group-policy)# wins-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

La première adresse IP spécifiée est celle du serveur WINS principal. La deuxième adresse IP (facultative) est celle du serveur WINS secondaire. La spécification du mot-clé **none** au lieu d'une adresse IP définit les serveurs WINS à une valeur nulle, ce qui n'autorise aucun serveur WINS et empêche d'hériter d'une valeur d'une stratégie de groupe par défaut ou d'une stratégie de groupe spécifiée.

Chaque fois que vous saisissez la commande **wins-server**, vous remplacez le paramètre existant. Par exemple, si vous configurez le serveur WINS x.x.x.x, puis le serveur WINS y.y.y.y, la deuxième commande remplace la première, et y.y.y.y devient le seul serveur WINS. La même chose est vraie pour plusieurs serveurs. Pour ajouter un serveur WINS plutôt que de remplacer les serveurs précédemment configurés, incluez les adresses IP de tous les serveurs WINS lorsque vous entrez cette commande.

L'exemple suivant montre comment configurer les serveurs WINS avec les adresses IP 10.10.10.15 et 10.10.10.30 pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30
hostname(config-group-policy)#
```

Étape 2 Précisez les serveurs DNS principal et secondaire :

```
hostname(config-group-policy)# dns-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

La première adresse IP spécifiée est celle du serveur DNS principal. La deuxième adresse IP (facultative) est celle du serveur DNS secondaire. La spécification du mot-clé **none** au lieu d'une adresse IP définit les serveurs DNS à une valeur nulle, ce qui n'autorise aucun serveur DNS et empêche d'hériter d'une valeur d'une politique par défaut ou d'un groupe spécifié. Vous pouvez spécifier jusqu'à quatre adresses de serveur DNS : jusqu'à deux adresses IPv4 et deux adresses IPv6.

Chaque fois que vous saisissez la commande **dns-server**, vous remplacez le paramètre existant. Par exemple, si vous configurez le serveur DNS x.x.x.x, puis le serveur DNS y.y.y.y, la deuxième commande remplace la première, et y.y.y.y devient le seul serveur DNS. La même chose est vraie pour plusieurs serveurs. Pour ajouter un serveur DNS plutôt que de remplacer les serveurs précédemment configurés, incluez les adresses IP de tous les serveurs DNS lorsque vous entrez cette commande.

L'exemple suivant montre comment configurer les serveurs DNS avec les adresses IP 10.10.10.15, 10.10.10.30, 2001:DB8::1 et 2001:DB8::2 pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dns-server value 10.10.10.15 10.10.10.30
2001:DB8::1 2001:DB8::2
hostname(config-group-policy)#
```

Étape 3 Si aucun nom de domaine par défaut n'est spécifié dans le groupe de serveurs **DNS DefaultDNS**, vous devez spécifier un domaine par défaut. Utilisez le nom de domaine et le domaine de premier niveau, par exemple **example.com**.

```
asa4(config)# group-policy FirstGroup attributes
asa4(config-group-policy)# default-domain value example.com
asa4(config-group-policy)#
```

Étape 4 (Facultatif) Configurez la portée du réseau DHCP :

```
dhcp-network-scope {ip_address | none}
```

Si vous configurez des serveurs DHCP pour l'ensemble d'adresses dans le profil de connexion, la portée de DHCP identifie les sous-réseaux à utiliser pour le regroupement pour ce groupe. Le serveur DHCP doit également avoir des adresses dans le même sous-réseau identifié par la portée. La portée vous permet de sélectionner un sous-ensemble des ensembles d'adresses définis dans le serveur DHCP à utiliser pour ce groupe précis.

Si vous ne définissez pas de portée réseau, le serveur DHCP attribue les adresses IP dans l'ordre des ensembles d'adresses configurés. Il parcourt les ensembles jusqu'à ce qu'il identifie une adresse non attribuée.

Pour spécifier une portée, saisissez une adresse routable sur le même sous-réseau que l'ensemble souhaité, mais en dehors de cet ensemble. Le serveur DHCP détermine à quel sous-réseau cette adresse IP appartient et attribue une adresse IP de cet ensemble d'adresses.

Nous vous recommandons d'utiliser l'adresse IP d'une interface chaque fois que cela est possible à des fins de routage. Par exemple, si l'ensemble d'adresses est 10.100.10.2-10.100.10.254 et que l'adresse d'interface est 10.100.10.1/24, utilisez 10.100.10.1 comme portée DHCP. N'utilisez pas le numéro de réseau. Vous ne pouvez utiliser DHCP que pour l'adressage IPv4. Si l'adresse que vous choisissez n'est pas une adresse d'interface, vous devrez peut-être créer une voie de routage statique pour l'adresse de portée.

La spécification de **none** empêche l'affectation d'adresses DHCP, par exemple, à partir d'une stratégie de groupe par défaut ou d'un système hérité.

Exemple :

L'exemple suivant passe en mode de configuration d'attributs pour FirstGroup et définit la portée DHCP à 10.100.10.1.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.100.10.1
```

Définir la politique de tunnellation fractionnée

Définissez les règles de tunnellation du trafic en précisant la politique de tunnellation fractionnée pour le trafic IPv4 :

split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

no split-tunnel-policy

Définissez les règles de tunnellation du trafic en précisant la politique de tunnellation fractionnée pour le trafic IPv6 :

ipv6-split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

no ipv6-split-tunnel-policy

Les options de politique sont les suivantes :

- **tunnelspecified** : tunnelise tout le trafic vers ou depuis les réseaux précisés dans la liste de réseaux à travers le tunnel. Les données destinées à toutes les autres adresses circulent en clair et sont acheminées par le fournisseur de services Internet de l'utilisateur distant.

Pour les versions de l'ASA 9.1.4 et ultérieures, lorsque vous précisez une liste d'inclusion, vous pouvez également préciser une liste d'exclusion pour un sous-réseau situé dans la plage d'inclusion. Les adresses du sous-réseau exclu ne seront pas tunnelisées, mais le reste de la liste d'inclusion le sera. Les réseaux dans la liste d'exclusion ne seront pas envoyés sur le tunnel. La liste d'exclusion est précisée à l'aide d'entrées deny, et la liste d'inclusion à l'aide d'entrées permit.

- **excludespecified** : ne tunnelise pas le trafic vers ou depuis les réseaux précisés dans la liste de réseaux. Le trafic de ou vers toutes les autres adresses est tunnelisé. Le profil du client VPN actif sur le client doit avoir l'option Local LAN Access activée. Cette option fonctionne uniquement avec les Secure Client (services client sécurisés).

**Remarque**

Les réseaux dans la liste d'exclusion qui ne sont pas un sous-ensemble de la liste d'inclusion sont ignorés par le client.

- **tunnelall** —Précise que tout le trafic passe par le tunnel. Cette politique désactive la tunnellation fractionnée. Les utilisateurs distants ont accès au réseau de l'entreprise, mais ils n'ont pas accès aux réseaux locaux. Il s'agit de l'option par défaut.

**Remarque**

La tunnellation fractionnée est une fonctionnalité de gestion du trafic, non une fonctionnalité de sécurité. Pour une sécurité optimale, nous vous recommandons de ne pas activer la tunnellation fractionnée.

Exemple

L'exemple suivant montre comment définir, pour la stratégie de groupe nommée FirstGroup, une politique de tunnellation fractionnée limitant le tunnel aux seuls réseaux spécifiés pour IPv4 et IPv6 :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified

hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
```

Préciser une liste de réseaux pour la tunnellation fractionnée

Dans la tunnellation fractionnée, les listes de réseau déterminent quel trafic réseau passe par le tunnel. Secure Client (services client sécurisés) prend les décisions de tunnellation fractionnée en fonction d'une liste de réseaux, qui est une ACL.

```
hostname(config-group-policy)# split-tunnel-network-list {value access-list_name | none}
hostname(config-group-policy)# no split-tunnel-network-list value [access-list_name]
```

- **value** nom de liste d'accès : identifie une ACL qui énumère les réseaux à tunneliser ou à ne pas tunneliser. L'ACL peut être une ACL unifiée avec des ACE qui précisent à la fois des adresses IPv4 et IPv6.
- **none** : indique qu'il n'y a pas de liste de réseaux pour la tunnelisation fractionnée ; l'ASA tunnelise tout le trafic. Le fait de préciser le mot-clé **none** définit une liste de réseaux de tunnellation fractionnée avec une valeur nulle, ce qui interdit la tunnellation fractionnée. Cela empêche également l'héritage d'une liste de réseaux de tunnellation fractionnée par défaut à partir d'une stratégie de groupe par défaut ou précisée.

Pour supprimer une liste de réseaux, saisissez la forme **no** de cette commande. Pour supprimer toutes les listes de réseaux de tunnellation fractionnée, entrez la commande **no split-tunnel-network-list** sans arguments. Cette commande supprime toutes les listes de réseaux configurées, y compris une liste nulle si vous en avez créé une en saisissant le mot-clé **none**.

Lorsqu'il n'y a aucune liste de réseaux de tunnellation fractionnée, les utilisateurs héritent de toute liste de réseaux présente dans la stratégie de groupe par défaut ou précisée. Pour empêcher les utilisateurs d'hériter de telles listes de réseaux, saisissez la commande **split-tunnel-network-list none**.

Exemple

L'exemple suivant montre comment créer une liste de réseaux nommée FirstList et l'ajouter à la stratégie de groupe nommée FirstGroup. FirstList est une liste d'exclusion et une liste d'inclusion qui est un sous-réseau de la liste d'exclusion :

```
hostname(config)# split-tunnel-policy tunnelspecified
hostname(config)# access-list FirstList deny ip 10.10.10.0 255.255.255.0 any
hostname(config)# access-list FirstList permit ip 10.0.0.0 255.0.0.0 any

hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list value FirstList
```

L'exemple suivant montre comment créer une liste de réseaux nommée v6 et ajouter la politique de tunnellation fractionnée v6 à la stratégie de groupe nommée GroupPolicy_ipv6-ikev2. v6 est une liste d'exclusion et une liste d'inclusion qui est un sous-réseau de la liste d'exclusion :

```
hostname(config)# access-list v6 extended permit ip fd90:5000::/32 any6
hostname(config)# access-list v6 extended deny ip fd90:5000:3000:2880::/64 any6

hostname(config)# group-policy GroupPolicy_ipv6-ikev2 internal
hostname(config)# group-policy GroupPolicy_ipv6-ikev2 attributes
hostname(config-group-policy)# vpn-tunnel-protocol ikev2 ssl-client
hostname(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
hostname(config-group-policy)# split-tunnel-network-list value v6
```

Vérifier la configuration de la tunnellation fractionnée

Exécutez la commande **show runn group-policy attributes** pour vérifier votre configuration. Cet exemple montre que l'administrateur a défini à la fois une politique réseau IPv4 et une politique réseau IPv6, et a utilisé la liste de réseaux (ACL unifiée), **FirstList** pour les deux politiques.

```
hostname(config-group-policy)# show runn group-policy FirstGroup attributes
group-policy FirstGroup attributes
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy tunnelspecified
split-tunnel-network-list value FirstList
```

Configurer les attributs de domaine pour la tunnellation fractionnée

Vous pouvez préciser un nom de domaine par défaut ou une liste de domaines à résoudre au moyen du tunnel fractionné, ce que nous appelons DNS fractionné.

AnyConnect 3.1 prend en charge la véritable fonctionnalité DNS fractionné pour les plateformes Windows et Mac OS X. Si la stratégie de groupe sur l'appareil de sécurité active la tunnellation fractionnée split-include et précise les noms DNS à tunneliser, AnyConnect tunnelise vers le serveur DNS privé toutes les requêtes DNS qui correspondent à ces noms. Le véritable DNS fractionné permet l'accès par tunnel uniquement aux requêtes DNS correspondant aux domaines transmis au client par l'ASA. Ces demandes ne sont pas envoyées en clair. D'un autre côté, si les requêtes DNS ne correspondent pas aux domaines transmis par l'ASA,

AnyConnect permet au résolveur DNS du système d'exploitation client de soumettre le nom d'hôte en clair pour résolution DNS.



Remarque

Le DNS fractionné prend en charge les requêtes standard et les mises à jour (y compris A, AAAA, NS, TXT, MX, SOA, ANY, SRV, PTR et CNAME). Les requêtes PTR correspondant à l'un des réseaux tunnelisés sont autorisées dans le tunnel.

Pour Mac OS X, AnyConnect ne peut utiliser le véritable DNS fractionné pour un protocole IP donné que si l'une des conditions suivantes est remplie :

- Le DNS fractionné est configuré pour un protocole IP, comme IPv4, et Client Bypass Protocol est configuré pour l'autre protocole IP, comme IPv6, dans la stratégie de groupe, sans ensemble d'adresses configuré pour ce dernier protocole IP.
- Le DNS fractionné est configuré pour les deux protocoles IP.

Définition d'un nom de domaine par défaut

L'ASA transmet le nom de domaine par défaut à Secure Client (services client sécurisés). Le client ajoute le nom de domaine aux requêtes DNS qui omettent le champ de domaine. Ce nom de domaine s'applique uniquement aux paquets tunnelisés. Lorsqu'il n'y a pas de nom de domaine par défaut, les utilisateurs héritent du nom de domaine par défaut dans la stratégie de groupe par défaut.

Pour spécifier le nom de domaine par défaut pour les utilisateurs de la stratégie de groupe, entrez la commande **default-domain** en mode de configuration de stratégie de groupe. Pour supprimer un nom de domaine, saisissez la forme **no** de cette commande.

```
hostname(config-group-policy)# default-domain {value domain-name | none}
hostname(config-group-policy)# no default-domain [domain-name]
```

Le paramètre de nom de domaine **value** identifie le nom de domaine par défaut pour le groupe. Pour spécifier qu'il n'y a pas de nom de domaine par défaut, saisissez le mot-clé **none**. Cette commande définit un nom de domaine par défaut avec une valeur nulle, ce qui n'autorise pas un nom de domaine par défaut et empêche d'hériter d'un nom de domaine par défaut d'une stratégie de groupe par défaut ou d'une stratégie de groupe spécifiée.

Pour supprimer tous les noms de domaine par défaut, entrez la commande **no default-domain** sans arguments. Cette commande supprime tous les noms de domaine par défaut configurés, y compris une liste nulle si vous en avez créé une en saisissant la commande **default-domain** avec le mot-clé **none**. La forme **no** permet d'hériter d'un nom de domaine.

L'exemple suivant montre comment définir un nom de domaine par défaut FirstDomain pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

Définir une liste de domaines pour la tunnellation fractionnée

Saisissez une liste de domaines à résoudre via le tunnel fractionné, en plus du domaine par défaut. Entrez la commande **split-dns** en mode de configuration de la stratégie de groupe. Pour supprimer une liste, saisissez la forme **no** de cette commande.

Lorsqu'il n'existe aucune liste de domaines de tunnellation fractionnée, les utilisateurs héritent de celles définies dans la stratégie de groupe par défaut. Pour empêcher les utilisateurs d'hériter de telles listes de domaines de tunnellation fractionnées, entrez la commande **split-dns** avec le mot-clé **none**.

Pour supprimer toutes les listes de domaines de tunnellation fractionnées, entrez la commande **no split-dns** sans arguments. Cela supprime toutes les listes de domaines de tunnellation fractionnée configurées, y compris une liste nulle créée en émettant la commande **split-dns** avec le mot-clé **none**.

Le paramètre domain-name **value** fournit un nom de domaine que l'ASA résout via le tunnel fractionné. Le mot-clé **none** indique qu'il n'y a pas de liste DNS fractionnée. Il définit également une liste DNS fractionnée avec une valeur nulle, interdisant ainsi une liste DNS fractionnée, et empêche d'hériter d'une liste DNS fractionnée d'une stratégie de groupe par défaut ou spécifiée. La syntaxe de la commande est la suivante :

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2... domain-nameN]
| none}
hostname(config-group-policy)# no split-dns [domain-name domain-name2 domain-nameN]
```

Saisissez un espace unique pour séparer chaque entrée dans la liste de domaines. Il n'y a aucune limite au nombre d'entrées, mais la chaîne complète ne peut pas dépasser 492 caractères. Vous ne pouvez utiliser que des caractères alphanumériques, des tirets (-) et des points (.). Si le nom de domaine par défaut doit être résolu par le tunnel, vous devez inclure explicitement ce nom dans cette liste.

L'exemple suivant montre comment configurer les domaines Domain1, Domain2, Domain3 et Domain4 pour qu'ils soient résolus au moyen de la tunnellation fractionnée pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```



Remarque

Lors de la configuration d'un DNS fractionné, vérifiez que les serveurs DNS privés spécifiés ne recoupent pas les serveurs DNS configurés pour la plateforme cliente. Si c'est le cas, la résolution de noms ne fonctionne pas correctement et des requêtes peuvent être rejetées.

Configurer l'interception DHCP pour Windows XP et la tunnellation fractionnée

Une anomalie Microsoft XP entraîne la corruption des noms de domaine si les options de tunnellation fractionnée dépassent 255 octets. Pour éviter ce problème, l'ASA limite le nombre de routes qu'il envoie à 27 à 40 routes, le nombre de routes dépendant des classes des routes.

DHCP Intercept permet aux clients Microsoft Windows XP d'utiliser la tunnellation fractionnée avec l'ASA. L'ASA répond directement au message DHCP Inform du client Microsoft Windows XP, en fournissant à ce client le masque de sous-réseau, le nom de domaine et les routes statiques sans classe pour l'adresse IP du tunnel. Pour les clients Windows antérieurs à Windows XP, DHCP Intercept fournit le nom de domaine et le masque de sous-réseau. Cela est utile dans les environnements où l'utilisation d'un serveur DHCP n'est pas avantageuse.

La commande **intercept-dhcp** active ou désactive l'interception DHCP.

```
hostname(config-group-policy)# intercept-dhcp netmask {enable | disable}
hostname(config-group-policy)#
```

La variable *netmask* fournit le masque de sous-réseau pour l'adresse IP du tunnel. La forme **no** de cette commande supprime l'interception DHCP de la configuration :

[no] intercept-dhcp

L'exemple suivant montre comment définir les interceptions DHCP pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# intercept-dhcp enable
```

Configurer les paramètres du proxy de navigateur pour une utilisation avec les clients d'accès à distance

Suivez ces étapes pour configurer les paramètres du serveur proxy pour un client.

Procédure

Étape 1 Configurez un proxy de navigateur et un port pour un périphérique client en saisissant la commande **msie-proxy server** en mode de configuration de stratégie de groupe :

```
hostname(config-group-policy)# msie-proxy server {value server[:port] | none}
hostname(config-group-policy)#
```

La valeur par défaut est **none**, qui ne spécifie aucun paramètre du proxy de navigateur du périphérique client. Pour supprimer l'attribut de la configuration, utilisez la forme **no** de la commande.

```
hostname(config-group-policy)# no msie-proxy server
hostname(config-group-policy)#
```

La ligne contenant l'adresse IP ou le nom d'hôte du proxy et le numéro de port doit comporter moins de 100 caractères.

L'exemple suivant montre comment configurer l'adresse IP 192.168.10.1 en tant que proxy de navigateur, en utilisant le port 880, pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server value 192.168.21.1:880
hostname(config-group-policy)#
```

Étape 2 Configurez les actions du proxy de navigateur (« méthodes ») pour un périphérique client en saisissant la commande **msie-proxy method** en mode de configuration de stratégie de groupe.

```
hostname(config-group-policy)# msie-proxy method [auto-detect | no-modify |
no-proxy | use-server]
hostname(config-group-policy)#
```

La valeur par défaut est **no-modify**. Pour supprimer l'attribut de la configuration, utilisez la forme **no** de la commande.

```
hostname(config-group-policy)# no msie-proxy method [auto-detect | no-modify |
no-proxy | use-server]
hostname(config-group-policy)#
```

Les méthodes disponibles sont les suivantes :

- **auto-detect** : active la détection automatique du serveur mandataire dans le navigateur du périphérique client.
- **no-modify** : conserve inchangé le paramètre du proxy dans le navigateur HTTP pour ce périphérique client.
- **no-proxy**—Désactive le paramètre du proxy HTTP dans le navigateur pour le périphérique client.
- **use-server**—Définit le paramètre du proxy HTTP dans le navigateur pour utiliser la valeur configurée dans la commande **msie-proxy server**.

La ligne contenant l'adresse IP ou le nom d'hôte du proxy et le numéro de port doit comporter moins de 100 caractères.

L'exemple suivant montre comment configurer la détection automatique en tant que paramètre du proxy de navigateur pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy method auto-detect
hostname(config-group-policy)#
```

L'exemple suivant configure le paramètre proxy de navigateur pour la stratégie de groupe nommée FirstGroup afin d'utiliser le serveur QAsrver, port 1001 comme serveur pour le périphérique client :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server QAsrver:port 1001
hostname(config-group-policy)# msie-proxy method use-server
hostname(config-group-policy)#
```

Étape 3

Configurez les paramètres de liste d'exceptions du proxy de navigateur pour un contournement local sur le périphérique client en saisissant la commande **msie-proxy except-list** en mode de configuration de stratégie de groupe. Ces adresses ne sont pas accessibles par un proxy. Cette liste correspond à la zone Exceptions dans la boîte de dialogue Paramètres de proxy.

```
hostname(config-group-policy)# msie-proxy except-list {value server[:port] | none}
hostname(config-group-policy)#
```

Pour supprimer l'attribut de la configuration, utilisez la forme **no** de la commande :

```
hostname(config-group-policy)# no msie-proxy except-list
hostname(config-group-policy)#
```

- **value server:port** : spécifie l'adresse IP ou le nom d'un serveur MSIE et le port appliqué à ce périphérique client. Le numéro de port est facultatif.
- **none** : indique qu'il n'y a pas d'adresse IP, de nom d'hôte ni de port et empêche d'hériter d'une liste d'exceptions.

Par défaut, **msie-proxy except-list** est désactivé.

La ligne contenant l'adresse IP ou le nom d'hôte du proxy et le numéro de port doit comporter moins de 100 caractères.

L'exemple suivant montre comment définir une liste d'exceptions de proxy de navigateur, composée du serveur à l'adresse IP 192.168.20.1, en utilisant le port 880, pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
hostname(config-group-policy)#
```

Étape 4

Activez ou désactivez les paramètres de contournement local du proxy de navigateur pour un périphérique client en saisissant la commande **msie-proxy local-bypass** en mode de configuration de stratégie de groupe.

```
hostname(config-group-policy)# msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

Pour supprimer l'attribut de la configuration, utilisez la forme **no** de la commande.

```
hostname(config-group-policy)# no msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

Par défaut, le contournement local du proxy est désactivé.

L'exemple suivant montre comment activer le contournement local du proxy de navigateur pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy local-bypass enable
hostname(config-group-policy)#
```

Configurer les attributs de sécurité pour les clients IPsec (IKEv1)

Pour spécifier les paramètres de sécurité pour un groupe, procédez comme suit.

Procédure

Étape 1

Précisez s'il faut autoriser les utilisateurs à enregistrer leurs mots de passe de connexion sur le système client, à l'aide de la commande **password-storage** avec le mot-clé **enable** en mode de configuration de stratégie de

groupe. Pour désactiver le stockage de mot de passe, utilisez la commande **password-storage** avec le mot-clé **disable**.

```
hostname(config-group-policy)# password-storage {enable | disable}
hostname(config-group-policy)#
```

Pour des raisons de sécurité, l'enregistrement des mots de passe est désactivé par défaut. Activez le stockage des mots de passe uniquement sur les systèmes que vous savez se trouver dans des sites sécurisés.

Pour supprimer l'attribut de stockage de mot de passe de la configuration en cours d'exécution, saisissez la forme **no** de cette commande :

```
hostname(config-group-policy)# no password-storage
hostname(config-group-policy)#
```

La spécification de cette forme **no** permet l'héritage d'une valeur de password-storage à partir d'une autre stratégie de groupe.

Cette commande ne s'applique pas à l'authentification interactive des clients matériels ni à l'authentification des utilisateurs individuels pour les clients matériels.

L'exemple suivant montre comment activer le stockage de mot de passe pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
hostname(config-group-policy)#
```

Étape 2

Précisez s'il faut activer la compression IP, qui est désactivée par défaut.

Remarque

La compression IP n'est pas prise en charge pour les connexions IPsec IKEv2.

```
hostname(config-group-policy)# ip-comp {enable | disable}
hostname(config-group-policy)#
```

Pour activer la compression IP LZS, entrez la commande **ip-comp** avec le mot-clé **enable** en mode de configuration de stratégie de groupe. Pour désactiver la compression IP, entrez la commande **ip-comp** avec le mot-clé **disable**.

Pour supprimer l'attribut **ip-comp** de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cela permet l'héritage d'une valeur d'une autre stratégie de groupe.

```
hostname(config-group-policy)# no ip-comp
hostname(config-group-policy)#
```

L'activation de la compression des données peut accélérer les débits de transmission de données pour les utilisateurs d'appels distants qui se connectent avec des modems.

Astuces

La compression des données augmente les besoins en mémoire et l'utilisation du processeur pour chaque session utilisateur et réduit par conséquent le débit global de l'ASA. Pour cette raison, nous vous recommandons

d'activer la compression des données uniquement pour les utilisateurs distants se connectant avec un modem. Concevez une stratégie de groupe spécifique aux utilisateurs de modem et activez la compression uniquement pour eux.

Étape 3

Précisez s'il faut exiger que les utilisateurs se réauthentifient lors du renouvellement IKE, à l'aide de la commande **re-xauth** avec le mot-clé **enable** en mode de configuration de stratégie de groupe.

Remarque

Le renouvellement IKE n'est pas pris en charge pour les connexions IKEv2.

Si vous activez la réauthentification lors du renouvellement IKE, l'ASA invite l'utilisateur à saisir un nom d'utilisateur et un mot de passe lors de la négociation initiale IKE de phase 1 et lui redemande également de s'authentifier à chaque renouvellement IKE. La réauthentification offre une sécurité supplémentaire.

Si l'intervalle de renouvellement configuré est très court, les utilisateurs peuvent trouver les demandes d'autorisation répétées peu pratiques. Pour éviter les demandes d'autorisation répétées, désactivez la réauthentification. Pour vérifier l'intervalle de renouvellement configuré, en mode de surveillance, saisissez la commande **show crypto ipsec sa** permettant d'afficher la durée de vie de l'association de sécurité en secondes et en kilo-octets de données. Pour désactiver la réauthentification de l'utilisateur lors du renouvellement IKE, saisissez le mot-clé **disable**. La réauthentification sur le renouvellement IKE est désactivée par défaut.

```
hostname(config-group-policy)# re-xauth {enable | disable}
hostname(config-group-policy)#
```

Pour activer l'héritité d'une valeur de réauthentification sur le renouvellement IKE à partir d'une autre stratégie de groupe, supprimez l'attribut re-xauth de la configuration en cours d'exécution en saisissant la forme **no** de cette commande :

```
hostname(config-group-policy)# no re-xauth
hostname(config-group-policy)#
```

Remarque

La réauthentification échoue s'il n'y a aucun utilisateur à l'autre extrémité de la connexion.

Étape 4

Précisez s'il faut activer la confidentialité de transmission parfaite. Dans les négociations IPsec, la confidentialité de transmission parfaite garantit que chaque nouvelle clé cryptographique n'est liée à aucune clé précédente. Une stratégie de groupe peut hériter d'une valeur de confidentialité de transmission parfaite d'une autre stratégie de groupe. La confidentialité de transmission parfaite est désactivée par défaut. Pour activer la confidentialité de transmission parfaite, utilisez la commande **pfs** avec le mot-clé **enable** en mode de configuration de stratégie de groupe.

```
hostname(config-group-policy)# pfs {enable | disable}
hostname(config-group-policy)#
```

Pour désactiver la confidentialité de transmission parfaite, entrez la commande **pfs** avec le mot-clé **disable**.

Pour supprimer l'attribut de confidentialité de transmission parfaite de la configuration en cours et éviter d'hériter d'une valeur, saisissez la forme **no** de cette commande.


```
hostname(config-group-policy)# no pfs
hostname(config-group-policy)#
```

Configurer les attributs IPsec-UDP pour les clients IKEv1

IPsec sur UDP, parfois appelé IPsec à travers NAT, permet à un client matériel de se connecter par UDP à un ASA qui exécute NAT. Il est désactivé par défaut. IPsec sur UDP est propriétaire ; il s'applique uniquement aux connexions d'accès à distance et nécessite une configuration de mode. L'ASA échange des paramètres de configuration avec le client pendant la négociation des SA. L'utilisation d'IPsec sur UDP peut dégrader légèrement les performances du système.

Pour activer IPsec sur UDP, configurez la commande **ipsec-udp** avec le mot-clé **enable** approprié en mode de configuration de stratégie de groupe, comme suit :

```
hostname(config-group-policy)# ipsec-udp {enable | disable}
hostname(config-group-policy)# no ipsec-udp
```

Pour utiliser IPsec sur UDP, vous devez également configurer la commande **ipsec-udp-port**, comme décrit dans cette section.

Pour désactiver IPsec sur UDP, saisissez le mot-clé **disable** . Pour supprimer l'attribut IPsec sur UDP de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cela permet l'hérité d'une valeur pour IPsec sur UDP provenant d'une autre stratégie de groupe.

L'exemple suivant montre comment définir IPsec sur UDP pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp enable
```

Si vous avez activé IPsec sur UDP, vous devez également configurer la commande **ipsec-udp-port** en mode de configuration de stratégie de groupe. Cette commande définit un numéro de port UDP pour IPsec sur UDP. Pendant les négociations IPsec, l'ASA écoute sur le port configuré et transfère le trafic UDP pour ce port même si d'autres règles de filtrage abandonnent le trafic UDP. Les numéros de port peuvent être compris entre 4001 et 49151. La valeur par défaut est 10000.

Pour désactiver le port UDP, saisissez la forme **no** de cette commande. Cela permet d'hériter d'une valeur pour le port IPsec sur UDP provenant d'une autre stratégie de groupe.

```
hostname(config-group-policy)# ipsec-udp-port port
```

L'exemple suivant montre comment définir un port UDP IPsec au port 4025 pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```

Configurer les attributs pour les clients de matériel VPN

Procédure

Étape 1 (Facultatif) Configurez le mode d'extension du réseau avec la commande suivante :

[no] nem [enable | disable]

Le mode d'extension du réseau permet aux clients matériels de présenter un réseau unique routable au réseau privé distant via le tunnel VPN. La PAT ne s'applique pas. Par conséquent, les périphériques derrière le serveur Easy VPN ont un accès direct aux périphériques du réseau privé derrière le client Easy VPN distant sur le tunnel et uniquement sur le tunnel, et vice versa. Le client matériel doit lancer le tunnel, mais une fois que le tunnel est opérationnel, l'un ou l'autre des côtés peut lancer l'échange de données.

Exemple :

L'exemple suivant montre comment définir NEM pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
```

Pour désactiver le protocole NEM, saisissez le mot-clé **disable** . Pour supprimer l'attribut NEM de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cette option permet l'hérité d'une valeur d'une autre stratégie de groupe.

Étape 2 (Facultatif) Configurez l'authentification de l'unité sécurisée avec la commande suivante :

[no] secure-unit-authentication [enable | disable]

L'authentification par unité sécurisée offre une sécurité supplémentaire en obligeant les clients de matériel VPN à s'authentifier à l'aide d'un nom d'utilisateur et d'un mot de passe chaque fois que le client amorce un tunnel. Avec cette fonctionnalité activée, le client matériel n'utilise pas le nom d'utilisateur et le mot de passe enregistrés. L'authentification par unité sécurisée est désactivée par défaut.

L'authentification par unité sécurisée nécessite que vous ayez un groupe de serveurs d'authentification configuré pour le profil de connexion utilisé par le ou les clients matériels. Si vous avez besoin d'une authentification par unité sécurisée sur l'appareil de sécurité adaptable Cisco principal, veillez à la configurer sur tous les serveurs de sauvegarde.

Remarque

Avec cette fonctionnalité activée, pour établir un tunnel VPN, un utilisateur doit être présent pour saisir le nom d'utilisateur et le mot de passe.

Exemple :

L'exemple suivant montre comment activer l'authentification par unité sécurisée pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)#group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-authentication enable
```

Pour désactiver l'authentification par unité sécurisée, saisissez le mot-clé **disable** . Pour supprimer l'attribut d'authentification par unité sécurisée de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cette option permet l'hérité d'une valeur pour l'authentification par unité sécurisée d'une autre stratégie de groupe.

Étape 3 (Facultatif) Configurez l'authentification des utilisateurs avec la commande suivante :

[no] user-authentication [enable | disable]

Lorsque cette option est activée, l'authentification des utilisateurs exige que les utilisateurs individuels derrière un client matériel s'authentifient pour obtenir l'accès au réseau via le tunnel. Les utilisateurs individuels s'authentifient en fonction de l'ordre des serveurs d'authentification que vous configurez. L'authentification des utilisateurs est désactivée par défaut.

Si vous avez besoin de l'authentification des utilisateurs sur l'appareil de sécurité adaptable Cisco principal, veuillez à la configurer sur tous les serveurs de sauvegarde.

Exemple :

L'exemple suivant montre comment activer l'authentification des utilisateurs pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
```

Pour désactiver l'authentification de l'utilisateur, saisissez le mot-clé **disable** . Pour supprimer l'attribut d'authentification de l'utilisateur de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cette option permet l'hérité d'une valeur pour l'authentification des utilisateurs d'une autre stratégie de groupe.

Étape 4 Définissez un délai d'inactivité pour les utilisateurs individuels qui se sont authentifiés avec la commande suivante :

[no] user-authentication-idle-timeout minutes | none]

Le paramètre *minutes* spécifie le nombre de minutes dans la période d'inactivité. Le minimum est de 1 minute, la valeur par défaut est de 30 minutes et le maximum est de 35 791 394 minutes.

S'il n'y a aucune activité de communication par un utilisateur derrière un client matériel pendant la période d'inactivité, l'ASA met fin à l'accès du client. Cette minuterie met fin uniquement à l'accès du client par le tunnel VPN, et non au tunnel VPN lui-même.

Exemple :

L'exemple suivant montre comment définir une valeur de délai d'inactivité de 45 minutes pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
hostname(config-group-policy)# user-authentication-idle-timeout 45
```

Pour supprimer la valeur de délai d'inactivité, saisissez la forme **no** de cette commande. Cette option permet l'hérité d'une valeur de délai d'inactivité d'une autre stratégie de groupe. Pour éviter d'hériter d'une valeur de délai d'inactivité, entrez la commande **user-authentication-idle-timeout** avec le mot-clé **none** . Cette commande définit le délai d'inactivité avec une valeur nulle, ce qui désactive le délai d'inactivité et empêche l'hérité d'une valeur de délai d'inactivité d'authentification d'utilisateur à partir d'une politique par défaut ou d'un groupe spécifié.

Remarque

Le délai d'inactivité indiqué en réponse à la commande **show uauth** est toujours la valeur du délai d'inactivité de l'utilisateur qui a authentifié le tunnel sur le périphérique distant du VPN Cisco Easy.

Étape 5 Configurez le contournement des téléphones IP avec la commande suivante :

ip-phone-bypass enable

Le contournement du téléphone IP permet aux téléphones IP derrière les clients matériels de se connecter sans subir les processus d'authentification des utilisateurs. Le contournement du téléphone IP est désactivé par défaut. Cela s'applique uniquement lorsque l'IUA est activée.

Remarque

Vous devez également configurer l'exemption d'adresse MAC sur le client pour exempter ces clients de l'authentification.

Pour désactiver le contournement du téléphone IP, saisissez le mot-clé **disable**. Pour supprimer l'attribut de contournement du téléphone IP de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cette option permet l'héritage d'une valeur pour le contournement du téléphone IP d'une autre stratégie de groupe.

Étape 6

Configurez le contournement LEAP avec la commande suivante :

leap-bypass enable

Le contournement LEAP s'applique uniquement lorsque **user-authentication** est activée. Cette commande permet aux paquets LEAP des périphériques de point d'accès sans fil Cisco d'établir l'authentification LEAP, puis de s'authentifier à nouveau par authentification de l'utilisateur. Le contournement LEAP est désactivé par défaut.

Les utilisateurs LEAP derrière un client matériel ont un dilemme circulaire : ils ne peuvent pas négocier l'authentification LEAP, car ils ne peuvent pas envoyer leurs informations d'authentification au serveur RADIUS derrière le périphérique de site central sur le tunnel. La raison pour laquelle ils ne peuvent pas envoyer leurs informations d'authentification sur le tunnel est qu'ils ne se sont pas authentifiés sur le réseau sans fil. Pour résoudre ce problème, le contournement LEAP permet aux paquets LEAP, et uniquement aux paquets LEAP, de traverser le tunnel pour authentifier la connexion sans fil avec un serveur RADIUS avant que les utilisateurs individuels ne s'authentifient. Les utilisateurs procèdent ensuite à l'authentification individuelle des utilisateurs.

Le contournement LEAP fonctionne correctement dans les conditions suivantes :

- **secure-unit-authentication** doit être désactivé. Si l'authentification de l'unité interactive est activée, un périphérique non LEAP (filaire) doit authentifier le client matériel avant que les périphériques LEAP puissent se connecter en utilisant ce tunnel.
- **user-authentication** est activé. Sinon, le contournement LEAP ne s'applique pas.
- Les points d'accès dans l'environnement sans fil doivent être des points d'accès Cisco Aironet exécutant le protocole de découverte Cisco (CDP). Les cartes réseau (NIC) sans fil pour PC peuvent être d'autres marques.

Exemple :

L'exemple suivant montre comment définir le contournement LEAP pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
hostname(config-group-policy)# leap-bypass enable
```

Pour désactiver le contournement LEAP, saisissez le mot-clé **disable**. Pour supprimer l'attribut de contournement LEAP de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cette option permet l'héritage d'une valeur pour le contournement LEAP d'une autre stratégie de groupe :

Configurer les attributs de stratégie de groupe pour les connexions Secure Client (services client sécurisés)

Après avoir activé les connexions Secure Client (services client sécurisés) comme décrit dans [Connexions du client VPN AnyConnect, à la page 235](#), vous pouvez activer ou exiger les fonctionnalités Secure Client (services client sécurisés) pour une stratégie de groupe. Suivez ces étapes en mode de configuration webvpn de stratégie de groupe :

Procédure

Étape 1 Entrez le mode de configuration webvpn de stratégie de groupe. Par exemple :

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
```

Étape 2 Pour désactiver l'installation permanente du Secure Client (services client sécurisés) sur l'ordinateur terminal, utilisez la commande AnyConnect keep-install avec le mot-clé **none**. Par exemple :

```
hostname(config-group-webvpn)# anyconnect keep-installer none
hostname(config-group-webvpn)#
```

La valeur par défaut est que l'installation permanente du client est activée. Le client reste installé sur le point terminal à la fin de la session Secure Client (services client sécurisés).

Étape 3 Pour activer la compression des données HTTP sur la connexion SSL Secure Client (services client sécurisés) pour la stratégie de groupe, saisissez la commande AnyConnect ssl compression. Par défaut, la compression est définie sur **none** (désactivé). Pour activer la compression, utilisez le mot-clé **deflate**. Par exemple :

```
hostname(config-group-webvpn)# anyconnect compression deflate
hostname(config-group-webvpn)#
```

Étape 4 [Configurer, à la page 251](#)

Étape 5 Vous pouvez vous assurer que la connexion Secure Client (services client sécurisés) par l'intermédiaire d'un proxy, d'un pare-feu ou d'un périphérique NAT reste ouverte, même si le périphérique limite la durée pendant laquelle la connexion peut être inactive, en ajustant la fréquence des messages keepalive à l'aide de la commande **anyconnect ssl keepalive command**:

anyconnect ssl keepalive {none | seconds}

Le réglage de keepalives garantit également que Secure Client (services client sécurisés) ne se déconnecte pas et ne se reconnecte pas lorsque l'utilisateur distant n'exécute pas activement une application basée sur des sockets, comme Microsoft Outlook ou Microsoft Internet Explorer.

L'exemple suivant configure l'appareil de sécurité pour activer Secure Client (services client sécurisés) afin d'envoyer des messages keepalive, avec une fréquence de 300 secondes (5 minutes) :

```
hostname(config-group-webvpn) # anyconnect ssl keepalive 300
hostname(config-group-webvpn) #
```

Étape 6 Pour permettre à Secure Client (services client sécurisés) d'effectuer un renouvellement sur une session SSL, utilisez la commande AnyConnect ssl rekey :

```
AnyConnect ssl rekey {method {ssl | new-tunnel} | time minutes | none}}
```

Par défaut, le renouvellement est désactivé.

La définition de la méthode en tant que new-tunnel spécifie que Secure Client (services client sécurisés) établit un nouveau tunnel pendant le renouvellement SSL. La spécification de la méthode comme aucune désactive le renouvellement. La définition de la méthode en tant que SSL indique que la renégociation SSL a lieu pendant le renouvellement. Au lieu de préciser la méthode, vous pouvez préciser l'heure : c'est-à-dire le nombre de minutes entre le début de la session et le renouvellement, de 1 à 10 080 (1 semaine).

L'exemple suivant configure Secure Client (services client sécurisés) pour renégocier avec SSL pendant le renouvellement et configure le renouvellement pour qu'il se produise 30 minutes après le début de la session :

```
hostname(config-group-webvpn) # anyconnect ssl rekey method ssl
hostname(config-group-webvpn) # anyconnect ssl rekey time 30
hostname(config-group-webvpn) #
```

Étape 7 La fonctionnalité Client Protocol Bypass vous permet de configurer la façon dont Secure Client (services client sécurisés) gère le trafic IPv4 lorsque l'ASA s'attend uniquement à du trafic IPv6 ou comment il gère le trafic IPv6 lorsqu'il s'attend uniquement à du trafic IPv4.

Lorsque Secure Client (services client sécurisés) établit une connexion VPN avec l'ASA, l'ASA peut lui attribuer une adresse IPv4, IPv6 ou à la fois une adresse IPv4 et IPv6. Si l'ASA attribue à la connexion Secure Client (services client sécurisés) uniquement une adresse IPv4 ou uniquement une adresse IPv6, vous pouvez maintenant configurer le protocole de contournement du client pour rejeter le trafic réseau pour lequel l'ASA n'a pas attribué d'adresse IP, ou permettre à ce trafic de contourner l'ASA et d'être envoyé par le client non chiffré ou « en clair ».

Par exemple, supposons que l'ASA attribue uniquement une adresse IPv4 à la connexion Secure Client (services client sécurisés) et que le point terminal soit en double pile. Lorsque le point terminal tente d'atteindre une adresse IPv6, si le protocole de contournement des clients est désactivé, le trafic IPv6 est abandonné; cependant, si le protocole de contournement client est activé, le trafic IPv6 est envoyé par le client en clair.

Si vous établissez un tunnel IPsec (par opposition à une connexion SSL), l'ASA n'est pas informé si IPv6 est activé ou non sur le client, donc l'ASA applique toujours le paramètre du protocole de contournement du client.

Utilisez la commande client-bypass-protocol pour activer ou désactiver la fonctionnalité du protocole de contournement du client. Voici la syntaxe de la commande :

```
client-bypass-protocol {enable | disable}
```

L'exemple suivant active le protocole de contournement du client :

```
hostname(config-group-policy) # client-bypass-protocol enable
hostname(config-group-policy) #
```

L'exemple suivant désactive le protocole de contournement du client :

```
hostname(config-group-policy) # client-bypass-protocol disable
hostname(config-group-policy) #
```

L'exemple suivant supprime un paramètre de protocole de contournement du client activé ou désactivé :

```
hostname(config-group-policy) # no client-bypass-protocol enable
hostname(config-group-policy) #
```

Étape 8

Si vous avez configuré l'équilibrage de charge entre vos périphériques ASA, spécifiez le FQDN de l'ASA afin de résoudre l'adresse IP de l'ASA utilisée pour rétablir la session VPN. Ce paramètre est essentiel pour prendre en charge l'itinérance des clients entre les réseaux de différents protocoles IP (comme IPv4 à IPv6).

Vous ne pouvez pas utiliser le FQDN de l'ASA présent dans le profil Secure Client (services client sécurisés) pour obtenir l'adresse IP de l'ASA après l'itinérance. Les adresses peuvent ne pas correspondre au bon périphérique (ce dernier vers lequel le tunnel a été établi) dans le scénario d'équilibrage de charge.

Si le nom de domaine complet du périphérique n'est pas transmis au client, le client tentera de se reconnecter à l'adresse IP que le tunnel avait précédemment établie. Afin de prendre en charge l'itinérance entre les réseaux de différents protocoles IP (de IPv4 à IPv6), Secure Client (services client sécurisés) doit effectuer la résolution de nom du FQDN du périphérique après l'itinérance, afin de pouvoir déterminer quelle adresse ASA utiliser pour rétablir le tunnel. Le client utilise le nom de domaine complet ASA présent dans son profil lors de la connexion initiale. Lors des reconnections de session ultérieures, il utilise toujours le nom de domaine complet du périphérique transmis par l'ASA (et configuré par l'administrateur dans la stratégie de groupe), le cas échéant. Si le nom de domaine complet n'est pas configuré, l'ASA détermine le nom de domaine complet du périphérique (et l'envoie au client) de tout ce qui est défini sous Configuration > Device Setup (Configuration du périphérique) > Device Name/Password and Domain Name (Nom du périphérique/mot de passe et nom de domaine).

Si le nom de domaine complet du périphérique n'est pas poussé par l'ASA, le client ne peut pas rétablir la session VPN après avoir effectué l'itinérance entre les réseaux de protocoles IP différents.

Utilisez la commande `gateway-fqdn` pour configurer le nom de domaine complet de l'ASA. Voici la syntaxe de la commande :

gateway-fqdn { value *FQDN_Name* | none } or no gateway-fqdn

L'exemple suivant définit le nom de domaine complet de l'ASA comme `ASAName.example.cisco.com`

```
hostname(config-group-policy) # gateway-fqdn value ASAName.example.cisco.com
hostname(config-group-policy) #
```

L'exemple suivant supprime le nom de domaine complet de l'ASA de la stratégie de groupe. La stratégie de groupe hérite ensuite de cette valeur de la stratégie de groupe par défaut.

```
hostname(config-group-policy) # no gateway-fqdn
hostname(config-group-policy) #
```

L'exemple suivant définit le nom de domaine complet comme une valeur vide. Le nom de domaine complet configuré à l'aide des commandes `hostname` et `domain-name` sera utilisé s'il est disponible.

```
hostname(config-group-policy) # gateway-fqdn none
```

```
hostname (config-group-policy) #
```

Configurer les attributs du serveur de sauvegarde

Configurez les serveurs de sauvegarde si vous prévoyez de les utiliser. Les serveurs de sauvegarde IPsec permettent à un client VPN de se connecter au site central lorsque l'ASA principal n'est pas disponible. Lorsque vous configurez les serveurs de sauvegarde, l'ASA transmet la liste des serveurs au client pendant l'établissement du tunnel IPsec. Les serveurs de sauvegarde n'existent pas tant que vous ne les avez pas configurés, que ce soit sur le client ou sur l'ASA principal.

Configurez les serveurs de sauvegarde sur le client ou sur l'ASA principal. Si vous configurez des serveurs de sauvegarde sur l'ASA, l'ASA transmet la liste des serveurs au client vers les clients du groupe, en remplacement de la liste de serveurs de sauvegarde sur le client si elle est configurée.



Remarque

Si vous utilisez des noms d'hôte, il est conseillé d'avoir des serveurs DNS et WINS de secours sur un réseau distinct de celui des serveurs DNS et WINS principaux. Sinon, si les clients derrière un client matériel obtiennent des informations DNS et WINS du client matériel par DHCP, et que la connexion au serveur principal est perdue, et que les serveurs de secours utilisent des informations DNS et WINS différentes, les clients ne peuvent pas être mis à jour tant que le bail DHCP n'expire pas. En outre, si vous utilisez des noms d'hôte et que le serveur DNS n'est pas disponible, des retards importants peuvent se produire.

Pour configurer les serveurs de sauvegarde, saisissez la commande **backup-servers** en mode de configuration de stratégie de groupe :

```
hostname (config-group-policy) # backup-servers {server1 server2... server10 |  
clear-client-config | keep-client-config}
```

Pour supprimer un serveur de sauvegarde, saisissez la forme **no** de cette commande avec le serveur de sauvegarde spécifié. Pour supprimer l'attribut backup-servers de la configuration en cours d'exécution et activer l'hérité d'une valeur pour backup-servers d'une autre stratégie de groupe, saisissez la forme **no** de cette commande sans arguments.

```
hostname (config-group-policy) # no backup-servers [server1 server2... server10 |  
clear-client-config | keep-client-config]
```

Le mot-clé **clear-client-config** spécifie que le client n'utilise aucun serveur de sauvegarde. L'ASA transmet une liste de serveurs vide.

Le mot-clé **keep-client-config** spécifie que l'ASA n'envoie aucune information sur les serveurs de sauvegarde. Le client utilise sa propre liste de serveurs de sauvegarde, le cas échéant. Il s'agit du paramètre par défaut.

La liste de paramètres *server1 server 2.... server10* est une liste de serveurs délimités par des espaces et ordonnés par priorité pour le client VPN à utiliser lorsque l'ASA principal n'est pas disponible. Cette liste identifie les serveurs par adresse IP ou nom d'hôte. La liste peut comporter 500 caractères et contenir jusqu'à 10 entrées.

L'exemple suivant montre comment configurer les serveurs de sauvegarde avec les adresses IP 10.10.10.1 et 192.168.10.14, pour la stratégie de groupe nommée FirstGroup :


```
hostname (config) # group-policy FirstGroup attributes
hostname (config-group-policy) # backup-servers 10.10.10.1 192.168.10.14
```

Configurer les paramètres du contrôle d'admission au réseau

Les commandes NAC de stratégie de groupe dans cette section ont toutes des valeurs par défaut. Sauf si vous avez une bonne raison de les modifier, acceptez les valeurs par défaut pour ces paramètres.

L'ASA utilise la messagerie EAP (Extensible Authentication Protocol) sur UDP (EAPoUDP) pour valider la posture des hôtes distants. La validation de posture consiste à vérifier qu'un hôte distant est conforme aux exigences de sécurité avant l'attribution d'une politique d'accès réseau. Un serveur de contrôle d'accès doit être configuré pour le contrôle d'admission au réseau avant de configurer la NAC sur l'appareil de sécurité.

Le serveur de contrôle d'accès télécharge le jeton de posture, une chaîne de texte d'information configurable sur l'ACS, vers le périphérique de sécurité afin d'aider à la surveillance du système, au reporting, au débogage et à la journalisation. Un jeton de posture typique est Healthy (En bonne santé), Checkup (Contrôle), Quarantine (Quarantaine), Infected (Infecté) ou Unknown (Inconnu). Après la validation de la posture ou l'authentification sans client, l'ACS télécharge la politique d'accès de la session sur l'appareil de sécurité.

Pour configurer les paramètres de contrôle d'admission au réseau pour la stratégie de groupe par défaut ou une autre stratégie de groupe, procédez comme suit.

Procédure

Étape 1

(Facultatif) Configurez la période de la minuterie de requête d'état. L'appareil de sécurité démarre la minuterie de requête d'état après chaque validation de posture et réponse à la requête d'état réussies. L'expiration de cette minuterie déclenche une requête pour les modifications de la posture de l'hôte, appelée requête d'état. Saisissez le nombre de secondes dans une plage de 30 à 1 800. Le paramètre par défaut est 300.

Pour préciser l'intervalle entre chaque validation de posture réussie dans une session de contrôle d'admission du réseau et la prochaine requête pour modifications de la posture d'hôte, utilisez la commande **nac-sq-period** en mode de configuration de stratégie de groupe :

```
hostname (config-group-policy) # nac-sq-period seconds
hostname (config-group-policy) #
```

Pour hériter de la valeur du minuteur de requête d'état depuis la stratégie de groupe par défaut, accédez à l'autre stratégie de groupe depuis laquelle vous souhaitez hériter, puis utilisez la forme **no** de cette commande :

```
hostname (config-group-policy) # no nac-sq-period [seconds]
hostname (config-group-policy) #
```

L'exemple suivant modifie la valeur de la minuterie de requête d'état à 1 800 secondes :

```
hostname (config-group-policy) # nac-sq-period 1800
hostname (config-group-policy) #
```

L'exemple suivant hérite de la valeur du minuteur de requête d'état depuis la stratégie de groupe par défaut :

```
hostname (config-group-policy) # no nac-sq-period
```

```
hostname (config-group-policy) #
```

Étape 2

(Facultatif) Configurez la période de revalidation de la NAC. L'appareil de sécurité démarre la minuterie de revalidation après chaque validation de posture réussie. L'expiration de cette minuterie déclenche la prochaine validation de posture inconditionnelle. L'appareil de sécurité conserve la validation de la posture pendant la revalidation. La stratégie de groupe par défaut entre en vigueur si le serveur de contrôle d'accès n'est pas disponible pendant la validation ou la revalidation de la posture. Saisissez l'intervalle en secondes entre chaque validation de posture réussie. La plage est de 300 à 86 400. Le paramètre par défaut est 36 000.

Pour préciser l'intervalle entre chaque validation de posture réussie dans une session de contrôle d'admission du réseau, utilisez la commande **nac-reval-period** en mode de configuration de stratégie de groupe :

```
hostname (config-group-policy) # nac-reval-period seconds
hostname (config-group-policy) #
```

Pour hériter de la valeur du minuteur de revalidation depuis la stratégie de groupe par défaut, accédez à l'autre stratégie de groupe depuis laquelle vous souhaitez hériter, puis utilisez la forme **no** de cette commande :

```
hostname (config-group-policy) # no nac-reval-period [seconds]
hostname (config-group-policy) #
```

L'exemple suivant modifie la minuterie de revalidation à 86 400 secondes :

```
hostname (config-group-policy) # nac-reval-period 86400
hostname (config-group-policy)
```

L'exemple suivant hérite de la valeur du délai de revalidation de la stratégie de groupe par défaut :

```
hostname (config-group-policy) # no nac-reval-period
hostname (config-group-policy) #
```

Étape 3

(Facultatif) Configurez l'ACL par défaut pour la NAC. L'appareil de sécurité applique la politique de sécurité associée à l'ACL sélectionnée si la validation de la posture échoue. Spécifiez **none** ou une liste de contrôle d'accès étendue. Le paramètre par défaut est **none**. Si le paramètre est **none** et que la validation de la posture échoue, l'appareil de sécurité applique la stratégie de groupe par défaut.

Pour spécifier la liste de contrôle d'accès à utiliser comme liste de contrôle d'accès par défaut pour les sessions de contrôle d'admission au réseau qui échouent à la validation de la posture, utilisez la commande **nac-default-acl** en mode de configuration de stratégie de groupe :

```
hostname (config-group-policy) # nac-default-acl {acl-name | none}
hostname (config-group-policy) #
```

Pour hériter de l'ACL de la stratégie de groupe par défaut, accédez à l'autre stratégie de groupe à partir de laquelle l'hériter, puis utilisez la forme **no** de cette commande :

```
hostname (config-group-policy) # no nac-default-acl [acl-name | none]
hostname (config-group-policy) #
```

Les éléments de cette commande sont les suivants :

- **acl-name** : spécifie le nom du groupe de serveurs de validation de posture, tel qu'il est configuré sur l'ASA à l'aide de la commande **aaa-server host**. Le nom doit correspondre à la variable de balise de serveur spécifiée dans cette commande.
- **none** : désactive l'hérité de l'ACL de la stratégie de groupe par défaut et n'applique pas d'ACL aux sessions de la NAC qui échouent la validation de la posture.

Comme la NAC est désactivée par défaut, le trafic VPN traversant l'ASA n'est pas soumis à l'ACL par défaut de la NAC tant que la NAC n'est pas activée.

L'exemple suivant identifie **acl-1** comme liste de contrôle d'accès à appliquer lorsque la validation de la posture échoue :

```
hostname(config-group-policy)# nac-default-acl acl-1
hostname(config-group-policy)#
```

L'exemple suivant hérite de l'ACL de la stratégie de groupe par défaut :

```
hostname(config-group-policy)# no nac-default-acl
hostname(config-group-policy)#
```

L'exemple suivant désactive l'hérité de l'ACL de la stratégie de groupe par défaut et n'applique pas d'ACL aux sessions de la NAC qui échouent la validation de la posture :

```
hostname(config-group-policy)# nac-default-acl none
hostname(config-group-policy)#
```

Étape 4

Configurer des exemptions NAC pour le VPN Par défaut, la liste d'exemptions est vide. La valeur par défaut de l'attribut de filtre est **none**. Saisissez la **commande vpn-nac-exempt** une fois pour chaque système d'exploitation (et liste de contrôle d'accès) à mettre en correspondance afin d'exempter les hôtes distants de la validation de la posture.

Pour ajouter une entrée à la liste des types d'ordinateurs distants qui sont exemptés de la validation de la posture, utilisez la commande **vpn-nac-exempt** en mode de configuration de stratégie de groupe :

```
hostname(config-group-policy)# vpn-nac-exempt os "os name" [filter {acl-name | none}]
[disable]
hostname(config-group-policy)#
```

Pour désactiver l'hérité et préciser que tous les hôtes sont soumis à la validation de la posture, utilisez le mot-clé **none** immédiatement après **vpn-nac-exempt** :

```
hostname(config-group-policy)# vpn-nac-exempt none
hostname(config-group-policy)#
```

Pour supprimer une entrée de la liste d'exemptions, utilisez la forme **no** de cette commande et nommez le système d'exploitation (et l'ACL) dans l'entrée à supprimer :

```
hostname(config-group-policy)# no vpn-nac-exempt [os "os name"] [filter {acl-name | none}]
[disable]
hostname(config-group-policy)#
```

Pour supprimer toutes les entrées de la liste d'exemptions associée à cette stratégie de groupe et hériter de la liste de la stratégie de groupe par défaut, utilisez la forme **no** de cette commande sans préciser de mots-clés supplémentaires :

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)#
```

Les éléments de syntaxe de ces commandes sont les suivants :

- **acl-name** : nom de l'ACL présente dans la configuration ASA.
- **disable** : désactive l'entrée dans la liste d'exemptions sans la supprimer de la liste.
- **filter** : (facultatif) Appliquez une ACL pour filtrer le trafic si l'ordinateur correspond au nom du système d'exploitation.
- **none** : lorsqu'il est saisi immédiatement après **vpn-nac-exempt**, ce mot-clé désactive l'hérité et spécifie que tous les hôtes sont soumis à la validation de la posture. Lorsqu'il est saisi immédiatement après **le filtre**, ce mot-clé indique que l'entrée ne spécifie pas d'ACL.
- **OS(système d'exploitation)** : exempté un système d'exploitation de la validation de la posture.
- **os name** : nom du système d'exploitation. Les guillemets sont requis uniquement si le nom comprend un espace (par exemple, « Windows XP »).

L'exemple suivant désactive l'hérité et spécifie que tous les hôtes seront soumis à la validation de la posture :

```
hostname(config-group-policy)# no vpn-nac-exempt none
hostname(config-group-policy)#
```

L'exemple suivant supprime toutes les entrées de la liste d'exemptions :

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)#
```

Étape 5

Activez ou désactivez le contrôle d'admission au réseau en entrant la commande suivante :

```
hostname(config-group-policy)# nac {enable | disable}
hostname(config-group-policy)#
```

Pour hériter du paramètre NAC de la stratégie de groupe par défaut, accédez à l'autre stratégie de groupe à partir de laquelle l'hériter, puis utilisez la forme **no** de cette commande :

```
hostname(config-group-policy)# no nac [enable | disable]
hostname(config-group-policy)#
```

Par défaut, la NAC est désactivée. L'activation de la NAC nécessite une validation de la posture pour l'accès à distance. Si l'ordinateur distant réussit les vérifications de validation, le serveur ACS télécharge la politique d'accès pour que l'ASA l'applique. La NAC est désactivée par défaut.

Un serveur de contrôle d'accès doit être présent sur le réseau.

L'exemple suivant active la NAC pour la stratégie de groupe :

```
hostname(config-group-policy)# nac enable  
hostname(config-group-policy)#
```

Configurer les politiques de pare-feu des clients VPN

Un pare-feu isole et protège un ordinateur contre Internet en inspectant chaque paquet de données entrant et sortant pour déterminer s'il faut l'autoriser à passer par le pare-feu ou l'abandonner. Les pare-feu offrent une sécurité supplémentaire si les utilisateurs distants d'un groupe ont configuré la tunnellation fractionnée. Dans ce cas, le pare-feu protège l'ordinateur de l'utilisateur, et, par conséquent, le réseau d'entreprise, contre les intrusions par Internet ou le réseau local (LAN) de l'utilisateur. Les utilisateurs distants se connectant à l'ASA avec le client VPN peuvent choisir l'option de pare-feu appropriée.

Définissez les politiques de pare-feu personnelles que l'ASA transmet au client VPN lors de la négociation du tunnel IKE à l'aide de la commande **client-firewall** en mode de configuration de stratégie de groupe. Pour supprimer une politique de pare-feu, entrez la forme **no** de cette commande.

Pour supprimer toutes les politiques de pare-feu, entrez la commande **no client-firewall** sans arguments. Cette commande supprime toutes les politiques de pare-feu configurées, y compris une politique nulle si vous en avez créé une en saisissant la commande **client-firewall** avec le mot-clé **none**.

En l'absence de politiques de pare-feu, les utilisateurs héritent de celles qui existent dans la politique par défaut ou dans une autre stratégie de groupe. Pour empêcher les utilisateurs d'hériter de ces politiques de pare-feu, entrez la commande **client-firewall** avec le mot-clé **none**.

La boîte de dialogue Ajouter ou Modifier une stratégie de groupe sous l'onglet Pare-feu client vous permet de configurer les paramètres de pare-feu pour les clients VPN pour la stratégie de groupe en cours d'ajout ou de modification.



Remarque

Seuls les clients VPN exécutant Microsoft Windows peuvent utiliser ces paramètres de pare-feu. Ils ne sont actuellement pas disponibles pour les clients matériels ou autres clients logiciels (non Windows).

Dans le premier scénario, un utilisateur distant dispose d'un pare-feu personnel installé sur le PC. Le client VPN applique la politique de pare-feu définie sur le pare-feu local et il surveille ce pare-feu pour s'assurer qu'il est en cours d'exécution. Si le pare-feu arrête de s'exécuter, le client VPN abandonne la connexion à l'ASA. (Ce mécanisme d'application du pare-feu est appelé Are You There (AYT), car le client VPN surveille le pare-feu en lui envoyant périodiquement des messages « are you there? » ; si aucune réponse n'est reçue, le client VPN sait que le pare-feu est hors service et met fin à sa connexion à l'ASA.) L'administrateur réseau peut configurer ces pare-feu de PC à l'origine, mais avec cette approche, chaque utilisateur peut personnaliser sa propre configuration.

Dans le deuxième scénario, vous pourriez préférer appliquer une politique de pare-feu centralisée pour les pare-feu personnels sur les PC clients VPN. Un exemple courant serait de bloquer le trafic Internet vers les PC distants d'un groupe à l'aide de la tunnellation fractionnée. Cette approche protège les PC, et donc le site central, contre les intrusions d'Internet pendant l'établissement des tunnels. Ce scénario de pare-feu est appelé politique poussée ou politique de protection centrale (CPP). Sur l'ASA, vous créez un ensemble de règles de gestion du trafic à appliquer au client VPN, vous associez ces règles à un filtre, puis vous désignez ce filtre comme politique de pare-feu. L'ASA transfère cette politique au client VPN. Le client VPN transmet ensuite la politique au pare-feu local, qui l'applique.

Configurer les politiques de pare-feu pour Secure Client (services client sécurisés)

Les règles de pare-feu pour Secure Client (services client sécurisés) peuvent préciser des adresses IPv4 et IPv6.

Avant de commencer

Vous avez créé des règles d'accès unifiées avec des adresses IPv6 spécifiées.

Procédure

-
- Étape 1** Entrez en mode de configuration de stratégie de groupe webvpn.
- webvpn**
- Exemple :**
- ```
hostname(config)# group-policy ac-client-group attributes
hostname(config-group-policy)# webvpn
```
- Étape 2** Précisez une règle de contrôle d'accès pour la règle de réseau privé ou public. La règle de réseau privé est la règle appliquée à l'interface d'adaptateur virtuel VPN sur le client.
- AnyConnect firewall-rule client-interface {private | public} value [RuleName]**
- ```
hostname(config-group-webvpn)# anyconnect firewall-rule client-interface private value ClientFWRule
```
- Étape 3** Affichez les attributs de la stratégie de groupe ainsi que l'attribut de politique webvpn pour la stratégie de groupe.
- show runn group-policy [value]**
- Exemple :**
- ```
hostname(config-group-webvpn)# show run group-policy FirstGroup
group-policy FirstGroup internal
group-policy FirstGroup attributes
webvpn
 anyconnect firewall-rule client-interface private value ClientFWRule
```
- Étape 4** Supprimez la règle de pare-feu client de la règle de réseau privé.
- no anyconnect firewall-rule client-interface private value [RuleName]**
- Exemple :**
- ```
hostname(config-group-webvpn)# no anyconnect firewall-rule client-interface private value
hostname(config-group-webvpn)#
```
-

Utiliser un serveur Zone Labs Integrity.

Cette section présente le serveur Zone Labs Integrity, également appelé serveur Check Point Integrity, et fournit un exemple de procédure de configuration de l'ASA pour prendre en charge le serveur Zone Labs Integrity. Le serveur Integrity est un poste de gestion centralisé pour la configuration et l'application des politiques de sécurité sur les ordinateurs distants. Si un PC distant ne se conforme pas à la politique de sécurité dictée par le serveur Integrity, il ne peut pas accéder au réseau privé protégé par le serveur Integrity et l'ASA.

Le logiciel client VPN et le logiciel client Integrity résident sur le même ordinateur distant. Les étapes suivantes résument les actions du PC distant, de l'ASA et du serveur Integrity dans l'établissement d'une session entre le PC et le réseau privé d'entreprise :

1. Le logiciel client VPN (résidant sur le même ordinateur distant que le logiciel client Integrity) se connecte à l'ASA et indique à ce dernier de quel type de client de pare-feu il s'agit.
2. Une fois que l'ASA a approuvé le type de pare-feu du client, l'ASA transmet les informations d'adresse du serveur Integrity au client Integrity.
3. Lorsque l'ASA agit comme proxy, le client Integrity établit une connexion restreinte avec le serveur Integrity. Une connexion restreinte existe uniquement entre le client Integrity et le serveur Integrity.
4. Le serveur Integrity détermine si le client Integrity est conforme aux politiques de sécurité obligatoires. Si le client Integrity est conforme aux politiques de sécurité, le serveur Integrity demande à l'ASA d'ouvrir la connexion et de fournir au client Integrity les détails de la connexion.
5. Sur le PC distant, le client VPN transmet les détails de la connexion au client Integrity et signale que l'application de la politique doit commencer immédiatement et que le client Integrity peut accéder au réseau privé.
6. Une fois la connexion VPN établie, le serveur Integrity continue de surveiller l'état du client Integrity à l'aide de messages de pulsation du client.



Remarque

La version actuelle de l'ASA prend en charge un seul serveur Integrity à la fois, même si les interfaces utilisateur permettent de configurer jusqu'à cinq serveurs Integrity. Si le serveur Integrity actif tombe en panne, configurez-en un autre sur l'ASA, puis rétablissez la session client VPN.

Pour configurer le serveur Integrity, procédez comme suit :

Procédure

Étape 1

Configurez un serveur Integrity en utilisant l'adresse IP 10.0.0.5.

```
zonelabs-Integrity server-address {hostname1 | ip-address1}
```

Exemple :

```
hostname(config)# zonelabs-Integrity server-address 10.0.0.5
```

Étape 2

Précisez le port 300 (le port par défaut est 5054).

```
zonelabs-integrity port port-number
```

Exemple :

```
hostname(config)# zonelabs-integrity port 300
```

Étape 3

Précisez l'interface interne pour les communications avec le serveur Integrity.

```
zonelabs-integrity interface interface
```

Exemple :

```
hostname(config)# zonelabs-integrity interface inside
```

Étape 4

Assurez-vous que l'ASA attend 12 secondes une réponse du serveur Integrity actif ou de secours avant de déclarer le serveur Integrity défaillant et de fermer les connexions des clients VPN.

Remarque

Si la connexion entre l'ASA et le serveur Integrity échoue, les connexions du client VPN restent ouvertes par défaut afin que le VPN d'entreprise ne soit pas interrompu par la défaillance d'un serveur Integrity. Cependant, vous pourriez vouloir fermer les connexions VPN si le serveur Zone Labs Integrity tombe en panne.

```
zonelabs-integrity fail-timeout timeout
```

Exemple :

```
hostname(config)# zonelabs-integrity fail-timeout 12
```

Étape 5

Configurez l'ASA de sorte que les connexions aux clients VPN se terminent lorsque la connexion entre l'ASA et le serveur Zone Labs Integrity échoue.

```
zonelabs-integrity fail-close
```

Exemple :

```
hostname(config)# zonelabs-integrity fail-close
```

Étape 6

Rétablissez l'état d'échec configuré de la connexion des clients VPN à sa valeur par défaut et assurez-vous que les connexions des clients restent ouvertes.

```
zonelabs-integrity fail-open
```

Exemple :

```
hostname(config)# zonelabs-integrity fail-open
```

Étape 7

Précisez que le serveur Integrity se connecte au port 300 (la valeur par défaut est le port 80) de l'ASA pour demander le certificat SSL du serveur.

```
zonelabs-integrity ssl-certificate-port cert-port-number
```

Exemple :

```
hostname(config)# zonelabs-integrity ssl-certificate-port 300
```

Étape 8

Alors que le certificat SSL du serveur est toujours authentifié, spécifiez que le certificat SSL client du serveur Integrity doit être authentifié.

```
zonelabs-integrity ssl-client-authentication {enable | disable}
```


Exemple :

```
hostname(config)# zonelabs-integrity ssl-client-authentication enable
```

Définir le type de client de pare-feu sur Zone Labs

Procédure

	Commande ou action	Objectif
Étape 1	Pour définir le type de client pare-feu sur le type Zone Labs Integrity, saisissez la commande suivante : Exemple : <pre>hostname(config)# client-firewall req zonelabs-integrity</pre>	client-firewall {opt req} zonelabs-integrity

Prochaine étape

Pour obtenir plus de renseignements, consultez [Configurer les politiques de pare-feu des clients VPN](#), à la [page 173](#). Les arguments de commande qui précisent les stratégies de pare-feu ne sont pas utilisés lorsque le type de pare-feu est **zonelabs-integrity**, car le serveur Integrity détermine ces stratégies.

Définir les paramètres de pare-feu client

Saisissez les commandes suivantes pour définir les paramètres de pare-feu client appropriés. Vous ne pouvez configurer qu'une seule instance de chaque commande. Pour obtenir plus de renseignements, consultez [Configurer les politiques de pare-feu des clients VPN](#), à la [page 173](#).

- Cisco Integrated Firewall

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-integrated
acl-in ACL acl-out ACL
```

- Cisco Security Agent

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-security-agent
```

- Aucun pare-feu

```
hostname(config-group-policy)# client-firewall none
```

- Pare-feu personnalisé

```
hostname(config-group-policy)# client-firewall {opt | req} custom vendor-id num product-id
num policy {AYT | CPP acl-in ACL acl-out ACL} [description string]
```

- Pare-feu de Zone Labs

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-integrity
```

**Remarque**

Lorsque le type de pare-feu est **zonelabs-integrity**, n'incluez pas d'arguments. Le serveur d'intégrité de Zone Labs détermine les politiques.

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-zonealarm  
policy {AYT | CPP acl-in ACL acl-out ACL}
```

```
hostname(config-group-policy)# client-firewall {opt | req}  
zonelabs-zonealarmpro policy {AYT | CPP acl-in ACL acl-out ACL}
```

```
client-firewall {opt | req} zonelabs-zonealarmpro policy {AYT | CPP acl-in  
ACL acl-out ACL}
```

- Pare-feu personnels Sygate

```
hostname(config-group-policy)# client-firewall {opt | req} sygate-personal
```

```
hostname(config-group-policy)# client-firewall {opt | req} sygate-personal-pro
```

```
hostname(config-group-policy)# client-firewall {opt | req} sygate-security-agent
```

- Network Ice, Black Ice Firewall

```
hostname(config-group-policy)# client-firewall {opt | req} networkice-blackice
```

Tableau 8 : Mots-clés et variables de commande client-firewall

Paramètre	Description
acl-in ACL	Fournit la politique utilisée par le client pour le trafic entrant.
acl-out ACL	Fournit la politique utilisée par le client pour le trafic sortant.
AYT	Spécifie que l'application de pare-feu du PC client contrôle la politique de pare-feu. L'ASA vérifie que le pare-feu est en cours d'exécution. Il demande : « Êtes-vous là ? ». S'il n'y a pas de réponse, l'ASA met fin au tunnel.
cisco-integrated	Spécifie le type de pare-feu intégré Cisco.
cisco-security-agent	Spécifie le type de pare-feu Cisco Intrusion Prevention Security Agent.
CPP	Spécifie la politique poussée comme source de la politique de pare-feu du client VPN.
custom	Spécifie le type de pare-feu personnalisé.
description string	Décrit le pare-feu.
networkice-blackice	Spécifie le type de pare-feu Network ICE Black ICE.

none (aucun)	Indique qu'il n'y a pas de politique de pare-feu client. Définit une politique de pare-feu avec une valeur nulle, interdisant ainsi une politique de pare-feu. Empêche d'hériter d'une politique de pare-feu d'une politique par défaut ou d'une stratégie de groupe précisée.
opt	Indique un type de pare-feu facultatif.
product-id	Identifie le produit de pare-feu.
req	Indique un type de pare-feu requis.
sygate-personal	Spécifie le type de pare-feu Sygate Personal.
sygate-personal-pro	Spécifie le type de pare-feu Sygate Personal Pro.
sygate-security-agent	Spécifie le type de pare-feu Sygate Security Agent.
vendor-id	Identifie le fournisseur de pare-feu.
zonelabs-integrity	Spécifie le type de pare-feu du serveur d'intégrité de Zone Labs Integrity.
zonelabs-zonealarm	Spécifie le type de pare-feu Zone Labs Zone Alarm.
zonelabs-zonealarmpro policy	Spécifie le type de pare-feu Zone Labs Zone Alarm ou Pro.
zonelabs-zonealarmpro policy	Spécifie le type de pare-feu Zone Labs Zone Alarm Pro.

L'exemple suivant montre comment définir une politique de pare-feu client qui nécessite Cisco Intrusion Prevention Security Agent pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
hostname(config-group-policy)#
```

Configurer les règles d'accès client

Configurez des règles qui limitent les types et les versions de clients d'accès à distance pouvant se connecter par IPsec à travers l'ASA, à l'aide de la commande **client-access-rule** en mode de configuration group-policy. Élaborez les règles selon les lignes directrices suivantes :

- Si vous ne définissez aucune règle, l'ASA autorise tous les types de connexion.
- Lorsqu'un client ne correspond à aucune des règles, l'ASA refuse la connexion. Si vous définissez une règle de refus, vous devez également définir au moins une règle d'autorisation ; dans le cas contraire, l'ASA refuse toutes les connexions.
- Pour les clients logiciels comme matériels, le type et la version doivent correspondre exactement à ce qui apparaît dans l'affichage **show vpn-sessiondb remote**.
- Le caractère * est un caractère générique, que vous pouvez saisir plusieurs fois dans chaque règle. Par exemple, **client-access rule 3 deny type * version 3.*** crée une règle d'accès client de priorité 3 qui refuse tous les types de clients exécutant une version 3.x du logiciel.
- Vous pouvez élaborer un maximum de 25 règles par stratégie de groupe.

- Il y a une limite de 255 caractères pour un ensemble complet de règles.
- Vous pouvez saisir n/a pour les clients qui n'envoient ni type de client ni version.

Pour supprimer une règle, saisissez la forme **no** de cette commande. Cette commande équivaut à la commande suivante :

```
hostname(config-group-policy)# client-access-rule 1 deny type "Cisco VPN Client" version 4.0
```

Pour supprimer toutes les règles, saisissez **no client-access-rule command** sans arguments. Cela supprime toutes les règles configurées, y compris une règle nulle si vous en avez créé une en exécutant la commande **client-access-rule** avec le mot-clé **none**.

Par défaut, il n'y a aucune règle d'accès. En l'absence de règle d'accès client, les utilisateurs héritent de toutes les règles qui existent dans la stratégie de groupe par défaut.

Pour empêcher les utilisateurs d'hériter des règles d'accès client, entrez la commande **client-access-rule** avec le mot-clé **none**. Le résultat de cette commande est que tous les types et versions de clients peuvent se connecter.

```
hostname(config-group-policy)# client-access rule priority {permit | deny} type type version {version | none}
```

```
hostname(config-group-policy)# no client-access rule [priority {permit | deny} type type version version]
```

Le tableau ci-dessous explique la signification des mots-clés et des paramètres dans ces commandes.

Tableau 9 : Mots-clés et variables de commande client-access rules

Paramètre	Description
deny	Refuse les connexions pour les périphériques d'un type et/ou d'une version particuliers.
none	N'autorise aucune restriction d'accès client. Définit la règle d'accès client à une valeur nulle, de sorte qu'aucune restriction n'est appliquée. Empêche d'hériter d'une valeur provenant d'une stratégie de groupe par défaut ou précisée.
permit	Autorise les connexions pour des périphériques d'un type ou d'une version particuliers.
<i>priority</i>	Détermine la priorité de la règle. La règle dont l'entier est le plus faible a la priorité la plus élevée. Par conséquent, la règle dont l'entier est le plus faible et qui correspond à un type ou à une version de client est celle qui s'applique. Si une règle de priorité inférieure est contradictoire, l'ASA l'ignore.
type type	Identifie les types de périphériques au moyen de chaînes de forme libre. La chaîne doit correspondre exactement à ce qui apparaît dans l'affichage show vpn-sessiondb remote , sauf que vous pouvez saisir le caractère * comme caractère générique.

Paramètre	Description
version version	Identifie la version du périphérique au moyen de chaînes de forme libre, par exemple 7.0. Une chaîne doit correspondre exactement à ce qui apparaît dans l'affichage show vpn-sessiondb remote , sauf que vous pouvez saisir le caractère * comme caractère générique.

L'exemple suivant montre comment créer des règles d'accès client pour la stratégie de groupe nommée FirstGroup. Ces règles autorisent les clients VPN Cisco exécutant la version 4.x du logiciel, tout en refusant tous les clients Windows NT :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 deny type WinNT version *
hostname(config-group-policy)# client-access-rule 2 permit "Cisco VPN Client"
version 4.*
```



Remarque

Le champ « type » est une chaîne de forme libre qui accepte n'importe quelle valeur, mais cette valeur doit correspondre à la valeur fixe que le client envoie à l'ASA au moment de la connexion.

Configurer les attributs d'utilisateur

Cette section décrit les attributs d'utilisateur et comment les configurer.

Par défaut, les utilisateurs héritent de tous les attributs utilisateur de la stratégie de groupe attribuée. L'ASA vous permet également d'attribuer des attributs individuels au niveau de l'utilisateur, en remplaçant les valeurs de la stratégie de groupe qui s'applique à cet utilisateur. Par exemple, vous pouvez préciser une stratégie de groupe qui donne à tous les utilisateurs l'accès pendant les heures ouvrables, mais accorder à un utilisateur précis un accès 24 heures sur 24.

Afficher la configuration du nom d'utilisateur

Pour afficher la configuration pour tous les noms d'utilisateurs, y compris les valeurs par défaut héritées de la stratégie de groupe, saisissez le mot-clé **all** avec la commande **show running-config username**, comme suit :

```
hostname# show running-config all username
hostname#
```

Cette commande affiche le mot de passe chiffré et le niveau de privilège pour tous les utilisateurs ou, si vous fournissez un nom d'utilisateur, pour cet utilisateur précis. Si vous omettez le mot-clé **all** (tout), seules les valeurs explicitement configurées s'affichent dans cette liste. L'exemple suivant montre le résultat de cette commande pour l'utilisateur nommé testuser :

```
hostname# show running-config all username testuse
username testuser password 12RsxXQnphyr/I9Z encrypted privilege 15
```

Configurer les attributs pour les utilisateurs individuels

Pour configurer des utilisateurs spécifiques, vous attribuez un mot de passe (ou aucun mot de passe) et des attributs à un utilisateur à l'aide de la commande **username**, qui passe en mode nom d'utilisateur. Tous les attributs que vous ne spécifiez pas sont hérités de la stratégie de groupe.

La base de données d'authentification des utilisateurs internes est composée des utilisateurs saisis avec la commande **username**. La commande **login** utilise cette base de données pour l'authentification. Pour ajouter un utilisateur à la base de données ASA, saisissez la commande **username** en mode de configuration globale. Pour supprimer un utilisateur, utilisez la version **no** de cette commande avec le nom d'utilisateur que vous souhaitez supprimer. Pour supprimer tous les noms d'utilisateurs, utilisez la commande **clear configure username** sans ajouter de nom d'utilisateur.

Définir un mot de passe d'utilisateur et un niveau de privilège

Entrez la commande **username** pour attribuer un mot de passe et un niveau de privilège à un utilisateur. Vous pouvez saisir le mot-clé **nopassword** pour préciser que cet utilisateur ne nécessite pas de mot de passe. Si vous spécifiez un mot de passe, vous pouvez préciser si ce mot de passe est stocké sous une forme chiffrée.

Le mot-clé facultatif **privilege** vous permet de définir un niveau de privilège pour cet utilisateur. Les niveaux de privilège vont de 0 (le plus bas) à 15. Les administrateurs système ont généralement le niveau de privilège le plus élevé. La valeur par défaut est 2.

```
hostname(config)# username name {nopassword | password password [encrypted]}
[privilege priv_level]}
```

```
hostname(config)# no username [name]
```

Le tableau ci-dessous décrit la signification des mots-clés et des variables utilisés dans cette commande.

Mots-clés et variables de la commande username

Mot clé/variable	Signification
encrypted	Indique que le mot de passe est chiffré.
<i>Nom</i>	Nom de l'utilisateur.
nopassword	Indique que cet utilisateur n'a pas besoin de mot de passe.
password password	Indique que cet utilisateur possède un mot de passe et spécifie le mot de passe.
niveau de privilège	Définit le niveau de privilège pour cet utilisateur. La plage est comprise entre 0 et 15, les nombres inférieurs ayant moins de capacité à utiliser des commandes et à gérer l'ASA. Le niveau de privilège par défaut est 2. Le niveau de privilège typique d'un administrateur système est de 15.

Par défaut, les utilisateurs VPN que vous ajoutez avec cette commande n'ont aucun attribut ni association de stratégie de groupe. Vous devez configurer toutes les valeurs explicitement.

L'exemple suivant montre comment configurer un utilisateur nommé anyuser avec un mot de passe chiffré de pw_12345678 et un niveau de privilège 12 :

```
hostname(config)# username anyuser password pw_12345678 encrypted privilege
```

12

```
hostname(config)#
```

Configurer les attributs d'utilisateur

Après avoir configuré le mot de passe de l'utilisateur (le cas échéant) et le niveau de privilège de l'utilisateur, vous définissez les autres attributs. Celles-ci peuvent être dans n'importe quel ordre. Pour supprimer une paire attribut-valeur, saisissez la forme **no** de la commande.

Entrez en mode nom d'utilisateur en entrant la commande **username** avec le mot-clé **attributes** :

```
hostname(config)# username name attributes
hostname(config-username)#
```

L'invite change pour indiquer le nouveau mode. Vous pouvez maintenant configurer les attributs.

Configurer les attributs d'utilisateur VPN

Les attributs d'utilisateur VPN définissent des valeurs spécifiques aux connexions VPN, comme décrit dans les sections suivantes.

Configurer l'héritage

Vous pouvez permettre aux utilisateurs d'hériter de la stratégie de groupe des valeurs d'attributs que vous n'avez pas configurés au niveau du nom d'utilisateur. Pour préciser le nom de la stratégie de groupe dont cet utilisateur hérite les attributs, saisissez la commande **vpn-group-policy**. Par défaut, les utilisateurs VPN n'ont aucune association à une stratégie de groupe :

```
hostname(config-username)# vpn-group-policy group-policy-name
hostname(config-username)# no vpn-group-policy group-policy-name
```

Pour un attribut disponible en mode nom d'utilisateur, vous pouvez remplacer la valeur d'un attribut dans une stratégie de groupe pour un utilisateur particulier en le configurant en mode nom d'utilisateur.

L'exemple suivant montre comment configurer un utilisateur nommé anyuser pour utiliser les attributs de la stratégie de groupe nommée FirstGroup :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
hostname(config-username)#
```

Configurer les heures d'accès

Associez les heures pendant lesquelles cet utilisateur est autorisé à accéder au système en précisant le nom d'une politique de plage temporelle configurée :

Pour supprimer l'attribut de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cette option permet l'hérité d'une valeur de plage temporelle d'une autre stratégie de groupe. Pour éviter d'hériter d'une valeur, entrez la commande **vpn-access-hours none**. La valeur par défaut est un accès non restreint.

```
hostname(config-username)# vpn-access-hours value {time-range | none}
```

```
hostname(config-username)# vpn-access-hours value none
hostname(config)#
```

L'exemple suivant montre comment associer l'utilisateur nommé anyuser à une politique de plage temporelle appelée 824 :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-access-hours 824
hostname(config-username)#
```

Configurer le nombre maximal de connexions simultanées

Simultaneous Logins Per User (connexions simultanées par utilisateur) : précise le nombre maximal de connexions simultanées autorisées pour cet utilisateur. La plage est comprise entre 0 et 2147483647. La valeur par défaut est de 3 connexions simultanées. Pour supprimer l'attribut de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Saisissez 0 pour désactiver la connexion et empêcher l'accès de l'utilisateur.

```
hostname(config-username)# vpn-simultaneous-logins integer
hostname(config-username)# no vpn-simultaneous-logins
hostname(config-username)# vpn-session-timeout alert-interval none
```



Remarque

Bien que la limite maximale du nombre de connexions simultanées soit très élevée, en autoriser plusieurs peut compromettre la sécurité et affecter les performances.

L'exemple suivant montre comment autoriser un maximum de 4 connexions simultanées pour l'utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-simultaneous-logins 4
hostname(config-username)#
```

Configurer le délai d'inactivité

Procédure

Étape 1

(Facultatif) Pour configurer un délai d'inactivité du VPN, utilisez la commande **vpn-idle-timeout minutes** en mode de configuration de stratégie de groupe ou en mode de configuration de nom d'utilisateur.

S'il n'y a aucune activité de communication sur la connexion pendant cette période, l'ASA arrête la connexion. La durée minimale est de 1 minute, la durée maximale est de 35 791 394 minutes et la valeur par défaut est de 30 minutes.

L'exemple suivant montre comment définir un délai d'inactivité VPN de 15 minutes pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
```



```
hostname(config-group-policy)#
```

Autres actions utilisant la commande **[no] vpn-idle-timeout {minutes | none}** :

- Saisissez **vpn-idle-timeout none** pour désactiver le délai d'inactivité du VPN et empêcher l'héritage d'une valeur de délai d'expiration.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout none
hostname(config-group-policy)#
```

Il en résulte Secure Client (services client sécurisés) (SSL et IPsec/IKEv2) et un VPN sans client utilisant la valeur globale **default-idle-timeout secondes webvpn**. Cette commande est saisie en mode **webvpn-config**, par exemple : `hostname(config-webvpn)# default-idle-timeout 300`. La valeur par défaut est de 1800 secondes (30 min), la plage est comprise entre 60 et 86400 secondes.

Pour toutes les connexions **webvpn**, la valeur **default-idle-timeout** est appliquée uniquement si **vpn-idle-timeout none** est défini dans l'attribut de stratégie de groupe/de nom d'utilisateur. Une valeur de délai d'inactivité non nulle est requise par l'ASA pour toutes les connexions Secure Client (services client sécurisés).

Pour les VPN de site à site (IKEv1, IKEv2) et VPN d'accès à distance IKEv1, nous vous recommandons de désactiver le délai d'expiration et d'autoriser une période d'inactivité illimitée.

- Pour désactiver le délai d'inactivité pour cette stratégie de groupe ou cette politique d'utilisateur, saisissez **no vpn-idle-timeout**. La valeur sera héritée.
- Si vous ne définissez pas du tout **vpn-idle-timeout**, de toute façon, la valeur est héritée, qui est par défaut de 30 minutes.

Remarque

vpn-idle-timeout contrôle uniquement la durée maximale d'une session parente. Les sessions enfants (SSL/DTLS) sont terminées de manière dynamique beaucoup plus tôt par un délai d'inactivité TCP de 5 minutes codé en dur ou en cas d'échec de la vérification Dead Peer Detection (DPD) (3 tentatives). Pour plus de détails, consultez la note dans [Configurer la détection d'homologue mort](#). Pour plus de détails sur les attributs DPD, keepalive et de temporisation, consultez [Answer AnyConnect FAQ - Tunnels, DPD et minuterie d'inactivité](#).

Étape 2

(Facultatif) Vous pouvez éventuellement configurer l'heure à laquelle un message d'alerte de délai d'inactivité s'affiche à l'utilisateur à l'aide de la commande **vpn-idle-timeout alert-interval {minutes}** .

Ce message d'alerte indique aux utilisateurs le nombre de minutes qu'il leur reste jusqu'à ce que leur session VPN soit déconnectée pour cause d'inactivité. L'intervalle d'alerte par défaut est d'une minute.

L'exemple suivant montre comment définir un intervalle d'alerte de délai d'inactivité du VPN de 3 minutes pour l'utilisateur nommé **anyuser** :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout alert-interval 3
hostname(config-username)#
```

Autres actions utilisant la commande **[no] vpn-idle-timeout alert-interval {minutes | none}** :

- Le paramètre **none** indique que les utilisateurs ne recevront pas d'alerte.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout none
hostname(config-username)#
```

- Pour supprimer l'intervalle d'alerte de cette stratégie de groupe ou d'utilisateur, saisissez **no vpn-idle-timeout alert-interval**. La valeur sera héritée.
- Si vous ne définissez pas ce paramètre du tout, l'intervalle d'alerte par défaut est d'une minute.

Configurer la durée maximale de connexion

Procédure

Étape 1

(Facultatif) Configurez une durée maximale pour les connexions VPN en utilisant la commande **vpn-session-timeout** {minutes} dans le mode de configuration de stratégie de groupe ou dans le mode de configuration du nom d'utilisateur.

La durée minimale est de 1 minute et la durée maximale est de 35 791 394 minutes. Il n'y a pas de valeur par défaut. À la fin de cette période, l'ASA met fin à la connexion.

L'exemple suivant montre comment définir un délai d'expiration de session VPN de 180 minutes pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

L'exemple suivant montre comment définir un délai d'expiration de session VPN de 180 minutes pour l'utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-session-timeout 180
hostname(config-username)#
```

Autres actions utilisant la commande **[no] vpn-session-timeout** {minutes | none} :

- Pour supprimer l'attribut de cette stratégie et autoriser l'héritage, saisissez la forme **no vpn-session-timeout** de cette commande.
- Pour autoriser un délai d'expiration illimité et ainsi empêcher l'héritage d'une valeur de délai d'expiration, saisissez **vpn-session-timeout none**.

Étape 2

Configurez le moment où un message d'alerte d'expiration de session s'affiche à l'utilisateur au moyen de la commande **vpn-session-timeout alert-interval** {minutes} | } .

Ce message d'alerte indique aux utilisateurs le nombre de minutes restantes avant la déconnexion automatique de leur session VPN. L'exemple suivant montre comment spécifier que les utilisateurs seront informés 20 minutes avant la déconnexion de leur session VPN. Vous pouvez spécifier une plage de 1 à 30 minutes.

```
hostname(config-webvpn)# vpn-session-timeout alert-interval 20
```

Autres actions utilisant la commande **[no] vpn-session-timeout alert-interval** {minutes | none} :

- Utilisez la forme **no** de la commande pour indiquer que l'attribut d'intervalle d'alerte du délai d'expiration de la session VPN sera hérité de la stratégie de groupe par défaut :

```
hostname(config-webvpn)# no vpn-session-timeout alert-interval
```

- Le **vpn-session-timeout alert-interval none** indique que les utilisateurs ne recevront pas d'alerte.

Appliquer un filtre ACL

Précisez le nom d'une liste de contrôle d'accès spécifique à l'utilisateur configurée précédemment à utiliser comme filtre pour les connexions VPN. Pour ignorer une liste de contrôle d'accès et empêcher d'hériter d'une liste de contrôle d'accès de la stratégie de groupe, saisissez la commande **vpn-filter** avec le mot-clé **none**. Pour supprimer la liste de contrôle d'accès, y compris une valeur nulle créée en saisissant la commande **vpn-filter none**, utilisez la forme **no** de cette commande. L'option **no** permet l'héritage d'une valeur à partir de la stratégie de groupe. Il n'y a pas de comportement ou de valeur par défaut pour cette commande.

Vous configurez les listes de contrôle d'accès pour autoriser ou refuser différents types de trafic pour cet utilisateur. Notez que le filtre VPN s'applique aux connexions initiales uniquement. Il ne s'applique pas aux connexions secondaires, comme une connexion de support SIP, qui sont ouvertes en raison de l'action de l'inspection d'application. Vous utilisez ensuite la commande **vpn-filter** pour appliquer ces listes de contrôle d'accès.

```
hostname(config-username) # vpn-filter {value ACL_name | none}
hostname(config-username) # no vpn-filter
hostname(config-username) #
```



Remarque Le VPN SSL sans client n'utilise pas les listes de contrôle d'accès définies dans la commande **vpn-filter**.

L'exemple suivant montre comment définir un filtre qui invoque une liste de contrôle d'accès nommée **acl_vpn** pour l'utilisateur nommé **anyuser** :

```
hostname(config) # username anyuser attributes
hostname(config-username) # vpn-filter value acl_vpn
hostname(config-username) #
```

Préciser l'adresse IPv4 et le masque réseau

Précisez l'adresse IP et le masque réseau à affecter à un utilisateur particulier. Pour supprimer l'adresse IP, saisissez la forme **no** de cette commande.

```
hostname(config-username) # vpn-framed-ip-address {ip_address}
hostname(config-username) # no vpn-framed-ip-address
hostname(config-username) #
```

L'exemple suivant montre comment définir l'adresse IP 10.92.166.7 pour un utilisateur nommé **anyuser** :

```
hostname(config) # username anyuser attributes
hostname(config-username) # vpn-framed-ip-address 10.92.166.7
hostname(config-username) #
```

Précisez le masque réseau à utiliser avec l'adresse IP spécifiée à l'étape précédente. Si vous avez utilisé la commande **no vpn-framed-ip-address**, ne spécifiez pas de masque réseau. Pour supprimer le masque de sous-réseau, saisissez la forme **no** de cette commande. Aucun comportement ni valeur par défaut.

```
hostname(config-username)# vpn-framed-ip-netmask {netmask}
hostname(config-username)# no vpn-framed-ip-netmask
hostname(config-username)
```

L'exemple suivant montre comment définir un masque de sous-réseau de 255.255.255.254 pour un utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-netmask 255.255.255.254
hostname(config-username)
```

Préciser l'adresse IPv6 et le masque réseau

Précisez l'adresse IPv6 et le masque de sous-réseau à attribuer à un utilisateur particulier. Pour supprimer l'adresse IP, saisissez la forme **no** de cette commande.

```
hostname(config-username)# vpn-framed-ipv6-address {ip_address}
hostname(config-username)# no vpn-framed-ipv6-address
hostname(config-username)
```

L'exemple suivant montre comment définir l'adresse IP et le masque de sous-réseau 2001::3000:1000:2000:1/64 pour un utilisateur nommé anyuser. Cette adresse indique une valeur de préfixe de 2001:0000:0000:0000 et un ID d'interface 3000:1000:2000:1.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ipv6-address 2001::3000:1000:2000:1/64
hostname(config-username)
```

Préciser le protocole de tunnel

Précisez les types de tunnels VPN (IPsec ou VPN SSL sans client) que cet utilisateur peut utiliser. La valeur par défaut est extraite de la stratégie de groupe par défaut, dont la valeur par défaut est IPsec. Pour supprimer l'attribut de la configuration en cours d'exécution, saisissez la forme **no** de cette commande.

```
hostname(config-username)# vpn-tunnel-protocol {webvpn | IPsec}
hostname(config-username)# no vpn-tunnel-protocol [webvpn | IPsec]
hostname(config-username)
```

Les valeurs des paramètres pour cette commande sont les suivantes :

- **IPsec**—Négocie un tunnel IPsec entre deux homologues (un client d'accès à distance ou une autre passerelle sécurisée). Crée des associations de sécurité qui régissent l'authentification, le chiffrement, l'encapsulation et la gestion des clés.
- **webvpn**—Fournit un accès VPN SSL sans client aux utilisateurs distants par l'intermédiaire d'un navigateur Web compatible avec le protocole HTTPS et ne nécessite pas de client.

Entrez cette commande pour configurer un ou plusieurs modes de tunnelisation. Au moins un mode de tunnelisation doit être configuré pour que les utilisateurs puissent se connecter sur un tunnel VPN.

L'exemple suivant montre comment configurer les modes de tunnelisation VPN SSL et IPsec sans client pour l'utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-tunnel-protocol webvpn
hostname(config-username)# vpn-tunnel-protocol IPsec
hostname(config-username)
```

Restreindre l'accès des utilisateurs distants

Configurez cet attribut **group-lock** avec le mot-clé **value** afin de restreindre les utilisateurs distants à un accès uniquement par le profil de connexion préexistant spécifié. Le verrouillage de groupe restreint les utilisateurs en vérifiant si le groupe configuré dans le client VPN est le même que le profil de connexion auquel l'utilisateur est affecté. Si ce n'est pas le cas, l'ASA empêche l'utilisateur de se connecter. Si vous ne configurez pas **group-lock**, l'ASA authentifie les utilisateurs sans tenir compte du groupe attribué.

Pour supprimer l'attribut **group-lock** de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cette option permet l'héritage d'une valeur à partir de la stratégie de groupe. Pour désactiver le verrouillage de groupe et pour éviter d'hériter d'une valeur de verrouillage de groupe d'une stratégie de groupe par défaut ou d'une stratégie de groupe spécifiée, saisissez la commande **group-lock** avec le mot-clé **none**.

```
hostname(config-username)# group-lock {value tunnel-grp-name | none}
hostname(config-username)# no group-lock
hostname(config-username)
```

L'exemple suivant montre comment définir le verrouillage de groupe pour l'utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# group-lock value tunnel-group-name
hostname(config-username)
```

Activer le stockage des mots de passe pour les utilisateurs de clients logiciels

Précisez s'il faut autoriser les utilisateurs à stocker leurs mots de passe de connexion sur le système client. Le stockage de mot de passe est désactivé par défaut. Activez le stockage des mots de passe uniquement sur les systèmes que vous savez se trouver dans des sites sécurisés. Pour désactiver le stockage de mot de passe, entrez la commande **password-storage** avec le mot-clé **disable**. Pour supprimer l'attribut de stockage de mot de passe de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cela permet l'héritage d'une valeur pour le stockage de mots de passe de la stratégie de groupe.

```
hostname(config-username)# password-storage {enable | disable}
hostname(config-username)# no password-storage
hostname(config-username)
```

Cette commande n'a aucune incidence sur l'authentification client matériel interactive ou l'authentification d'utilisateur individuel pour les clients de matériel.

L'exemple suivant montre comment activer le stockage de mot de passe pour l'utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# password-storage enable
```

```
hostname (config-username)
```

Bonnes pratiques pour la configuration et l'ajustement de l'ACL du filtre de VPN

Cette section présente les bonnes pratiques à suivre lors de la mise à jour d'une liste de contrôle d'accès de filtre de VPN existante sans interrompre le trafic.

Mise à jour d'une liste de contrôle d'accès de filtre VPN existante

Suivez ces étapes lorsque vous souhaitez mettre à jour une liste de contrôle d'accès de filtre vpn appliquée sur l' périphérique ASA :

1. Créez une nouvelle liste de contrôle d'accès vpn-filter sur votre système (exemple : *new_acl.txt*).
2. Téléchargez l'ACL vpn-filter actuelle à partir du périphérique (exemple : *old_acl.txt*).
3. Créez des instructions de modification pour l'ACL :

```
* Add update in-progress to ACL remark
echo ?access-list <name> line 1 ACL update in-progress? > push.txt
* Delete old rules
sed ?s/^/no /g? old_acl >> push.txt
* Add new rules
cat new_acl >> push.txt
* Remove update in-progress to ACL remark
echo ?no access-list <name> ACL update in-progress? >> push.txt
```

4. Chargez le fichier push.txt sur l' périphérique.

Remplacement d'une liste de contrôle d'accès de filtre VPN existante par une nouvelle

Suivez les étapes suivantes pour remplacer la liste de contrôle d'accès vpn-filter appliquée sur l' périphérique ASA :

1. Créez une nouvelle liste de contrôle d'accès vpn-filter chaque fois que vous souhaitez en remplacer une existante.
2. Mettez à jour la stratégie de groupe avec l'ACL vpn-filter.
3. Supprimez l'ancienne liste de contrôle d'accès vpn-filter appliquée sur le périphérique.



CHAPITRE 6

Adresses IP pour les VPN

- Configurer une politique d'attribution d'adresses IP, à la page 191
- Configurer les ensembles d'adresses IP locales, à la page 193
- Configurer l'adressage AAA, à la page 195
- Configurer l'adressage DHCP, à la page 196

Configurer une politique d'attribution d'adresses IP

L'ASA peut utiliser une ou plusieurs des méthodes suivantes pour attribuer des adresses IP aux clients d'accès à distance. Si vous configurez plusieurs méthodes d'affectation d'adresses, l'ASA parcourt chacune des options jusqu'à ce qu'il trouve une adresse IP. Par défaut, toutes les méthodes sont activées.

- **aaa** (Utiliser le serveur d'authentification) récupère les adresses à partir d'un serveur externe d'authentification, d'autorisation et de comptabilisation, sur une base par utilisateur. Si vous utilisez un serveur d'authentification sur lequel des adresses IP sont configurées, nous vous recommandons d'utiliser cette méthode. Cette méthode est disponible pour les politiques d'attribution IPv4 et IPv6.
- **dhcp** (Utiliser DHCP) obtient les adresses IP à partir d'un serveur DHCP. Si vous souhaitez utiliser DHCP, vous devez configurer un serveur DHCP. Vous devez également définir la plage d'adresses IP que le serveur DHCP peut utiliser. Cette méthode est disponible pour les politiques d'attribution IPv4.
- **local** les ensembles d'adresses configurés en interne constituent la méthode d'affectation la plus simple à configurer. Si vous choisissez local, vous devez également utiliser la **ip-local-pool** commande pour définir la plage d'adresses IP à utiliser. Cette méthode est disponible pour les politiques d'attribution IPv4 et IPv6.
 - Allow the reuse of an IP address so many minutes after it is released (Autoriser la réutilisation d'une adresse IP un certain nombre de minutes après sa libération) : retarde la réutilisation d'une adresse IP après son retour dans l'ensemble d'adresses. L'ajout d'un délai permet d'éviter les problèmes que les pare-feu peuvent rencontrer lorsqu'une adresse IP est réaffectée rapidement. Par défaut l'ASA n'applique pas de délai. Cet élément configurable est disponible pour les politiques d'attribution IPv4.

Utilisez l'une des méthodes suivantes pour préciser un moyen d'affecter les adresses IP aux clients d'accès à distance.

Configurer les adresses IPv4

Procédure

Activez une méthode d'affectation d'adresse que l'ASA utilise lors de l'affectation d'une adresse IPv4 aux connexions VPN. Les méthodes disponibles pour obtenir une adresse IP sont celles d'un serveur AAA, d'un serveur DHCP ou d'un ensemble d'adresses locales. Ceux-ci sont activés par défaut.

vpn-addr-assign {aaa | dhcp | local [reuse-delay minutes]}

Exemple :

Par exemple, vous pouvez configurer la réutilisation d'une adresse IP entre 0 et 480 minutes après la libération de l'adresse IP.

```
hostname(config)#vpn-addr-assign aaa
hostname(config)#vpn-addr-assign local reuse-delay 180
```

Cet exemple utilise la forme no de la commande pour désactiver une méthode d'affectation d'adresse.

```
hostname(config)# no vpn-addr-assign dhcp
```

Configurer l'attribution des adresses IPv6

Procédure

Activez une méthode d'attribution d'adresse que l'ASA utilise lors de l'affectation d'une adresse IPv6 aux connexions VPN. Les méthodes disponibles pour obtenir une adresse IP proviennent d'un serveur AAA ou d'un ensemble d'adresses locales. Ces deux méthodes sont activées par défaut.

ipv6-vpn-addr-assign {aaa | local}

Exemple :

```
hostname(config)# ipv6-vpn-addr-assign aaa
```

Cet exemple utilise la forme no de la commande pour désactiver une méthode d'affectation d'adresse.

```
hostname(config)# no ipv6-vpn-addr-assign local
```

Afficher les méthodes d'attribution d'adresses

Procédure

Utilisez l'une de ces méthodes pour afficher la méthode d'affectation d'adresse configurée sur l'ASA :

- Afficher les affectations d'adresses IPv4

Afficher la méthode d'affectation d'adresse configurée. La méthode d'adresse configurée peut être AAA, DHCP ou locale.

```
show running-config all vpn-addr-assign
vpn-addr-assign aaa
vpn-addr-assign dhcp
vpn-addr-assign local
```

- Afficher les affectations d'adresses IPv6

Afficher la méthode d'affectation d'adresse configurée. Les méthodes d'adresse configurées peuvent être AAA ou locales.

```
show running-config all ipv6-vpn-addr-assign
ipv6-vpn-addr-assign aaa
ipv6-vpn-addr-assign local reuse-delay 0
```

Configurer les ensembles d'adresses IP locales

Pour configurer les ensembles d'adresses IPv4 à utiliser pour les tunnels VPN d'accès à distance, saisissez la commande **ip local pool** en mode de configuration globale. Pour supprimer des ensembles d'adresses, saisissez la forme **no** de cette commande.

Pour configurer les ensembles d'adresses IPv6 à utiliser pour les tunnels VPN d'accès à distance, saisissez la commande **ipv6 local pool** en mode de configuration globale. Pour supprimer des ensembles d'adresses, saisissez la forme **no** de cette commande.

L'ASA utilise les ensembles d'adresses en fonction du profil de connexion ou de la stratégie de groupe associés à la connexion. L'ordre dans lequel vous spécifiez les ensembles est important. Si vous configurez plusieurs ensembles d'adresses pour un profil de connexion ou une politique de groupe, l'ASA les utilise dans l'ordre dans lequel vous les avez ajoutées à l'ASA.

Si vous affectez des adresses à partir d'un sous-réseau non local, nous vous suggérons d'ajouter des pools qui se situent dans les limites de sous-réseau pour faciliter l'ajout de routes pour ces réseaux.

**Remarque**

Lorsque vous modifiez des ensembles d'adresses existants actuellement utilisés dans un groupe de tunnels actif (c'est-à-dire ouvert aux utilisateurs finaux pour les connexions), vous devez effectuer la modification dans une fenêtre de maintenance et vous assurer de ce qui suit :

- Les utilisateurs connectés sont déconnectés.
- Les ensembles d'adresses sont supprimés du groupe de tunnels et modifiés au besoin.
- Les ensembles d'adresses modifiés sont ensuite rajoutés dans le groupe de tunnels.

Si un ensemble d'adresses n'est pas modifié de cette manière, il peut entraîner des incohérences dans le comportement de l'ASA.

Configurer les ensembles d'adresses IPv4 locales

**Remarque**

Lorsque vous souhaitez modifier dans l'interface de ligne de commande un ensemble d'adresses existant actuellement utilisé dans un groupe de tunnels actif (c'est-à-dire ouvert aux utilisateurs finaux pour les connexions), il est recommandé d'effectuer cette modification pendant une fenêtre de changement. Les utilisateurs connectés doivent être déconnectés, l'ensemble d'adresses doit être supprimé du groupe de tunnels, modifié au besoin, puis ajouté de nouveau au groupe de tunnels. Si cela n'est pas fait de cette manière, des incohérences peuvent se produire dans le comportement de l'ASA.

Procédure

Étape 1

Configurez les ensembles d'adresses IP comme méthode d'attribution d'adresses. Saisissez la commande **vpn-addr-assign** avec l'argument **local**.

Exemple :

```
hostname(config)# vpn-addr-assign local
```

Étape 2

Configurez un ensemble d'adresses. La commande nomme l'ensemble, précise une plage d'adresses IPv4 et le masque de sous-réseau.

```
ip local pool poolname first_address-last_address mask mask
```

Exemple :

Cet exemple configure un ensemble d'adresses IP nommé *firstpool*. L'adresse de début est 10.20.30.40 et l'adresse de fin est 10.20.30.50. Le masque de sous-réseau est 255.255.255.0.

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

Cet exemple supprime l'ensemble d'adresses IP nommé **firstpool**.

```
hostname(config)# no ip local pool firstpool
```

Configurer les ensembles d'adresses IPv6 locaux

Procédure

Étape 1 Pour configurer les ensembles d'adresses IP comme méthode d'affectation, saisissez la commande **ipv6-vpn-addr-assign** avec l'argument **local**.

Exemple :

```
hostname(config)# ipv6-vpn-addr-assign local
```

Étape 2 Configurez l'ensemble d'adresses. La commande nomme l'ensemble, identifie l'adresse IPv6 de départ, la longueur du préfixe en bits et le nombre d'adresses à utiliser dans la plage.

ipv6 local pool *pool_name starting_address prefix_length number_of_addresses*

Exemple :

Cet exemple configure un ensemble d'adresses IP nommé *ipv6pool*. L'adresse de départ est 2001:DB8::1, la longueur du préfixe est de 32 bits et le nombre d'adresses à utiliser dans l'ensemble est de 100.

```
hostname(config)# ipv6 local pool ipv6pool 2001:DB8::1/32 100
```

Cet exemple supprime l'ensemble d'adresses IP nommé *ipv6ensemble*.

```
hostname(config)# no ipv6 local pool ipv6pool
```

Configurer l'adressage AAA

Pour utiliser un serveur AAA afin d'attribuer des adresses aux clients d'accès à distance VPN, vous devez d'abord configurer un serveur ou un groupe de serveurs AAA. Consultez la commande **aaa-server protocol** dans la référence de commande.

En outre, l'utilisateur doit correspondre à un profil de connexion configuré pour l'authentification RADIUS.

Les exemples suivants illustrent comment définir un groupe de serveurs AAA appelé RAD2 pour le groupe de tunnels nommé FirstGroup. Il comprend une étape de plus que nécessaire, en ce que vous avez peut-être nommé le groupe de tunnels et défini le type de groupe de tunnels. Cette étape s'affiche dans l'exemple suivant pour vous rappeler que vous n'avez pas accès aux commandes de groupe de tunnels suivantes tant que vous n'avez pas défini ces valeurs.

Voici un aperçu de la configuration créée par ces exemples :

```
hostname(config)# vpn-addr-assign aaa
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config)# authentication-server-group RAD2
```

Pour configurer AAA pour l'adressage IP, procédez comme suit :

Procédure

- Étape 1** Pour configurer AAA comme méthode d'affectation d'adresses, entrez la commande **vpn-addr-assign** avec l'argument **aaa** :

```
hostname(config)# vpn-addr-assign aaa
hostname(config)#
```

- Étape 2** Pour établir le groupe de tunnels appelé FirstGroup en tant que groupe de tunnels d'accès à distance ou LAN à LAN, saisissez la commande **tunnel-group** avec le mot-clé **type**. L'exemple suivant configure un groupe de tunnels d'accès à distance.

```
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)#
```

- Étape 3** Pour passer en mode de configuration d'attributs généraux, qui vous permet de définir un groupe de serveurs AAA pour le groupe de tunnels appelé FirstGroup, saisissez la commande **tunnel-group** avec l'argument **general-attributes**.

```
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)#
```

- Étape 4** Pour préciser le groupe de serveurs AAA à utiliser pour l'authentification, saisissez la commande **authentication-server-group**.

```
hostname(config-general)# authentication-server-group RAD2
hostname(config-general)#
```

Prochaine étape

Cette commande comporte plus d'arguments que cet exemple inclut. Consultez la référence de commande pour en savoir plus.

Configurer l'adressage DHCP

Pour utiliser le DHCP afin d'attribuer des adresses aux clients VPN, vous devez d'abord configurer un serveur DHCP et la plage d'adresses IP que le serveur DHCP peut utiliser. Vous définissez ensuite le serveur DHCP par profil de connexion. Vous pouvez également définir une portée réseau DHCP dans la stratégie de groupe associée à un profil de connexion ou à un nom d'utilisateur.

L'exemple suivant définit le serveur DHCP à l'adresse 172.33.44.19 pour le profil de connexion nommé **firstgroup**. L'exemple définit également une portée réseau DHCP de 10.100.10.1 pour la stratégie de groupe nommée **remotegroup**. (La stratégie de groupe nommée remotegroup est associée au profil de connexion nommé firstgroup.) Si vous ne définissez pas de portée réseau, le serveur DHCP attribue les adresses IP dans l'ordre des ensembles d'adresses configurés. Il parcourt les ensembles jusqu'à ce qu'il identifie une adresse non attribuée.

Avant de commencer

Vous ne pouvez utiliser une adresse IPv4 que pour identifier un serveur DHCP afin d'attribuer des adresses client. De plus, les options DHCP ne sont pas transférées aux utilisateurs ; ils reçoivent uniquement une attribution d'adresse.

Procédure

- Étape 1** Configurez les ensembles d'adresses IP comme méthode d'attribution d'adresses.
- vpn-addr-assign dhcp**
- Étape 2** Définissez le profil de connexion appelé **firstgroup** comme profil de connexion d'accès à distance.
- tunnel-group firstgroup type remote-access**
- Étape 3** Entrez en mode de configuration general-attributes pour le profil de connexion afin de pouvoir configurer un serveur DHCP.
- tunnel-group firstgroup general-attributes**
- Étape 4** Définissez le serveur DHCP au moyen de son adresse IPv4, puis quittez le mode de configuration tunnel-group.
- dhcp-server IPv4_address_of_DHCP_server**
- Vous ne pouvez pas définir un serveur DHCP au moyen d'une adresse IPv6. Vous pouvez préciser plusieurs adresses de serveur DHCP pour un profil de connexion. Entrez la commande dhcp-server. Cette commande vous permet de configurer l'ASA pour envoyer des options supplémentaires aux serveurs DHCP précisés lorsqu'il tente d'obtenir des adresses IP pour les clients VPN.
- Exemple :**
- L'exemple configure un serveur DHCP à l'adresse IP 172.33.44.19. Ensuite, quittez le mode de configuration tunnel-group.
- ```
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)# exit
hostname(config)#
```
- Étape 5** Si le groupe n'existe pas déjà, créez une stratégie de groupe interne appelée **remotegroup**.
- hostname(config)# group-policy remotegroup internal**
- Étape 6** (Facultatif) Entrez en mode de configuration des attributs group-policy et définissez la portée réseau DHCP.
- dhcp-network-scope ip\_address**
- Si vous configurez des serveurs DHCP pour l'ensemble d'adresses dans le profil de connexion, la portée de DHCP identifie les sous-réseaux à utiliser pour le regroupement pour ce groupe. Le serveur DHCP doit également avoir des adresses dans le même sous-réseau identifié par la portée. La portée vous permet de sélectionner un sous-ensemble des ensembles d'adresses définis dans le serveur DHCP à utiliser pour ce groupe précis.
- Si vous ne définissez pas de portée réseau, le serveur DHCP attribue les adresses IP dans l'ordre des ensembles d'adresses configurés. Il parcourt les ensembles jusqu'à ce qu'il identifie une adresse non attribuée.

### Remarque

Pour préciser une portée, entrez une adresse routable sur le même sous-réseau que l'ensemble d'adresses souhaité, mais à l'extérieur de cet ensemble. Le serveur DHCP détermine à quel sous-réseau cette adresse IP appartient et attribue une adresse IP de cet ensemble d'adresses.

Nous vous recommandons d'utiliser l'adresse IP d'une interface chaque fois que cela est possible à des fins de routage. Par exemple, si l'ensemble d'adresses est 10.100.10.2-10.100.10.254 et que l'adresse d'interface est 10.100.10.1/24, utilisez 10.100.10.1 comme portée DHCP. N'utilisez pas le numéro de réseau. Vous ne pouvez utiliser DHCP que pour l'adressage IPv4. Si l'adresse que vous choisissez n'est pas une adresse d'interface, vous devrez peut-être créer une voie de routage statique pour l'adresse de portée.

### Exemple :

L'exemple suivant passe en mode de configuration des attributs pour remotegroup et définit la portée DHCP à 10.100.10.1.

```
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.100.10.1
```

---

### Exemple

Voici un résumé de la configuration créée par ces exemples :

```
hostname(config)# vpn-addr-assign dhcp
hostname(config)# tunnel-group firstgroup type remote-access
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)# exit
hostname(config)# group-policy remotegroup internal
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.100.10.1
```



## CHAPITRE 7

# VPN IPsec d'accès à distance

- Présentation des VPN d'accès à distance IPsec, à la page 199
- Exigences de licence pour le module AnyConnect VPN de Cisco Secure Client, à la page 201
- Restrictions pour le VPN IPsec d'accès à distance, à la page 201
- Configurer les VPN d'accès à distance IPsec, à la page 202
- Authentification VPN à l'aide de clés prépartagées post-quantiques, à la page 209
- Exemples de configuration pour les VPN d'accès à distance IPsec, à la page 214
- Exemples de configuration pour le VPN d'accès à distance IPsec IKEv2 basé sur les normes en mode multi-contexte, à la page 215
- Exemples de configuration pour le VPN d'accès à distance Secure Client (services client sécurisés) IPsec IKEv2 en mode multicontexte, à la page 216
- Historique des VPN d'accès à distance, à la page 217

## Présentation des VPN d'accès à distance IPsec

Les VPN d'accès à distance permettent aux utilisateurs de se connecter à un site central par le biais d'une connexion sécurisée sur un réseau TCP/IP. Le protocole Internet Security Association and Key Management, également appelé IKE, est le protocole de négociation qui permet au client IPsec sur le PC distant et l'ASA de convenir de la manière de créer une association de sécurité IPsec. Chaque négociation ISAKMP est divisée en deux sections appelées Phase 1 et Phase 2.

La Phase 1 crée le premier tunnel pour protéger les messages de négociation ISAKMP ultérieurs. La Phase 2 crée le tunnel qui protège les données circulant sur la connexion sécurisée.

Pour définir les termes des négociations ISAKMP, vous créez une politique ISAKMP. Elle comprend les éléments suivants :

- Une méthode d'authentification pour garantir l'identité des homologues.
- Une méthode de chiffrement pour protéger les données et garantir la confidentialité.
- Une méthode HMAC (hachage de codes d'authentification de message) pour s'assurer de l'identité de l'expéditeur et pour s'assurer que le message n'a pas été modifié pendant le transfert.
- Un groupe Diffie-Hellman pour définir la taille de la clé de chiffrement.
- Une limite de temps pendant laquelle l'ASA utilise une clé de chiffrement avant de la remplacer.

Un ensemble de transformation combine une méthode de chiffrement et une méthode d'authentification. Lors de la négociation de l'association de sécurité IPsec avec ISAKMP, les pairs conviennent d'utiliser un ensemble de transformation particulier pour protéger un flux de données particulier. L'ensemble de transformation doit être le même pour les deux homologues.

Un ensemble de transformation protège les flux de données pour l'ACL spécifiée dans l'entrée de carte de chiffrement associée. Vous pouvez créer des ensembles de transformation dans la configuration ASA, puis spécifier un maximum de 11 d'entre eux dans une carte de chiffrement ou une entrée de carte de chiffrement dynamique. Pour obtenir plus de renseignements, y compris un tableau qui répertorie les méthodes de chiffrement et d'authentification valides, consultez [Créer un ensemble de transformation IKEv1 ou une proposition IKEv2](#), à la page 204.

Vous pouvez configurer l'ASA pour attribuer une adresse IPv4, une adresse IPv6 ou à la fois une adresse IPv4 et une adresse IPv6 à Secure Client (services client sécurisés) en créant des regroupements internes d'adresses sur l'ASA ou en attribuant une adresse dédiée à un utilisateur local sur l'ASA.

Le point terminal doit être doté du protocole à double pile dans son système d'exploitation pour attribuer les deux types d'adresses. Dans les deux scénarios, lorsqu'il n'y a plus d'ensembles d'adresses IPv6 mais que les adresses IPv4 sont disponibles ou lorsqu'il n'y a plus d'ensembles d'adresses IPv4 mais que les adresses IPv6 sont disponibles, la connexion se produit toujours. Le client n'est pas informé ; cependant, l'administrateur doit consulter les journaux ASA pour obtenir les détails.

L'attribution d'une adresse IPv6 au client est prise en charge pour le protocole SSL.

## À propos des VPN Mobike et d'accès à distance

Mobile IKEv2 (mobike) étend les VPN d'accès à distance ASA pour prendre en charge l'itinérance des périphériques portables. Cette prise en charge signifie que l'adresse IP de point terminal de l'association de sécurité IKE/IPSEC d'un périphérique portable peut être mise à jour plutôt que d'être supprimée lorsque le périphérique passe de son point de connexion actuel à un autre.

Mobike est disponible par défaut sur les ASAs depuis la version 9.8(1), ce qui signifie que Mobike est « toujours activé ». Mobike est activé pour chaque SA uniquement lorsque le client le propose et que l'ASA l'accepte. Cette négociation se produit dans le cadre de l'échange IKE\_AUTH.

Une fois la SA établie avec la prise en charge de mobike activée, le client peut modifier son adresse à tout moment et notifier l'ASA à l'aide de l'échange INFORMATIONAL avec la charge utile UPDATE\_SA\_ADDRESS indiquant la nouvelle adresse. L'ASA traitera ce message et mettra à jour la SA avec la nouvelle adresse IP du client.



### Remarque

Vous pouvez utiliser la commande `show crypto ikev2 sa detail` pour déterminer si mobike est activé pour tous les SA actuels.

L'implémentation actuelle de Mobike prend en charge les éléments suivants :

- Adresses IPv4 :
- Modifications des mappages NAT
- Connectivité du chemin et détection des pannes au moyen de la vérification facultative de la route de retour
- Basculement actif/de secours



- Équilibrage de la charge VPN

Si la fonction de vérification de retour de routage (RRC) est activée, un message RRC est envoyé au client mobile pour confirmer la nouvelle adresse IP avant la mise à jour de la SA.

## Exigences de licence pour le module AnyConnect VPN de Cisco Secure Client



### Remarque

Cette fonctionnalité n'est pas disponible dans les modèles sans chiffrement de charge utile.

Si vous souhaitez déployer Cisco Secure Client (y compris AnyConnect) à partir d'une tête de réseau Secure Firewall ASA et utiliser les modules VPN et Secure Firewall Posture ou HostScan, une licence Advantage ou Premier est requise. Des licences d'essai sont disponibles. Consultez le [guide de commande Cisco Secure Client](#). Consultez [les licences pour fonctionnalités de la gamme Cisco ASA](#) pour connaître les valeurs maximales par modèle.

## Restrictions pour le VPN IPsec d'accès à distance

- Directives relatives au mode pare-feu : prises en charge uniquement en mode de pare-feu routé. Le mode transparent n'est pas pris en charge.
- Directives de basculement : les sessions VPN IPsec sont répliquées uniquement dans les configurations de basculement actif/veille. Les configurations de basculement actif/actif ne sont pas prises en charge.
- Les modifications de configuration sont bloquées pendant la synchronisation à haute disponibilité. Si un utilisateur tente de se connecter pendant ce temps, l'installation de la règle DACL dans le pare-feu peut échouer. Une fois la synchronisation HA terminée, l'utilisateur peut se connecter avec succès.
- L'ASA n'accepte pas les sessions VPN d'accès à distance si le client tiers envoie un agent utilisateur nul.
- L'utilisation de listes de contrôle d'accès (ACL) de nom de domaine complet (FQDN) pour un domaine qui se résout en plusieurs adresses IP qui changent fréquemment peut avoir une incidence sur la résolution des adresses DHCP dans un environnement VPN d'accès à distance. Ce problème peut se produire si un serveur DHCP externe est configuré et qu'une validation transactionnelle pour la traduction d'adresses réseau (NAT) est activée.
- L'évaluation de la posture à l'aide d'Advanced Endpoint Assessment peut entraîner des messages syslog de connexion SSL qui ne sont pas associés à un événement de connexion ou de déconnexion VPN.
- L'authentification locale n'est pas possible, car l'ASA ne termine aucune méthode EAP.

L'ASA prend en charge EAP uniquement en relais et exige l'authentification par certificat pour les clients VPN dans le cadre de l'authentification EAP des clients. Lorsque vous configurez le protocole EAP comme méthode d'authentification à distance, veillez à configurer l'authentification par certificat pour les clients VPN. Des erreurs s'affichent même si plusieurs méthodes d'authentification à distance, telles que EAP, PSK ou des certificats, sont configurées avec EAP.

# Configurer les VPN d'accès à distance IPsec

Cette section décrit comment configurer les VPN d'accès à distance.

## Configurer une interface

Un ASA comporte au moins deux interfaces, appelées ici outside et inside. En règle générale, l'interface externe est connectée à l'Internet public, tandis que l'interface interne est connectée à un réseau privé et est protégée contre tout accès public.

Pour commencer, configurez et activez deux interfaces sur l'ASA. Attribuez ensuite un nom, une adresse IP et un masque de sous-réseau. Vous pouvez également configurer son niveau de sécurité, sa vitesse et son fonctionnement en duplex sur l'appareil de sécurité.

### Procédure

---

**Étape 1** Entrez le mode de configuration d'interface à partir du mode de configuration globale :

**interface** {*interface*}

**Exemple :**

```
hostname(config)# interface ethernet0
hostname(config-if)#
```

**Étape 2** Définissez l'adresse IP et le masque de sous-réseau pour l'interface :

**ip address** *ip\_address* [*mask*] [*standby ip\_address*]

**Exemple :**

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
```

**Étape 3** Spécifiez un nom pour l'interface (maximum 48 caractères). Vous ne pourrez pas modifier ce nom ultérieurement.

**nameif** *nom*

**Exemple :**

```
hostname(config-if)# nameif outside
hostname(config-if)#
```

**Étape 4** Activez l'interface. Par défaut, les interfaces sont désactivées.

**Exemple :**

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

---

# Configurer la politique ISAKMP et activer ISAKMP sur l'interface externe

## Procédure

- Étape 1** Précisez la méthode d'authentification et l'ensemble de paramètres à utiliser lors de la négociation IKEv1. La priorité identifie de manière unique la politique Internet Key Exchange (IKE) et lui attribue une priorité. Utilisez un entier de 1 à 65 534, 1 étant la priorité la plus élevée et 65 534 la priorité la plus basse. Dans les étapes qui suivent, nous définissons la priorité à 1.
- Étape 2** Précisez la méthode de chiffrement à utiliser dans une politique IKE :
- ```
crypto ikev1 policy priority encryption {aes-192 | aes-256 | | }
```
- Exemple :**
- Étape 3** Précisez l'algorithme de hachage d'une politique IKE (également appelé variante HMAC) :
- ```
crypto ikev1 policy priority hash { | sha }
```
- Exemple :**
- ```
hostname(config)# crypto ikev1 policy 1 hash sha
hostname(config)#
```
- Étape 4** Précisez le groupe Diffie-Hellman pour la politique IKE, le protocole cryptographique qui permet au client IPsec et à l'ASA d'établir une clé secrète partagée :
- ```
crypto ikev1 policy priority group {14 | | 19 | 20 | 21 }
```
- Exemple :**
- ```
hostname(config)#crypto ikev1 policy 1 group 14
hostname(config)#
```
- Étape 5** Précisez la durée de vie de la clé de chiffrement : le nombre de secondes que chaque association de sécurité doit exister avant d'expirer :
- ```
crypto ikev1 policy priority lifetime {seconds}
```
- La plage est comprise entre 120 et 2 147 483 647 secondes. Utilisez 0 seconde pour une durée de vie infinie.
- Exemple :**
- ```
hostname(config)# crypto ikev1 policy 1 lifetime 43200
hostname(config)#
```
- Étape 6** Activez ISAKMP sur l'interface nommée à l'extérieur :
- ```
crypto ikev1 enable interface-name
```
- Exemple :**
- ```
hostname(config)# crypto ikev1 enable outside
hostname(config)#
```
- Étape 7** Enregistrez les modifications de configuration :

write memory

Configurer un ensemble d'adresses

L'ASA nécessite une méthode pour attribuer des adresses IP aux utilisateurs. Cette section utilise les ensembles d'adresses comme exemple.

Procédure

Créez un ensemble d'adresses avec une plage d'adresses IP, à partir de laquelle l'ASA att

ip local pool *poolname first-address—last-address [mask mask]*

Le masque d'adresse est facultatif. Cependant, vous devez fournir la valeur de masque lorsque les adresses IP attribuées aux clients VPN appartiennent à un réseau non standard et que les données peuvent être acheminées incorrectement si vous utilisez le masque par défaut. Un exemple typique est lorsque l'ensemble local d'adresses IP contient 10.10.10.0/255.255.255.0, car il s'agit d'un réseau de classe A par défaut. Cela peut entraîner des problèmes de routage lorsque le client VPN doit accéder à différents sous-réseaux du réseau 10 sur différentes interfaces.

Exemple :

```
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)#
```

Ajouter un utilisateur

Procédure

Créez un utilisateur, un mot de passe et un niveau de privilège pour l'utilisateur :

username *name {nopassword | password password [mschap | encrypted | nt-encrypted]}* [*privilege priv_level*]

Exemple :

```
Hostname(config)# username testuser password 12345678
```

Créer un ensemble de transformation IKEv1 ou une proposition IKEv2

Cette section montre comment configurer un ensemble de transformation (IKEv1) ou une proposition (IKEv2), qui combine une méthode de chiffrement et une méthode d'authentification.

Les étapes suivantes montrent comment créer une proposition IKEv1 et IKEv2.

Procédure

Étape 1

Configurez un ensemble de transformation IKEv1 qui spécifie les algorithmes de chiffrement et de hachage IKEv1 d'IPsec à utiliser pour assurer l'intégrité des données.

crypto ipsec ikev1 transform-set *transform-set-name* (nom d'ensemble de transformation) *encryption-method* (méthode de chiffrement) [*authentication*]

Utilisez l'une des valeurs suivantes pour le chiffrement :

- esp-aes pour utiliser AES avec une clé de 128 bits.
- esp-aes-192 pour utiliser AES avec une clé de 192 bits.
- esp-aes-256 pour utiliser AES avec une clé de 256 bits.
- esp-null pour ne pas utiliser le chiffrement.

Utilisez l'une des valeurs suivantes pour l'authentification :

- esp-md5-hmac pour utiliser MD5/HMAC-128 comme algorithme de hachage.
- esp-sha-hmac pour utiliser SHA/HMAC-160 comme algorithme de hachage.
- esp-none pour ne pas utiliser l'authentification HMAC.

Exemple :

Pour configurer un ensemble de transformation IKEv1 à l'aide d'AES :

```
hostname(config)# crypto ipsec transform set FirstSet esp-aes esp-sha-hmac
```

Étape 2

Configurez un ensemble de propositions IKEv2 qui spécifie le protocole IPsec IKEv2 et les algorithmes de chiffrement et d'intégrité à utiliser.

esp spécifie le protocole IPsec d'Encapsulating Security Payload (ESP) (actuellement le seul protocole pris en charge pour IPsec).

crypto ipsec ikev2 ipsec-proposal *proposal_name*

protocol {esp} {**encryption** { | aes | aes-192 | aes-256 | } | **integrity** { | sha-1 }

Utilisez l'une des valeurs suivantes pour le chiffrement :

- aes pour utiliser AES (par défaut) avec un chiffrement de clé de 128 bits pour ESP.
- aes-192 pour utiliser AES avec un chiffrement de clé de 192 bits pour ESP.
- aes-256 pour utiliser AES avec un chiffrement de clé de 256 bits pour ESP.

Utilisez l'une des valeurs suivantes pour l'intégrité :

- sha-1 (par défaut) spécifie l'algorithme de hachage sécurisé (SHA) SHA-1, défini dans la norme FIPS (Federal Information Processing Standard) des États-Unis, pour la protection de l'intégrité d'ESP.

Pour configurer une proposition IKEv2 :

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure_proposal
```

```
hostname(config-ipsec-proposal)# protocol esp encryption aes integrity sha-1
```

Définir un groupe de tunnels

Un groupe de tunnels est un ensemble de politiques de connexion de tunnel. Vous configurez un groupe de tunnels pour identifier les serveurs AAA, préciser les paramètres de connexion et définir une stratégie de groupe par défaut. L'ASA stocke les groupes de tunnels en interne.

Il existe deux groupes de tunnels par défaut dans le système ASA : DefaultRAGroup, qui est le groupe de tunnels d'accès à distance par défaut, et DefaultL2Lgroup, qui est le groupe de tunnels par défaut de LAN à LAN. Vous pouvez modifier ces groupes, mais pas les supprimer. L'ASA utilise ces groupes pour configurer les paramètres de tunnel par défaut pour les groupes de tunnels d'accès à distance et de réseau local (LAN) lorsqu'aucun groupe de tunnels spécifique n'est identifié lors de la négociation du tunnel.

Procédure

- Étape 1** Créez un groupe de tunnels d'accès à distance IPsec (également appelé profil de connexion) :
- tunnel-group** *name* *type* *type*
- Exemple :**
- ```
hostname(config)# tunnel-group testgroup type ipsec-ra
hostname(config)#
```
- Étape 2** Entrez le mode d'attributs généraux du groupe de tunnels où vous pouvez saisir une méthode d'authentification :
- tunnel-group** *name* **general-attributes**
- Exemple :**
- ```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)#
```
- Étape 3** Précisez un ensemble d'adresses à utiliser pour le groupe de tunnels :
- address-pool** [(*nom de l'interface*)] *address_pool1* [...*address_pool6*]
- Exemple :**
- ```
hostname(config-general)# address-pool testpool
```
- Étape 4** Entrez en mode d'attributs IPsec de groupe de tunnels où vous pouvez entrer des attributs spécifiques à IPsec pour les connexions IKEv1 :
- tunnel-group** *name* **ipsec-attributes**
- Exemple :**
- ```
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-tunnel-ipsec)#
```

Étape 5 (Facultatif) Configurez une clé prépartagée (IKEv1 uniquement). La clé peut comporter entre 1 et 128 caractères alphanumériques.

Les clés de l'appareil de sécurité adaptatif et du client doivent être identiques. Si un client VPN Cisco avec une clé prépartagée de taille différente tente de se connecter, le client consigne un message d'erreur indiquant qu'il n'a pas réussi à authentifier l'homologue.

ikev1 pre-shared-key *key*

Exemple :

```
hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnfxx
```

Créer une carte de chiffrement dynamique

Les cartes de chiffrement dynamiques définissent des modèles de politique dans lesquels tous les paramètres ne sont pas configurés. Cela permet à l'ASA de recevoir des connexions d'homologues qui ont des adresses IP inconnues, comme les clients d'accès à distance.

Les entrées de carte de chiffrement dynamique identifient l'ensemble de transformation pour la connexion. Vous pouvez également activer le routage inverse, ce qui permet à l'ASA d'apprendre les informations de routage pour les clients connectés et de les annoncer via RIP ou OSPF.

Procédure

Étape 1 Créez une carte de chiffrement dynamique et spécifiez un ensemble de transformation IKEv1 ou une proposition IKEv2 pour la carte :

- Pour IKEv1, utilisez cette commande :

crypto dynamic-map *dynamic-map-name seq-num set ikev1 transform-set transform-set-name*

- Pour IKEv2, utilisez cette commande :

crypto dynamic-map *dynamic-map-name seq-num set ikev2 ipsec-proposal proposal-name*

Exemple :

```
hostname(config)# crypto dynamic-map dyn1 1 set ikev1 transform-set FirstSet
hostname(config)#
```

```
hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal secure_proposal
hostname(config)#
```

Étape 2 (Facultatif) Activez l'injection de route inverse pour toute connexion basée sur cette entrée de carte de chiffrement :

crypto dynamic-map *dynamic-map-name dynamic-seq-num set reverse-route*

Exemple :

```
hostname(config)# crypto dynamic-map dyn1 1 set reverse route
hostname(config)#
```

Créer une entrée de carte de chiffrement pour utiliser la carte de chiffrement dynamique

Créez une entrée de carte de chiffrement qui permet à l'ASA d'utiliser la carte de chiffrement dynamique pour définir les paramètres des associations de sécurité IPsec.

Dans les exemples suivants pour cette commande, le nom de la carte de chiffrement est mymap, le numéro de séquence est 1 et le nom de la carte de chiffrement dynamique est dyn1, que vous avez créée dans la rubrique [Créer une carte de chiffrement dynamique](#).

Procédure

Étape 1 Créez une entrée de carte de chiffrement qui utilise une carte de chiffrement dynamique :

crypto map *map-name* *seq-num* **ipsec-isakmp** **dynamic** *dynamic-map-name*

Exemple :

```
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
```

Étape 2 Appliquez la carte de chiffrement à l'interface externe :

crypto map *map-name* **interface** *interface-name*

Exemple :

```
hostname(config)# crypto map mymap interface outside
```

Étape 3 Enregistrez les modifications dans la configuration :

write memory

Configurer un VPN d'accès à distance IPSec IKEv2 en mode multicontexte

Pour plus d'informations sur la configuration des VPN d'accès à distance IPsec, consultez les sections suivantes :

- [Configurer une interface, à la page 202](#)
- [Configurer un ensemble d'adresses, à la page 204](#)
- [Ajouter un utilisateur, à la page 204](#)
- [Créer un ensemble de transformation IKEv1 ou une proposition IKEv2, à la page 204](#)
- [Définir un groupe de tunnels, à la page 206](#)
- [Créer une carte de chiffrement dynamique, à la page 207](#)
- [Créer une entrée de carte de chiffrement pour utiliser la carte de chiffrement dynamique, à la page 208](#)

Authentification VPN à l'aide de clés prépartagées post-quantiques

Vous pouvez configurer IKEv2 avec une nouvelle clé, une clé prépartagée (PPK) post-quantique, ainsi que des clés prépartagées (PSK) pour sécuriser la communication IPsec entre Secure Client et un ASA contre les attaques d'ordinateurs quantiques. Vous devez configurer des ensembles correspondants de PPK et de PSK sur le client et l'ASA pour une connexion IPsec sécurisée. Secure Client et ASA utilisent les clés PPK et PSK pour obtenir les clés de chiffrement et de déchiffrement du trafic réseau.

Les PPK sont générés par chiffrement au format binaire. Pour les configurations ASA et Secure Client, vous devez convertir le PPK binaire en une chaîne hexadécimale de 256 bits et de 64 caractères.

Conditions préalables à l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN

- Licence : l'ASA doit disposer d'une licence de cryptage renforcé
- Versions prises en charge
 - ASA Version 9.18.1 et ultérieures
 - Secure Client Version 5.1.8.x et ultérieures
- Configurez tous les autres paramètres sur l'ASA pour la connexion VPN d'accès à distance IPsec/IKEv2, comme l'ensemble d'adresses, la proposition IKEv2 et la carte de chiffrement
- Générez le PPK binaire.
- Convertissez le PPK binaire en chaîne hexadécimale de 64 caractères sur 256 bits.
- Configurez à la fois le PPK et les deux PSK pour Secure Client dans le Windows Credential Manager (WCM) de votre machine cliente. Consultez, [Configurer les clés prépartagées post-quantiques et les clés prépartagées dans Windows Credential Manager](#), à la page 211.
- Configurez les attributs PPK dans le profil VPN de Secure Client. Consultez, [Configurer le profil VPN pour Secure Client avec des attributs de clé prépartagée post-quantique](#), à la page 212.
- Assurez-vous que les valeurs PPK et PPK ID sont identiques sur l'ASA et dans Secure Client.

Lignes directrices et limites relatives à l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN

Directives

- L'administrateur doit assurer la génération, la qualité et la distribution des PPK et des PSK sur chaque périphérique client.

Restrictions

- Prend en charge uniquement IKEv2 avec PSK et PPK.
- Prend en charge uniquement Windows pour Secure Client.
- Le client ne peut stocker les informations d'authentification que pour un seul ASA dans WCM.

Flux de travail pour l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN

Tableau 10 : Flux de travail pour l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN

Étape	Action	Autres renseignements
1	Générez le PPK binaire et convertissez-le en une chaîne hexadécimale de 256 bits et 64 caractères.	-
2	Configurez le PPK et le PSK dans le gestionnaire d'informations d'authentification Windows (WCM).	Configurer les clés prépartagées post-quantiques et les clés prépartagées dans Windows Credential Manager, à la page 211
3	Configurez le profil VPN de Secure Client avec les paramètres PPK.	Configurer le profil VPN pour Secure Client avec des attributs de clé prépartagée post-quantique, à la page 212
4	Configurez le groupe de tunnels de l'ASA.	Configurer l'authentification VPN sur ASA à l'aide de clés prépartagées post-quantiques, à la page 212
5	L'utilisateur ouvre une session dans Secure Client pour se connecter à l'ASA.	-
6	Secure Client utilise le PPK_ID dans le profil VPN pour récupérer le PPK et deux PSK à partir du WCM.	-
7	Secure Client vérifie les paramètres PPK et PSK du WCM par rapport aux paramètres du groupe de tunnels de l'ASA.	-
8	Secure Client établit une connexion VPN avec l'ASA si les PPK et les PSK de Secure Client et de l'ASA correspondent. La connexion VPN avec l'ASA échoue si les PPK et PSK ne correspondent pas.	-

Configurer les clés prépartagées post-quantiques et les clés prépartagées dans Windows Credential Manager

Vous devez configurer des entrées d'informations d'authentification distinctes pour un PPK, un PSK local et un PSK distant.

Avant de commencer

Assurez-vous d'avoir consulté [Conditions préalables à l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN](#), à la page 209 et [Lignes directrices et limites relatives à l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN](#), à la page 209.

Procédure

-
Étape 1	Sur votre ordinateur client Windows, choisissez Control Panel (Panneau de configuration) > User Accounts (Comptes d'utilisateurs) > Credential Manager (Gestionnaire d'informations d'authentification) .
Étape 2	Cliquez sur l'onglet Windows Credentials (Informations d'authentification Windows).
Étape 3	Cliquez sur Add a Generic Credential (Ajouter une information d'identification générique).
Étape 4	Dans le champ Internet or network address (Adresse Internet ou réseau), spécifiez l'une des valeurs suivantes : • Pour un PPK, spécifiez la valeur suivante : AC/PPK/<HostAddress> : une clé prépartagée post-quantique. Il est stocké sous forme de 64 caractères hexadécimaux dans WCM et le client le convertit en binaire, puis inclut la clé dans la dérivation des clés de chiffrement et de déchiffrement dans IKEv2. • Pour une clé PSK locale, spécifiez la valeur suivante : AC/PSK_Local/<HostAddress> : PSK du client. • Pour une clé PSK distante, spécifiez la valeur suivante : AC/PSK_Remote/<HostAddress> : PSK de l'ASA.
Étape 5	Dans le champ User name (Nom d'utilisateur) , spécifiez la valeur n/a , car elle n'est pas utilisée par Secure Client.
Étape 6	Dans le champ Password (Mot de passe), spécifiez l'une des valeurs suivantes : • Pour un PPK, spécifiez une chaîne hexadécimale de 64 caractères de 256 bits. • Pour un PSK local et distant, spécifiez une chaîne qui définit l'alias du groupe de tunnels.
Étape 7	Cliquez sur OK .
-

Lorsque le client et l'ASA sont correctement configurés, le client utilise le PPK_ID dans le profil VPN pour récupérer le PPK et les deux PSK à partir de WCM. Secure Client utilise les valeurs PPK et PSK ci-dessus, convertit le PPK en binaire, fait correspondre les valeurs PPK et PSK avec la configuration de l'ASA, puis effectue l'authentification VPN. Aucune autre entrée n'est requise pour l'établissement de la connexion VPN, car ces trois clés sont les informations d'authentification.

Configurer le profil VPN pour Secure Client avec des attributs de clé prépartagée post-quantique

Le paramètre **HostEntry** dans le profil VPN comprend les nouveaux champs suivants pour configurer les paramètres PPK pour Secure Client :

- **IKEIdentity** : spécifiez une chaîne pour identifier l'ASA homologue. Cette chaîne doit correspondre au nom du groupe de tunnels dans l'ASA.
- **PPK_ID** : spécifiez une chaîne unique pour identifier le PPK. Cette valeur doit correspondre à l'ID PPK dans l'ASA.
- **PPK_mandatory** : spécifiez la valeur « true » si le PPK est obligatoire pour la connexion VPN. Si vous ne configurez pas cette valeur, la configuration PPK sera facultative.

Exemple

Un exemple d'entrée d'hôte dans le profil VPN est donné ci-dessous :

```
<HostEntry>
<HostName> ASAv_PPK</HostName>
<HostAddress>192.168.1.2</HostAddress>
<UserGroup>IPSec_Profile</UserGroup>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true</StandardAuthenticationOnly>
  <IKEIdentity>secure_client_PPK</IKEIdentity>
  <PPK_ID>PPKID_test</PPK_ID>
</PrimaryProtocol>
</HostEntry>
```

Configurer l'authentification VPN sur ASA à l'aide de clés prépartagées post-quantiques

Les groupes de tunnels sur l'ASA identifient la stratégie de groupe d'une connexion VPN. Vous pouvez configurer la stratégie du groupe de tunnels pour activer l'authentification VPN à l'aide de PPK et de PSK.

Avant de commencer

Assurez-vous d'avoir consulté [Conditions préalables à l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN](#), à la page 209 et [Lignes directrices et limites relatives à l'utilisation de clés prépartagées post-quantiques pour l'authentification VPN](#), à la page 209.

Procédure

Étape 1 Configurez les attributs IPsec du groupe de tunnels.

tunnel-group name ipsec-attributes

Exemple :

```
hostname(config)# tunnel-group secure_client_PPK ipsec-attributes
hostname(config-tunnel-ipsec)#
```

Étape 2 Configurer le PSK du client.

ikev2 remote-authentication pre-shared-key *key*

Exemple :

```
hostname(config-tunnel-ipsec)#ikev2 remote-authentication pre-shared-key *****
```

Étape 3 Configurer le PSK de l'ASA

ikev2 local-authentication pre-shared-key *key*

Exemple :

```
hostname(config-tunnel-ipsec)#ikev2 local-authentication pre-shared-key *****
```

Étape 4 Configurer le PPK du client

ikev2 remote-authentication post-quantum-key *key* **identifier** *id* **mandatory**

- **key** (clé) : spécifiez la clé PPK.
- **ID** : spécifiez la chaîne unique permettant d'identifier le PPK. Cette valeur doit correspondre à l'ID PPK dans le profil VPN de Secure Client.
- **mandatory** (obligatoire) : spécifiez si PPK est obligatoire pour la connexion VPN. Si vous ne spécifiez pas obligatoire, la configuration PPK sera facultative.

Exemple :

```
hostname(config-tunnel-ipsec)#ikev2 remote-authentication post-quantum-key *****
  identifier PPKID_test mandatory
```

L'exemple suivant montre un extrait de la configuration du groupe de tunnels de l'ASA à l'aide de PPK et de PSK :

Exemple

```
tunnel-group secure_client_PPK ipsec-attributes
  ikev2 remote-authentication pre-shared-key *****
  ikev2 local-authentication pre-shared-key *****
  ikev2 remote-authentication post-quantum-key ***** identity PPKID_test mandatory
```

Tenez compte des points suivants :

- Le nom du groupe de tunnels doit correspondre à la chaîne IKEIdentity du profil VPN.
- L'ID PPK dans la configuration du groupe de tunnels doit correspondre à l'ID_PPK du profil VPN.

Références supplémentaires

- RFC 8784
- Guide de l'administrateur de Cisco Secure Client (y compris AnyConnect), version 5

Exemples de configuration pour les VPN d'accès à distance IPsec

L'exemple suivant montre comment configurer un VPN IPsec/IKEv1 d'accès à distance :

```
hostname(config)# crypto ikev1 policy 10
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption aes-256
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config)# crypto ikev1 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev1 transform set AES256-SHA
esp-aes-256 esp-sha-hmac
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-ipsec)# ikev1 pre-shared-key ravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev1
transform-set AES256-SHA
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
hostname(config)# crypto map CMAP interface outside
```

L'exemple suivant montre comment configurer un VPN IPsec/IKEv2 d'accès à distance :

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)# integrity sha512
hostname(config-ikev2-policy)# prf sha512
hostname(config)# crypto ikev2 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev2 ipsec-proposal AES256-SHA512
hostname(config-ipsec-proposal)# protocol esp encryption aes-256
hostname(config-ipsec-proposal)# protocol esp integrity sha-512
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-tunnel-ipsec)# ikev2 local-authentication
pre-shared-key localravpnkey
hostname(config-tunnel-ipsec)# ikev2 remote-authentication
pre-shared-key remoteravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev2
ipsec-proposal AES256-SHA512
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
hostname(config)# crypto map CMAP interface outside
```

Exemples de configuration pour le VPN d'accès à distance IPsec IKEv2 basé sur les normes en mode multi-contexte

Les exemples suivants montrent comment configurer l'ASA pour le VPN d'accès à distance IPsec/IKEv2 basé sur les normes en mode multicontexte. Les exemples fournissent respectivement des renseignements sur les configurations du contexte système et du contexte d'utilisateur.

Pour la configuration de contexte système :

```
class default
  limit-resource All 0
  limit-resource Mac-addresses 65536
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource VPN AnyConnect 4.0%

hostname(config)#context CTX2
hostname(config-ctx)#member default =====> License allotment for contexts using
class
hostname(config-ctx)#allocate-interface Ethernet1/1.200
hostname(config-ctx)#allocate-interface Ethernet1/3.100
hostname(config-ctx)#config-url disk0:/CTX2.cfg
```

Pour la configuration en contexte d'utilisateur :

```
hostname/CTX2(config)#ip local pool CTX2-pool 1.1.2.1-1.1.2.250 mask 255.255.255.0
hostname/CTX2(config)#aaa-server ISE protocol radius
hostname/CTX2(config)#aaa-server ISE (inside) host 10.10.190.100
hostname/CTX2(config-aaa-server-host)#key *****
hostname/CTX2(config-aaa-server-host)#exit
hostname/CTX2(config)#

hostname/CTX2(config)#group-policy GroupPolicy_CTX2-IKEv2 internal
hostname/CTX2(config)#group-policy GroupPolicy_CTX2-IKEv2 attributes
hostname/CTX2(config-group-policy)#vpn-tunnel-protocol ikev2
hostname/CTX2(config-group-policy)#exit
hostname/CTX2(config)#

hostname/CTX2(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX2(config)#crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTOMAP
hostname/CTX2(config)#crypto map outside_map interface outside
```

Les connexions d'accès à distance IPsec/IKEv2 des clients basés sur des normes aboutissent par défaut au groupe de tunnels DefaultRAGroup :

```
hostname/CTX2(config)#tunnel-group DefaultRAGroup type remote-access
hostname/CTX2(config)#tunnel-group DefaultRAGroup general-attributes
hostname/CTX2(config-tunnel-general)#default-group-policy GroupPolicy_CTX2-IKEv2
hostname/CTX2(config-tunnel-general)#address-pool CTX2-pool
hostname/CTX2(config-tunnel-general)#authentication-server-group ISE
```

```

hostname/CTX2 (config-tunnel-general) #exit
hostname/CTX2 (config) #

hostname/CTX2 (config) #tunnel-group DefaultRAGroup ipsec-attributes
hostname/CTX2 (config-tunnel-ipsec) #ikev2 remote-authentication eap query-identity
hostname/CTX2 (config-tunnel-ipsec) #ikev2 local-authentication certificate ASDM_TrustPoint0
hostname/CTX2 (config-tunnel-ipsec) #exit
hostname/CTX2 (config) #

```

Exemples de configuration pour le VPN d'accès à distance Secure Client (services client sécurisés) IPsec IKEv2 en mode multicontexte

Les exemples suivants montrent comment configurer l'ASA pour le VPN d'accès à distance IPsec/IKEv2 Secure Client (services client sécurisés) en mode multicontexte. Les exemples fournissent respectivement des renseignements sur les configurations du contexte système et du contexte d'utilisateur.

Pour la configuration de contexte système :

```

class default
  limit-resource All 0
  limit-resource Mac-addresses 65536
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource VPN AnyConnect 4.0%

hostname (config) #context CTX3
hostname (config-ctx) #member default =====> License allotment for contexts using
class
hostname (config-ctx) #allocate-interface Ethernet1/1.200
hostname (config-ctx) #allocate-interface Ethernet1/3.100
hostname (config-ctx) #config-url disk0:/CTX3.cfg

```

La création d'un système de fichiers virtuel pour chaque contexte peut contenir des fichiers Secure Client (services client sécurisés) comme l'image et le profil.

```
hostname (config-ctx) #storage-url shared disk0:/shared disk0
```

Pour la configuration en contexte d'utilisateur :

```

hostname/CTX3 (config) #ip local pool ctx3-pool 1.1.3.1-1.1.3.250 mask 255.255.255.0
hostname/CTX3 (config) #webvpn
hostname/CTX3 (config-webvpn) #enable outside
hostname/CTX3 (config-webvpn) # anyconnect image
disk0:/anyconnect-win-4.6.00010-webdeploy-k9.pkg 1
hostname/CTX3 (config-webvpn) #anyconnect profiles IKEv2-ctx1 disk0:/ikev2-ctx1.xml
hostname/CTX3 (config-webvpn) #anyconnect enable
hostname/CTX3 (config-webvpn) #tunnel-group-list enable

hostname/CTX3 (config) #username cisco password *****
hostname/CTX3 (config) #ssl trust-point ASDM_TrustPoint0 outside

```



```
hostname/CTX3(config)#group-policy GroupPolicy_CTX3-IKEv2 internal
hostname/CTX3(config)#group-policy GroupPolicy_CTX3-IKEv2 attributes

hostname/CTX3(config-group-policy)#vpn-tunnel-protocol ikev2 ssl-client
hostname/CTX3(config-group-policy)#dns-server value 10.3.5.6
hostname/CTX3(config-group-policy)#wins-server none
hostname/CTX3(config-group-policy)#default-domain none
hostname/CTX3(config-group-policy)#webvpn
hostname/CTX3(config-group-webvpn)#anyconnect profiles value IKEv2-ctx1 type user
```

Dans l'exemple ci-dessous, pour activer les services client, utilisez la commande **crypto ikev2 enable outside client-services**.

Le serveur de services client fournit un accès HTTPS (SSL) pour permettre au téléchargeur Secure Client de recevoir les mises à jour logicielles, les profils, les fichiers de localisation et de personnalisation, les CSD, les SCEP et les autres téléchargements de fichiers requis par le client. Si vous sélectionnez cette option, précisez le numéro de port des services client. Si vous n'activez pas le serveur de services client, les utilisateurs ne pourront pas télécharger les fichiers dont le Secure Client pourrait avoir besoin.



Remarque

Vous pouvez utiliser le même port que celui que vous utilisez pour le VPN SSL sur le même périphérique. Même si vous avez configuré un VPN SSL, vous devez sélectionner cette option pour activer les téléchargements de fichiers sur SSL pour les clients IPsec-IKEv2.

```
hostname/CTX3(config)#crypto ikev2 enable outside client-services port 443
hostname/CTX3(config)#crypto ikev2 remote-access trustpoint ASDM_TrustPoint0
hostname/CTX3(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX3(config)#crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTOMAP
hostname/CTX3(config)#crypto map outside_map interface outside

hostname/CTX3(config)#tunnel-group CTX3-IKEv2 type remote-access
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 general-attributes
hostname/CTX3(config-tunnel-general)#default-group-policy GroupPolicy_CTX3-IKEv2
hostname/CTX3(config-tunnel-general)#address-pool ctx3-pool
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 webvpn-attributes
hostname/CTX3(config-tunnel-webvpn)#group-alias CTX3-IKEv2 enable
```

Historique des VPN d'accès à distance

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
VPN d'accès à distance pour IPsec IKEv1 et SSL.	7.0	Les VPN d'accès à distance permettent aux utilisateurs de se connecter à un site central par le biais d'une connexion sécurisée sur un réseau TCP/IP comme Internet.
VPN d'accès à distance pour IPsec IKEv2.	v 8.4(1)	Ajout de la prise en charge d'IPsec IKEv2 pour le Secure Client (services client sécurisés).

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge automatique de MOBIKE pour les VPN d'accès à distance.	9.8(1)	Ajout de la prise en charge de Mobile IKE (MOBIKE) pour les VPN d'accès à distance IPsec IKEv2. Mobike est toujours activé. Ajout de la commande <code>ikev2 mobike-rrc</code> pour activer la vérification de la routabilité de retour pendant les communications mobike pour les connexions VPN IKEv2 RA.
Prise en charge des VPN d'accès à distance IPsec IKEv2 en mode multi-contexte	9.9(2)	Prise en charge de la configuration d'ASA pour permettre à Secure Client (services client sécurisés) et aux clients VPN IPsec IKEv2 tiers basés sur les normes d'établir des sessions VPN d'accès à distance avec l'ASA fonctionnant en mode de contexte multiple. Ajout de la commande <code>ikev2 rsa-sig-hash sha1</code> pour signer la charge utile d'authentification.
RSA avec algorithme de hachage SHA-1 pour signer la charge utile d'authentification	9.12(1)	Prise en charge de la signature de la charge utile d'authentification avec l'algorithme de hachage SHA-1 lors de l'utilisation de clients VPN IPsec IKEv2 tiers basés sur les normes pour établir des sessions VPN d'accès à distance avec l'ASA.
Dépréciation des chiffrements IKE/IPsec (chiffrement et intégrité/PRF) Prise en charge du groupe DH 14 pour IKEv1	9.13(1)	Les chiffrements/intégrité/PRF suivants sont obsolètes et seront supprimés dans la version ultérieure - 9.14(1) : • Chiffrement 3DES • Chiffrement DES • Intégrité MD5 Ajout de la prise en charge du groupe DH 14 (par défaut) pour IKEv1. Les options de commande groupe 2 et groupe 5 ont été abandonnées et seront supprimées dans la version ultérieure - 9.14(1).



CHAPITRE 8

VPN IPsec de LAN à LAN

Un VPN de LAN à LAN connecte des réseaux dans différents emplacements géographiques.

Vous pouvez créer des connexions IPsec de LAN à LAN avec des homologues Cisco et des homologues tiers conformes à toutes les normes pertinentes. Ces homologues peuvent avoir n'importe quelle combinaison d'adresses IPv4 et IPv6 internes et externes.

L'ASA ne permet pas au trafic d'origine locale autre que le message ping de passer par le tunnel VPN.

Ce chapitre décrit comment établir une connexion VPN de LAN à LAN.

- [Résumé de la configuration, à la page 219](#)
- [Configurer le VPN de site à site en mode de contexte multiple, à la page 220](#)
- [Interfaces de configuration, à la page 221](#)
- [Configurer la politique ISAKMP et activer ISAKMP sur l'interface externe, à la page 222](#)
- [Créer un ensemble de transformation IKEv1, à la page 227](#)
- [Créer une proposition IKEv2, à la page 228](#)
- [Configurer une ACL, à la page 229](#)
- [Définition d'un groupe de tunnels, à la page 230](#)
- [Créer une carte de chiffrement et l'appliquer à une interface, à la page 231](#)

Résumé de la configuration

Cette section fournit un résumé de l'exemple de configuration LAN-à-LAN décrit dans ce chapitre. Les sections ultérieures fournissent des instructions détaillées.

```
hostname(config)# interface ethernet0/0
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption aes
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)# lifetime 43200
hostname(config)# crypto ikev1 enable outside
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# # encryption aes
hostname(config-ikev2-policy)# group 2
hostname(config-ikev12-policy)# prf sha
```

```

hostname(config-ikev2-policy)# lifetime 43200
hostname(config)# crypto ikev2 enable outside
hostname(config)# crypto ipsec ikev1 transform-set FirstSet esp-aes esp-sha-hmac
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)# protocol esp encryption aes
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config)# access-list 121_list extended permit ip 192.168.0.0 255.255.0.0 150.150.0.0
255.255.0.0
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key 44kkao159636jnfx
hostname(config)# crypto map abcmap 1 match address 121_list
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)# crypto map abcmap 1 set ikev1 transform-set FirstSet
hostname(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname(config)# crypto map abcmap interface outside
hostname(config)# write memory

```

Configurer le VPN de site à site en mode de contexte multiple

Suivez ces étapes pour permettre la prise en charge de site à site en mode multi-contexte. En effectuant ces étapes, vous pouvez voir comment l'affectation des ressources se décompose.

Procédure

- Étape 1** Pour configurer le VPN en mode multi-contexte, configurez une classe de ressources et choisissez les licences VPN dans le cadre des ressources autorisées. La « configuration d'une classe pour la gestion des ressources » présente ces étapes de configuration. Voici un exemple de configuration :

```

class ctx1
  limit-resource VPN Burst Other 100
  limit-resource VPN Other 1000

```

- Étape 2** Configurez un contexte et faites-en membre de la classe configurée qui autorise les licences VPN. Voici un exemple de configuration :

```

context context1
  member ctx1
  allocate-interface GigabitEthernet3/0.2
  allocate-interface GigabitEthernet3/1.2
  allocate-interface Management0/0
  config-url disk0:/sm_s2s_ik1_ip4_no_webvpn.txt
  join-failover-group 1

```

- Étape 3** Configurez les profils de connexion, les politiques, les cartes de chiffrement, etc., comme vous le feriez avec une configuration VPN de site à site en mode contexte unique.

Interfaces de configuration

Un ASA comporte au moins deux interfaces, appelées ici outside et inside. En règle générale, l'interface externe est connectée à l'Internet public, tandis que l'interface interne est connectée à un réseau privé et est protégée contre tout accès public.

Pour commencer, configurez et activez deux interfaces sur l'ASA. Attribuez ensuite un nom, une adresse IP et un masque de sous-réseau. Vous pouvez également configurer son niveau de sécurité, sa vitesse et son fonctionnement en duplex sur l'appareil de sécurité.



Remarque

L'adresse de l'interface externe de l'ASA (pour IPv4 et IPv6) ne peut pas chevaucher l'espace d'adresse du côté privé.

Procédure

- Étape 1** Pour passer en mode de configuration d'interface, en mode de configuration globale, saisissez la commande **interface** avec le nom par défaut de l'interface à configurer. Dans l'exemple suivant, l'interface est ethernet0.

```
hostname(config)# interface ethernet0/0
hostname(config-if)#
```

- Étape 2** Pour définir l'adresse IP et le masque de sous-réseau de l'interface, saisissez la commande **ip address**. Dans l'exemple suivant, l'adresse IP est 10.10.4.100 et le masque de sous-réseau est 255.255.0.0.

```
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)#
```

- Étape 3** Pour nommer l'interface, entrez la commande **nameif**, maximum de 48 caractères. Vous ne pourrez pas modifier ce nom ultérieurement. Dans l'exemple suivant, le nom de l'interface ethernet0 est externe.

```
hostname(config-if)# nameif outside
hostname(config-if)##
```

- Étape 4** Pour activer l'interface, saisissez la version **no** de la commande **shutdown**. Par défaut, les interfaces sont désactivées.

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

- Étape 5** Pour enregistrer vos modifications, entrez la commande **write memory** :

```
hostname(config-if)# write memory
hostname(config-if)#
```

- Étape 6** Pour configurer une deuxième interface, utilisez la même procédure.

Configurer la politique ISAKMP et activer ISAKMP sur l'interface externe

ISAKMP est le protocole de négociation qui permet à deux hôtes de s'accorder sur la façon de créer une association de sécurité IPsec (SA). Il fournit un cadre commun pour convenir du format des attributs SA. Cela inclut la négociation avec l'homologue au sujet de la SA et la modification ou la suppression de la SA. ISAKMP sépare la négociation en deux étapes : la phase 1 et la phase 2. La phase 1 crée le premier tunnel, qui protège les messages de négociation ISAKMP ultérieurs. La phase 2 crée le tunnel qui protège les données.

IKE utilise ISAKMP pour configurer la SA pour l'utilisation d'IPsec. IKE crée les clés cryptographiques utilisées pour authentifier les homologues.

L'ASA prend en charge IKEv1 pour les connexions de l'ancien client VPN Cisco et IKEv2 pour le client VPN AnyConnect.

Pour définir les termes des négociations ISAKMP, vous créez une politique IKE, qui comprend les éléments suivants :

- Le type d'authentification requis pour l'homologue IKEv1, soit signature RSA à l'aide de certificats, soit clé prépartagée (PSK).
- Une méthode de chiffrement pour protéger les données et garantir la confidentialité.
- Une méthode HMAC (hachage de codes d'authentification de message) pour s'assurer de l'identité de l'expéditeur et pour s'assurer que le message n'a pas été modifié pendant le transfert.
- Un groupe Diffie-Hellman pour déterminer la force de l'algorithme de détermination de la clé de chiffrement. L'ASA utilise cet algorithme pour dériver les clés de chiffrement et de hachage.
- Pour IKEv2, une fonction pseudo-aléatoire (PRF) distincte est utilisée comme algorithme pour dériver le matériel de clé et effectuer les opérations de hachage nécessaires au chiffrement du tunnel IKEv2.
- Une limite de temps pendant laquelle le périphérique utilise une clé de chiffrement avant de la remplacer.

Avec les politiques IKEv1, pour chaque paramètre, vous définissez une valeur. Pour IKEv2, vous pouvez configurer plusieurs algorithmes de chiffrement et d'authentification pour une seule politique. Le système classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue dans cet ordre. Cela vous permet d'envoyer potentiellement une seule proposition pour transmettre toutes les combinaisons autorisées au lieu d'avoir besoin d'envoyer chaque combinaison autorisée individuellement, comme avec IKEv1.

Les sections suivantes fournissent des procédures pour créer des politiques IKEv1 et IKEv2 et les activer sur une interface :

- [Configurer les politiques ISAKMP pour les connexions IKEv1, à la page 222](#)
- [Configurer les politiques ISAKMP pour les connexions IKEv2, à la page 224](#)

Configurer les politiques ISAKMP pour les connexions IKEv1

Pour configurer les politiques ISAKMP pour les connexions IKEv1, utilisez la commande de priorité **crypto ikev1 policy** pour passer en mode de configuration de politique IKEv1 où vous pouvez configurer les paramètres IKEv1.

Procédure

Étape 1 Entrez en mode de configuration de politique IPsec IKEv1. Par exemple :

```
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)#
```

Étape 2 Définissez la méthode d'authentification. L'exemple suivant configure une clé prépartagée :

```
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)#
```

Étape 3 Choisissez la méthode de chiffrement. L'exemple suivant configure l' :

```
hostname(config-ikev1-policy)# encryption aes
hostname(config-ikev1-policy)#
```

Étape 4 Définissez la méthode HMAC. L'exemple suivant configure SHA-1 :

```
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)#
```

Étape 5 Définissez le groupe Diffie-Hellman. L'exemple suivant configure le groupe 14 :

```
hostname(config-ikev1-policy)# group 14
hostname(config-ikev1-policy)#
```

Étape 6 Définissez la durée de vie de la clé de chiffrement. L'exemple suivant configure 43 200 secondes (12 heures) :

```
hostname(config-ikev1-policy)# lifetime 43200
hostname(config-ikev1-policy)#
```

Étape 7 Activez IKEv1 sur l'interface nommée outside en mode contexte unique ou multiple :

```
hostname(config)# crypto ikev1 enable outside
hostname(config)#
```

Étape 8 Pour enregistrer vos modifications, entrez la commande **write memory** :

```
hostname(config)# write memory
hostname(config)#
```

Configurer les politiques ISAKMP pour les connexions IKEv2

Pour configurer les politiques ISAKMP pour les connexions IKEv2, utilisez la commande de priorité **crypto ikev2 policy** pour passer en mode de configuration de politique IKEv2 où vous pouvez configurer les paramètres IKEv2.

Procédure

-
- Étape 1** Entrez en mode de configuration de politique IPsec IKEv2. Par exemple :
- ```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)#
```
- Étape 2** Choisissez la méthode de chiffrement. L'exemple suivant configure AES :
- ```
hostname(config-ikev2-policy)# encryption aes
hostname(config-ikev2-policy)#
```
- Étape 3** Définissez le groupe Diffie-Hellman. L'exemple suivant configure le groupe 15 :
- ```
hostname(config-ikev2-policy)# group 15
hostname(config-ikev2-policy)#
```
- Étape 4** Définissez la fonction pseudo-aléatoire (PRF) utilisée comme algorithme pour générer le matériel de clé et les opérations de hachage nécessaires au chiffrement du tunnel IKEv2. L'exemple suivant configure SHA-1 (une variante de HMAC) :
- ```
hostname(config-ikev2-policy)# prf sha
hostname(config-ikev2-policy)#
```
- Étape 5** Définissez la durée de vie de la clé de chiffrement. L'exemple suivant configure 43 200 secondes (12 heures) :
- ```
hostname(config-ikev2-policy)# lifetime seconds 43200
hostname(config-ikev2-policy)#
```
- Étape 6** Activez IKEv2 sur l'interface nommée outside :
- ```
hostname(config)# crypto ikev2 enable outside
hostname(config)#
```
- Étape 7** Pour enregistrer vos modifications, entrez la commande **write memory** :
- ```
hostname(config)# write memory
hostname(config)#
```
- 

## Plusieurs échanges de clés pour IKEv2

IKEv2 utilise des groupes Diffie-Hellman (DH) pour établir un secret partagé entre un initiateur et un répondeur. IKEv2 prend en charge les échanges de clés supplémentaires pour sécuriser la communication IPsec contre



les attaques d'ordinateurs quantiques. Chaque échange utilise des groupes DH différents. Le secret partagé calculé pour la configuration SA est une combinaison de toutes les clés dérivées de chaque échange. Une SA IKE est établie après les multiples échanges de clés entre les homologues IKE.

L'ASA utilise sept nouveaux types de transformation pour les échanges de clés multiples :

- Échange de clé supplémentaire : valeur IANA 6
- Échange de clé supplémentaire : valeur IANA 7
- Échange de clé supplémentaire : valeur IANA 8
- Échange de clé supplémentaire : valeur IANA 9
- Échange de clé supplémentaire : valeur IANA 10
- Échange de clé supplémentaire : valeur IANA 11
- Échange de clé supplémentaire : valeur IANA 12

Vous pouvez configurer un maximum de sept échanges de clés multiples. Pour chaque échange de clés supplémentaire que vous configurez, vous devez préciser les groupes DH. L'ASA chiffre les échanges de clés intermédiaires à l'aide des clés dérivées de l'échange précédent. Si les homologues entre l'initiateur et le répondeur ne s'accordent pas avec un groupe DH, la négociation échoue et une notification d'erreur **NO\_PROPOSAL\_CHOSEN** est envoyée à l'initiateur. Vous pouvez également configurer la transformation comme nulle. Ce faisant, l'échange de clés n'a pas lieu.

Pour un initiateur, si la méthode d'échange de clés est configurée à **aucune** pour un échange de clés supplémentaire *n* :

- Le répondeur peut choisir la méthode d'échange de clés comme **none** pour l'échange de clés supplémentaire *n*.
- L'échange de clés supplémentaire est optionnel.

Pour une négociation de proposition réussie, toutes les transformations de la proposition de l'initiateur doivent correspondre aux transformations du répondeur.

Dans l'exemple suivant pour un initiateur :

```
crypto ikev2 policy 1
encryption aes
integrity sha256
group 14
prf sha256
lifetime seconds 120
additional-key-exchange 5
key-exchange-method none
```

Le répondeur doit avoir un échange de clé supplémentaire 5 pour que la proposition corresponde.

Si l'homologue ne prend pas en charge l'échange de clé supplémentaire, l'un des événements suivants se produit :

- Si l'initiateur a une autre proposition IKEv2 qui correspond à la proposition du répondeur, une SA IKEv2 est établie.
- L'homologue traite tout type de transformation d'échange de clés supplémentaire dans le message d'échange **IKE\_SA\_INIT** comme un type inconnu et ignore ces propositions. La négociation échoue et une notification d'erreur **NO\_PROPOSAL\_CHOSEN** est envoyée à l'initiateur.

Pour en savoir plus sur cette fonctionnalité, consultez la RFC 9242.

## Lignes directrices et limites relatives aux échanges de clés multiples, IKEv2

- Vous pouvez avoir un maximum de sept échanges de clés multiples.
- Vous ne pouvez pas utiliser le même groupe DH dans les échanges de clés suivants.

Pour cette fonctionnalité, l'ASA ne prend pas en charge :

- IKEv1
- Combinaison d'un échange de clés classique et d'un échange de clés fondé sur un algorithme post-quantique.
- VPN d'accès à distance. Seuls les VPN de site à site prennent en charge les échanges de clés multiples IKEv2.
- Mise en grappes

## Vérifier les configurations d'échanges de clés multiples IKEv2

Utilisez les commandes show suivantes pour afficher ou vérifier les configurations d'échanges de clés multiples IKEv2 :

### • show running-config crypto ikev2

```
crypto ikev2 policy 1
encryption aes
integrity sha256
group 14
prf sha256
lifetime seconds 120
additional-key-exchange 1
key-exchange-method 21 31
additional-key-exchange 2
key-exchange-method 20 21
...
```

### • show crypto ikev2 sa detail

```
IKEv2 SAs:
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local Remote fvrf/ivrf Status Role
41567725 192.168.15.1/500 192.168.15.2/500 READY INITIATOR
Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Additional Key Exchange Group: AKE1: 31 AKE2: 21 AKE3: 20 AKE4: 19 AKE5: 16 AKE6: 15
AKE7: 14
Life/Active Time: 120/5 sec
Session-id: 4
Status Description: Negotiation done
Local spi: 6BB6B7BFA0BAADF4 Remote spi: 7030C7xxx xxxxxxE9DBDE77EB
Local id: 192.168.15.1
Remote id: 192.168.15.2
Local req mess id: 9 Remote req mess id: 0
Local next mess id: 9 Remote next mess id: 0
Local req queued: 9 Remote req queued: 0
Local window: 1 Remote window: 1
DPD configured for 10 seconds, retry 2
NAT-T is not detected
IKEv2 Fragmentation Configured MTU: 576 bytes, Overhead: 28 bytes, Effective MTU: 548
```

```

bytes
Parent SA Extended Status:
Delete in progress: FALSE
Marked for delete: FALSE
Child sa: local selector 20.0.0.0/0 - 20.0.0.255/65535
remote selector 30.0.0.0/0 - 30.0.0.255/65535
ESP spi in/out: 0x4a7d5da2/0x56a28fa8
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel

```

## Créer un ensemble de transformation IKEv1

Un ensemble de transformation IKEv1 combine une méthode de chiffrement et une méthode d'authentification. Lors de la négociation de l'association de sécurité IPsec avec ISAKMP, les homologues conviennent d'utiliser un ensemble de transformation particulier pour protéger un flux de données particulier. L'ensemble de transformation doit être le même pour les deux homologues.

Un ensemble de transformation protège les flux de données pour l'ACL spécifiée dans l'entrée de carte de chiffrement associée. Vous pouvez créer des ensembles de transformations dans la configuration ASA, puis spécifier un maximum de 11 parmi ceux-ci dans une carte de chiffrement ou une entrée de carte de chiffrement dynamique.

Le tableau ci-dessous répertorie les méthodes de chiffrement et d'authentification valides.

**Tableau 11 : Méthodes de chiffrement et d'authentification valides**

| Méthodes de chiffrement valides             | Méthodes d'authentification valides |
|---------------------------------------------|-------------------------------------|
|                                             | esp-sha-hmac (par défaut)           |
| esp-aes (chiffrement 128 bits) (par défaut) |                                     |
| esp-aes-192                                 |                                     |
| esp-aes-256                                 |                                     |
| esp-null                                    |                                     |

Le mode tunnel est la méthode habituelle pour mettre en œuvre IPsec entre deux ASAs connectés sur un réseau non fiable, tel qu'Internet. Le mode tunnel est la configuration par défaut et ne nécessite aucune configuration.

Pour configurer un ensemble de transformations, effectuez les tâches de site à site suivantes en mode contexte unique ou multiple :

## Procédure

**Étape 1** En mode de configuration globale, entrez la commande **crypto ipsec ikev1 transform-set**. L'exemple suivant configure un ensemble de transformation avec le nom FirstSet, le chiffrement esp-aes, , et l'authentification esp-sha-hmac. La syntaxe est la suivante :

esp-sha-hmac (par défaut)

**crypto ipsec ikev1 transform-set transform-set-name encryption-method authentication-method**

```
hostname(config)#
crypto ipsec transform-set FirstSet esp-aes esp-sha-hmac
hostname(config)#
```

**Étape 2** Enregistrez vos modifications.

```
hostname(config)# write memory
hostname(config)#
```

# Créer une proposition IKEv2

Pour IKEv2, vous pouvez configurer plusieurs algorithmes de chiffrement et d'authentification, et plusieurs algorithmes d'intégrité pour une seule politique. Le système classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue dans cet ordre. Cela vous permet d'envoyer potentiellement une seule proposition pour transmettre toutes les combinaisons autorisées au lieu d'avoir besoin d'envoyer chaque combinaison autorisée individuellement, comme avec IKEv1.

Le tableau ci-dessous répertorie les méthodes de chiffrement et d'authentification IKEv2 valides.

**Tableau 12 : Méthodes de chiffrement et d'intégrité IKEv2 valides**

| Méthodes de chiffrement valides                  | Méthodes d'intégrité valides |
|--------------------------------------------------|------------------------------|
|                                                  | sha (par défaut)             |
| aes (par défaut) - AES avec une clé de 128 bits. |                              |
| aes-192                                          |                              |
| aes-256                                          |                              |

Pour configurer une proposition IKEv2, effectuez les tâches suivantes en mode contexte unique ou multiple :

## Procédure

- Étape 1** En mode de configuration globale, utilisez la commande **crypto ipsec ikev2 ipsec-proposal** pour passer en mode de configuration de proposition ipsec où vous pouvez spécifier plusieurs types de chiffrement et d'intégrité pour la proposition. Dans cet exemple, *secure* est le nom de la proposition :
- ```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)#
```
- Étape 2** Saisissez ensuite un protocole et des types de chiffrement. ESP est le seul protocole pris en charge. Par exemple :
- ```
hostname(config-ipsec-proposal)# protocol esp encryption aes
hostname(config-ipsec-proposal)#
```
- Étape 3** Saisissez un type d'intégrité. Par exemple :
- ```
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config-ipsec-proposal)#
```
- Étape 4** Enregistrez vos modifications.

Configurer une ACL

L'ASA utilise des listes de contrôle d'accès pour contrôler l'accès au réseau. Par défaut, l'appareil de sécurité adaptatif refuse tout le trafic. Vous devez configurer une liste de contrôle d'accès qui autorise le trafic. Pour en savoir plus, consultez « Renseignements sur les listes de contrôle d'accès » dans le guide de configuration sur les opérations générales.

Les listes de contrôle d'accès que vous configurez pour ces connexions de contrôle VPN de réseau local (LAN) à réseau local (LAN) sont basées sur les adresses IP source et de destination traduite et, éventuellement, sur les ports. Configurez des listes de contrôle d'accès qui sont symétriques des deux côtés de la connexion.

Une liste de contrôle d'accès pour le trafic VPN utilise l'adresse traduite.



Remarque

Pour plus d'informations sur la configuration d'une liste de contrôle d'accès avec un filtre VPN, consultez [Préciser un réseau VLAN pour l'accès à distance ou appliquer une règle de contrôle d'accès unifiée à la stratégie de groupe](#), à la page 141.

Procédure

- Étape 1** Entrez la commande **access-list extended**.

access-list listname extended permit ip source-ipaddress source-netmask destination-ipaddress destination-netmask

L'exemple suivant configure une liste de contrôle d'accès nommée `l2l_list` qui permet au trafic des adresses IP du réseau 192.168.0.0 d'accéder au réseau 150.150.0.0.

```
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0 150.150.0.0
255.255.0.0
hostname(config)#
```

Étape 2

Configurez une liste de contrôle d'accès pour l'ASA de l'autre côté de la connexion qui reflète l'ACL.

Les sous-réseaux qui sont définis dans une liste de contrôle d'accès dans une carte de chiffrement ou dans deux listes de contrôle d'accès de chiffrement différentes qui sont associées à la même carte de chiffrement ne doivent pas se chevaucher.

Dans l'exemple suivant, l'invite pour l'homologue est `hostname2`.

```
hostname2(config)# access-list l2l_list extended permit ip 150.150.0.0 255.255.0.0 192.168.0.0
255.255.0.0
hostname2(config)#
```

Définition d'un groupe de tunnels

Un groupe de tunnels est un ensemble d'enregistrements qui contiennent des politiques de connexion de tunnel. Vous configurez un groupe de tunnels pour identifier les serveurs AAA, préciser les paramètres de connexion et définir une stratégie de groupe par défaut. L'ASA stocke les groupes de tunnels en interne.

Il existe deux groupes de tunnels par défaut dans l'ASA : `DefaultRAGroup`, qui est le groupe de tunnels d'accès à distance IPsec par défaut, et `DefaultL2Lgroup`, qui est le groupe de tunnels IPsec de LAN à LAN par défaut. Vous pouvez les modifier, mais pas les supprimer.

La principale différence entre les versions IKE 1 et 2 réside dans la méthode d'authentification qu'elles autorisent. IKEv1 n'autorise qu'un seul type d'authentification aux deux extrémités du VPN (c'est-à-dire clé prépartagée ou certificat). Cependant, IKEv2 permet la configuration de méthodes d'authentification asymétriques (c'est-à-dire authentification par clé prépartagée pour l'initiateur, mais authentification par certificat pour le répondeur) à l'aide d'interfaces de ligne de commande d'authentification locales et distantes distinctes. Par conséquent, avec IKEv2, vous avez une authentification asymétrique, dans laquelle un côté s'authentifie avec un identifiant et l'autre côté utilise un autre identifiant (une clé prépartagée ou un certificat).

Vous pouvez également créer un ou plusieurs nouveaux groupes de tunnels en fonction de votre environnement. L'ASA utilise ces groupes pour configurer les paramètres de tunnel par défaut pour les groupes de tunnels d'accès à distance et de LAN à LAN lorsqu'aucun groupe de tunnels spécifique n'est identifié lors de la négociation du tunnel.

Pour établir une connexion de base de LAN à LAN, vous devez définir deux attributs pour un groupe de tunnels :

- Définissez le type de connexion sur IPsec de LAN à LAN.
- Configurez une méthode d'authentification pour l'adresse IP (c'est-à-dire une clé prépartagée pour IKEv1 et IKEv2).

Procédure

Étape 1 Pour définir le type de connexion sur IPsec de LAN à LAN, entrez la commande **tunnel-group**.
La syntaxe est **tunnel-group nom type**, où nom est le nom que vous attribuez au groupe de tunnels, et type est le type de tunnel. Les types de tunnels tels que vous les saisissez dans l'interface de ligne de commande sont les suivants :

- **remote-access** (accès à distance IPsec, SSL et SSL sans client)
- **ipsec-l2l** (IPsec de LAN à LAN)

Dans l'exemple suivant, le nom du groupe de tunnels est l'adresse IP de l'homologue de LAN à LAN, 10.10.4.108.

```
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)#
```

Remarque

Les groupes de tunnels de LAN à LAN dont les noms ne sont pas des adresses IP peuvent être utilisés uniquement si la méthode d'authentification du tunnel est Digital Certificates (Certificats numériques) et/ou si l'homologue est configuré pour utiliser le Aggressive Mode (Mode agressif).

Étape 2 Pour définir la méthode d'authentification afin d'utiliser une clé prépartagée, passez en mode ipsec-attributes, puis saisissez la commande **ikev1pre-shared-key** pour créer la clé prépartagée. Vous devez utiliser la même clé prépartagée sur les deux ASA pour cette connexion de LAN à LAN.

La clé est une chaîne alphanumérique de 1 à 128 caractères.

Dans l'exemple suivant, la clé prépartagée IKEv1 est 44kkaol59636jnfx :

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1-pre-shared-key 44kkaol59636jnfx
```

Étape 3 Enregistrez vos modifications.

```
hostname(config)# write memory
hostname(config)#
```

Pour vérifier que le tunnel est opérationnel et en cours d'exécution, utilisez la commande **show vpn-sessiondb summary**, **show vpn-sessiondb detail l2l**, ou **show crypto ipsec sa**.

Créer une carte de chiffrement et l'appliquer à une interface

Les entrées de carte de chiffrement regroupent les différents éléments des associations de sécurité IPsec, notamment les suivants :

- Quel trafic IPsec doit protéger, que vous définissez dans une liste de contrôle d'accès.

- Où envoyer le trafic protégé par IPsec, en identifiant l'homologue.
- La sécurité IPsec qui s'applique à ce trafic, laquelle est précisée par un ensemble de transformation.
- L'adresse locale pour le trafic IPsec, que vous identifiez en appliquant la carte de chiffrement à une interface.

Pour qu'IPsec réussisse, les deux homologues doivent avoir des entrées de carte de chiffrement avec des configurations compatibles. Pour que deux entrées de carte de chiffrement soient compatibles, elles doivent, au minimum, répondre aux critères suivants :

- Les entrées de la carte de chiffrement doivent contenir des listes de contrôle d'accès de chiffrement compatibles (par exemple, listes de contrôle d'accès d'image miroir). Si l'homologue qui répond utilise des cartes de chiffrement dynamiques, les entrées de la liste de contrôle d'accès de chiffrement de l'ASA doivent être « autorisées » par la liste de contrôle d'accès crypto de l'homologue.
- Les entrées de la carte de chiffrement doivent chacune identifier l'autre homologue (sauf si l'homologue répondeur utilise une carte de chiffrement dynamique).
- Les entrées de carte de chiffrement doivent avoir au moins un ensemble de transformation en commun.

Si vous créez plusieurs entrées de carte de chiffrement pour une interface donnée, utilisez le numéro de séquence (seq-num) de chaque entrée pour les classer : plus le numéro de séquence est faible, plus la priorité est élevée. Sur l'interface à laquelle la carte de chiffrement est appliquée, l'ASA évalue d'abord le trafic en fonction des entrées des cartes de priorité plus élevée.

Si l'injection de route inverse (RRI) est appliquée à une carte de chiffrement, cette carte doit être propre à une seule interface de l'ASA. En d'autres termes, la même carte de chiffrement ne peut pas être appliquée à plusieurs interfaces. Si plus d'une carte de chiffrement est appliquée à plusieurs interfaces, les routes risquent de ne pas être supprimées correctement. Si plusieurs interfaces nécessitent une carte de chiffrement, chacune doit utiliser une carte définie de manière unique.

Créez plusieurs entrées de carte de chiffrement pour une interface donnée si l'une des conditions suivantes s'applique :

- Chaque homologue gère différents flux de données.
- Vous souhaitez appliquer une sécurité IPsec différente à différents types de trafic (vers le même ou des homologues distincts), par exemple, si vous souhaitez que le trafic entre un ensemble de sous-réseaux soit authentifié et que le trafic entre un autre ensemble de sous-réseaux soit à la fois authentifié et chiffré. Dans ce cas, définissez les différents types de trafic dans deux listes de contrôle d'accès distinctes et créez une entrée de carte de chiffrement distincte pour chaque liste de contrôle d'accès de chiffrement.

Application d'une carte de chiffrement sur plusieurs interfaces

Dans un environnement à double FSI, vous pouvez appliquer une carte de chiffrement aux interfaces externes et de secours de l'ASA. L'option d'origine uniquement n'est pas disponible lorsque vous utilisez cette configuration. Vous devez utiliser Virtual Tunnel Interface (VTI) si vous avez besoin de cette redondance.

Lorsque vous utilisez une carte de chiffrement sur plusieurs interfaces :

- Vous devez avoir un protocole de routage ou un suivi de route.
- Assurez-vous que le côté distant utilise également des protocoles de routage.
- Vous devez choisir avec soin plusieurs interfaces pour une même carte de chiffrement, car l'ASA permet une connexion provenant d'un site distant sur l'interface dont la route est la moins privilégiée.

Pour créer une carte de chiffrement et l'appliquer à l'interface externe en mode de configuration globale, effectuez les étapes suivantes en mode de contexte unique ou multiple :

Procédure

Étape 1

Pour attribuer une ACL à une entrée de carte de chiffrement, saisissez la commande **crypto map match address**.

La syntaxe est **crypto map** map-name seq-num **match address** aclname. Dans l'exemple suivant, le nom de la carte est abcmmap, le numéro de séquence est 1 et le nom de l'ACL est **121_list**.

```
hostname(config)# crypto map abcmmap 1 match address 121_list  
hostname(config)#
```

Étape 2

Pour identifier le ou les homologues de la connexion IPsec, saisissez la commande **crypto map set peer**.

La syntaxe est **crypto map** map-name seq-num **set peer** {ip_address1 | hostname1} [... ip_address10 | hostname10]. Dans l'exemple suivant, le nom d'homologue est 10.10.4.108.

```
hostname(config)# crypto map abcmmap 1 set peer 10.10.4.108  
hostname(config)#
```

Étape 3

Pour spécifier un ensemble de transformation IKEv1 pour une entrée de carte de chiffrement, saisissez la commande **crypto map ikev1 set transform-set**.

La syntaxe est **crypto map** map-name seq-num **ikev1 set transform-set** transform-set-name. Dans l'exemple suivant, le nom de l'ensemble de transformation est FirstSet.

```
hostname(config)# crypto map abcmmap 1 set transform-set FirstSet  
hostname(config)#
```

Étape 4

Pour préciser une proposition IKEv2 pour une entrée de carte crypto, saisissez la commande **crypto map ikev2 set ipsec-proposal** :

La syntaxe est **crypto map** map-name seq-num **set ikev2 ipsec-proposal proposal-name**. Dans l'exemple suivant, le nom de la proposition est secure.

La commande **crypto map** vous permet de spécifier plusieurs propositions IPsec pour un seul index de carte. Dans ce cas, plusieurs propositions sont transmises à l'homologue IKEv2 dans le cadre de la négociation, et l'ordre des propositions est déterminé par l'administrateur lors de l'ordonnancement de l'entrée de carte de chiffrement.

Remarque

Si des algorithmes en mode combiné (AES-GCM/GMAC) et en mode normal (tous les autres) existent dans la proposition IPsec, vous ne pouvez pas envoyer une seule proposition à l'homologue. Vous devez avoir au moins deux propositions dans ce cas, une pour le mode combiné et une pour les algorithmes en mode normal.

```
hostname(config)# crypto map abcmmap 1 set ikev2 ipsec-proposal secure  
hostname(config)#
```

Appliquer les cartes de chiffrement aux interfaces

Vous devez appliquer un ensemble de cartes de chiffrement à chaque interface par laquelle le trafic IPsec passe. L'ASA prend en charge IPsec sur toutes les interfaces. L'application de l'ensemble de cartes de chiffrement à une interface demande à l'ASA d'évaluer tout le trafic de l'interface par rapport à l'ensemble de cartes de chiffrement et d'utiliser la politique précisée lors des négociations de connexion ou d'association de sécurité.

La liaison d'une carte de chiffrement à une interface initialise également les structures de données d'exécution, telles que la base de données des associations de sécurité et la base de données des politiques de sécurité. Lorsque vous modifiez ultérieurement une carte de chiffrement de quelque manière que ce soit, l'ASA applique automatiquement les modifications à la configuration en cours. Il supprime les connexions existantes et les rétablit après avoir appliqué la nouvelle carte de chiffrement.

Pour appliquer la carte de chiffrement configurée à l'interface externe, procédez comme suit :

Procédure

Étape 1 Entrez la commande **crypto map interface**. La syntaxe est **crypto map** map-name **interface** interface-name.

```
hostname(config)# crypto map abcmap interface outside
hostname(config)#
```

Étape 2 Enregistrez vos modifications.

```
hostname(config)# write memory
hostname(config)#
```



CHAPITRE 9

Connexions du client VPN AnyConnect

Cette section décrit comment configurer les connexions client VPN AnyConnect.

- [À propos du client VPN Secure Client \(services client sécurisés\), à la page 235](#)
- [Exigences de licence pour Secure Client \(services client sécurisés\), à la page 236](#)
- [Configurer les connexions pour Secure Client \(services client sécurisés\), à la page 237](#)
- [SAML 2.0, à la page 256](#)
- [Surveiller les connexions Secure Client \(services client sécurisés\), à la page 267](#)
- [Déconnecter les sessions VPN AnyConnect, à la page 268](#)
- [Historique des fonctionnalités pour les connexions Secure Client \(services client sécurisés\), à la page 269](#)

À propos du client VPN Secure Client (services client sécurisés)

Le Secure Client (services client sécurisés) fournit aux utilisateurs distants des connexions SSL et IPsec/IKEv2 sécurisées vers l'ASA. Sans client déjà installé, les utilisateurs distants saisissent dans leur navigateur l'adresse IP d'une interface configurée pour accepter les connexions VPN SSL ou IPsec/IKEv2. À moins que l'ASA ne soit configuré pour rediriger les requêtes `http://` vers `https://`, les utilisateurs doivent saisir l'URL sous la forme `https://adresse`.

Une fois que l'utilisateur a saisi l'URL, le navigateur se connecte à cette interface et affiche l'écran de connexion. Si l'utilisateur satisfait aux exigences de connexion et d'authentification, et que l'ASA détermine que cet utilisateur a besoin du client, il télécharge le client correspondant au système d'exploitation de l'ordinateur distant. Après le téléchargement, le client s'installe et se configure, établit une connexion sécurisée SSL ou IPsec/IKEv2, puis soit demeure installé, soit se désinstalle, selon la configuration, lorsque la connexion se termine.

Dans le cas d'un client déjà installé, lorsque l'utilisateur s'authentifie, l'ASA vérifie la version du client et le met à niveau au besoin.

Lorsque le client négocie une connexion VPN SSL avec l'ASA, il se connecte en utilisant le protocole Transport Layer Security (TLS) et, éventuellement, Datagram Transport Layer Security (DTLS). L'utilisation de DTLS évite les problèmes de latence et de bande passante associés à certaines connexions SSL et améliore la performance des applications en temps réel sensibles aux retards de paquets.

Le Secure Client (services client sécurisés) peut être téléchargé depuis l'ASA, ou installé manuellement sur le PC distant par l'administrateur système. Pour plus d'informations sur l'installation manuelle du client, consultez la version appropriée du [Guide de configuration de la solution de mobilité sécurisée Cisco AnyConnect](#).

L'ASA télécharge le client en fonction de la stratégie de groupe ou des attributs de nom d'utilisateur de l'utilisateur établissant la connexion. Vous pouvez configurer l'ASA pour télécharger automatiquement le client, ou pour demander à l'utilisateur distant s'il souhaite télécharger le client. Dans ce dernier cas, si l'utilisateur ne répond pas, vous pouvez configurer l'ASA pour télécharger le client après un délai d'expiration ou présenter la page de connexion.

Exigences pour Secure Client (services client sécurisés)

Pour les exigences des ordinateurs terminaux exécutant Secure Client (services client sécurisés), consultez la version appropriée des [notes de version de solution de mobilité sécurisée Cisco AnyConnect](#).

Lignes directrices et limites pour Secure Client (services client sécurisés)

- L'ASA ne vérifie pas les certificats HTTPS distants.
- Pris en charge en mode contexte unique ou multiple. Une licence AnyConnect Apex est requise pour le VPN d'accès à distance en mode multi-contexte. Bien que l'ASA ne reconnaisse pas expressément une licence AnyConnect Apex, il applique les caractéristiques d'une licence Apex, comme AnyConnect Premium sous licence jusqu'à la limite de la plateforme, Secure Client (services client sécurisés) pour les périphériques mobiles, Secure Client (services client sécurisés) pour le téléphone VPN Cisco et pour l'évaluation avancée des postes clients. Les licences partagées, AnyConnect Essentials, l'agrégation de licences de basculement et les licences flex ou à durée déterminée ne sont pas prises en charge.
- L'émission de commandes telles que **curl** sur la tête de réseau du VPN d'accès à distance n'est pas directement prise en charge et pourrait ne pas donner les résultats souhaitables. Par exemple, la tête de réseau ne répond pas aux requêtes HTTP HEAD.
- Lorsque des téléphones VPN matériels, comme ceux de la série Cisco 88xx, utilisent Secure Client (services client sécurisés), ils peuvent subir une reconnexion malgré l'activation de DTLS et la configuration de Dead Peer Detection (DPD).
- Lorsqu'un client se connecte à Secure Client (services client sécurisés), son adresse IP change avant et après la connexion. L'ASA prend en charge ce comportement.

Exigences de licence pour Secure Client (services client sécurisés)



Remarque Cette fonctionnalité n'est pas disponible sur les modèles sans chiffrement de charge utile.

Les licences VPN d'accès à distance nécessitent une licence AnyConnect Plus ou Apex, disponible séparément. Consultez [les licences pour fonctionnalités de la gamme Cisco ASA](#) pour connaître les valeurs maximales par modèle.

Si vous démarrez une session SSL VPN sans client, puis démarrez la session Secure Client (services client sécurisés) à partir du portail, une session est utilisée au total. Cependant, si vous démarrez d'abord le Secure Client (services client sécurisés) (à partir d'un client autonome, par exemple), puis que vous vous connectez au portail SSL VPN sans client, deux sessions sont utilisées.

Configurer les connexions pour Secure Client (services client sécurisés)

Cette section décrit les conditions préalables, les restrictions et les tâches détaillées pour configurer l'ASA afin qu'il accepte les connexions des clients VPN AnyConnect.

Configurer l'ASA pour déployer le client via le Web

Cette section décrit les étapes permettant de configurer l'ASA pour le déploiement Web de Secure Client (services client sécurisés).

Avant de commencer

Copiez le paquet d'image client dans l'ASA à l'aide de TFTP ou d'une autre méthode.



Remarque

Même si la fonctionnalité VPN sans client est désactivée sur l'ASA, lorsque vous utilisez un navigateur Web pour accéder au déploiement Web d'AnyConnect (<https://x.x.x.x<ASA IP address>>), la session VPN sur l'ASA est comptabilisée comme une session sans client.

Procédure

Étape 1

Identifiez un fichier sur la mémoire flash comme le fichier de paquet Secure Client (services client sécurisés).

L'ASA décompresse le fichier dans la mémoire cache pour le télécharger sur des PC distants. Si vous avez plusieurs clients, attribuez un ordre aux images client avec l'argument d'ordre.

L'ASA télécharge des parties de chaque client dans l'ordre que vous spécifiez jusqu'à ce qu'il corresponde au système d'exploitation du PC distant. Par conséquent, attribuez le numéro le plus bas à l'image utilisée par le système d'exploitation le plus souvent rencontré.

anyconnect image *filename order*

Exemple :

```
hostname(config-webvpn)# anyconnect image
anyconnect-win-2.3.0254-k9.pkg 1
hostname(config-webvpn)# anyconnect image
anyconnect-macosx-i386-2.3.0254-k9.pkg 2
hostname(config-webvpn)# anyconnect image
anyconnect-linux-2.3.0254-k9.pkg 3
```

Remarque

Vous devez émettre la commande **AnyConnect enable** après avoir configuré les images Secure Client (services client sécurisés) avec la commande **AnyConnect image**. Si vous n'activez pas Secure Client (services client sécurisés), il ne fonctionnera pas comme prévu, et la commande **show webvpn anyconnect** considérera le client VPN SSL comme non activé au lieu de répertorier les paquets Secure Client (services client sécurisés) installés.

- Étape 2** Activez SSL sur une interface pour les connexions sans client ou Secure Client (services client sécurisés) SSL.
- enable interface**
- Exemple :**
- ```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```
- Étape 3** Sans l'exécution de cette commande, Secure Client (services client sécurisés) ne fonctionne pas comme prévu, et une commande **show webvpn anyconnect** renvoie que « le VPN SSL n'est pas activé » au lieu de répertorier les paquets Secure Client (services client sécurisés) installés.
- anyconnect enable**
- Étape 4** (Facultatif) Créez un ensemble d'adresses IP. Vous pouvez utiliser une autre méthode d'affectation d'adresses, telle que DHCP et/ou l'adressage attribué par l'utilisateur.
- ip local pool poolname startaddr-endaddr mask mask**
- Exemple :**
- ```
hostname(config)# ip local pool vpn_users 209.165.200.225-209.165.200.254
mask 255.255.255.224
```
- Étape 5** Attribuez un ensemble d'adresses à un groupe de tunnels.
- address-pool poolname**
- Exemple :**
- ```
hostname(config)# tunnel-group telecommuters general-attributes
hostname(config-tunnel-general)# address-pool vpn_users
```
- Étape 6** Attribuez une stratégie de groupe par défaut au groupe de tunnels.
- default-group-policy name**
- ```
hostname(config-tunnel-general)# default-group-policy sales
```
- Étape 7** Activez l'affichage de la liste des groupes de tunnels sur le portail sans client et la page de connexion de l'interface graphique Secure Client (services client sécurisés). La liste des alias est définie par la commande **group-alias name enable**.
- group-alias name enable**
- Exemple :**
- ```
hostname(config)# tunnel-group telecommuters webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias sales_department enable
```
- Étape 8** Précisez Secure Client (services client sécurisés) comme protocole de tunnelisation VPN autorisé pour le groupe ou l'utilisateur.
- tunnel-group-list enable**
- Exemple :**

```
hostname(config)# webvpn
hostname(config-webvpn)# tunnel-group-list enable
```

### Étape 9

Précisez SSL comme protocole de tunnelisation VPN autorisé pour le groupe ou l'utilisateur. Vous pouvez également spécifier des protocoles supplémentaires. Pour de plus amples informations, consultez la commande `vpn-tunnel-protocol` dans la référence de commande.

#### vpn-tunnel-protocol

##### Exemple :

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# vpn-tunnel-protocol
```

### Prochaine étape

Pour en savoir plus sur l'affectation d'utilisateurs aux stratégies de groupe, consultez le chapitre 6, Configuration des profils de connexion, des stratégies de groupe et des utilisateurs.

## Activer l'installation permanente du client

L'activation de l'installation permanente du client désactive la fonction de désinstallation automatique du client. Le client reste installé sur l'ordinateur distant pour les connexions ultérieures, ce qui réduit le temps de connexion pour l'utilisateur distant.

Pour activer l'installation permanente du client pour un groupe ou un utilisateur spécifique, utilisez la commande `anyconnect keep-install` à partir des modes de stratégie de groupe ou de nom d'utilisateur `webvpn`.

La valeur par défaut est que l'installation permanente du client est activée. Le client reste sur l'ordinateur distant à la fin de la session. L'exemple suivant configure la stratégie de groupe existante `sales` pour supprimer le client sur l'ordinateur distant à la fin de la session :

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# anyconnect keep-installer installed none
```

## Configurer DTLS

Datagram Transport Layer Security (DTLS) permet à Secure Client (services client sécurisés) d'établir une connexion VPN SSL pour utiliser deux tunnels simultanés : un tunnel SSL et un tunnel DTLS. L'utilisation de DTLS évite les problèmes de latence et de bande passante associés aux connexions SSL et améliore la performance des applications en temps réel sensibles aux retards de paquets.

### Avant de commencer

Consultez [Configurer les paramètres avancés SSL, à la page 89](#) pour configurer DTLS sur cette tête de réseau et quelle version de DTLS est utilisée.

Pour que DTLS passe à une connexion TLS, la détection d'homologue mort (DPD) doit être activée. Si vous n'activez pas DPD et que la connexion DTLS rencontre un problème, la connexion se termine au lieu de revenir à TLS. Pour en savoir plus sur DPD, consultez [Configurer, à la page 251](#).

## Procédure

**Étape 1** Précisez les options DTLS pour les connexions VPN Secure Client (services client sécurisés) :

- a) Activez SSL et DTLS sur l'interface en mode webvpn.

Par défaut, DTLS est activé lorsque l'accès VPN SSL est activé sur une interface.

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

Désactivez DTLS pour tous les utilisateurs Secure Client (services client sécurisés) avec la commande **enable interface tls-only** en mode de configuration webvpn.

Si vous désactivez DTLS, les connexions VPN SSL se connectent uniquement à l'aide d'un tunnel SSL.

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside tls-only
```

- b) Configurez les ports pour SSL et DTLS à l'aide des commandes **port** et **dtls port**.

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
hostname(config-webvpn)# port 555
hostname(config-webvpn)# dtls port 556
```

**Étape 2** Précisez les options DTLS pour des stratégies de groupe spécifiques.

- a) Activez DTLS pour des groupes ou des utilisateurs spécifiques avec la commande **anyconnect ssl dtls** en mode de configuration de stratégie de groupe webvpn ou de nom d'utilisateur webvpn.

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl dtls enable
```

- b) Si vous le souhaitez, activez la compression DTLS à l'aide de la commande AnyConnect dtls compression.

```
hostname(config-group-webvpn)# anyconnect dtls compression lz
```

## Inviter les utilisateurs distants

### Procédure

Vous pouvez activer l'ASA afin qu'il invite les utilisateurs distants du client VPN SSL à télécharger le client à l'aide de la commande **anyconnect ask** depuis les modes de configuration webvpn de stratégie de groupe ou de nom d'utilisateur :

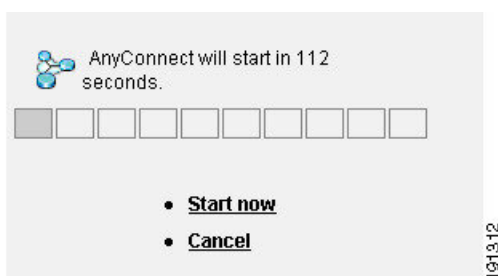
```
[no] anyconnect ask {none | enable [default {webvpn | } timeout value]}
```



- **anyconnect enable** invite l'utilisateur distant à télécharger le client ou à accéder à la page du portail sans client et attend indéfiniment la réponse de l'utilisateur.
- **anyconnect ask enable default** télécharge immédiatement le client.
- **anyconnect ask enable default webvpn** passe immédiatement à la page du portail.
- La valeur **anyconnect ask enable default timeout** invite l'utilisateur distant à télécharger le client ou à accéder à la page du portail sans client et attend la durée de *value (valeur)* avant d'entreprendre l'action par défaut : télécharger le client.
- La valeur **anyconnect ask enable default clientless timeout** invite l'utilisateur distant à télécharger le client ou à accéder à la page du portail sans client et attend la durée de *value (valeur)* avant d'entreprendre l'action par défaut : afficher la page du portail sans client.

La figure ci-dessous montre l'invite affichée aux utilisateurs distants lorsque la valeur **default anyconnect timeout** ou la valeur **default webvpn timeout** est configurée :

**Illustration 6 : Invite affichée pour les utilisateurs distants pour le téléchargement du client VPN SSL**



### Exemple

L'exemple suivant configure l'ASA pour inviter l'utilisateur à télécharger le client ou à se rendre à la page du portail sans client et à attendre *10 secondes pour obtenir une réponse* avant de télécharger le client :

```
hostname(config-group-webvpn)# anyconnect ask enable default anyconnect timeout
10
```

## Activer le téléchargement du profil Secure Client (services client sécurisés)

Vous activez les fonctionnalités Secure Client (services client sécurisés) dans les profils Secure Client (services client sécurisés), fichiers XML qui contiennent les paramètres de configuration pour le client principal avec sa fonctionnalité VPN et pour les modules clients facultatifs. L'ASA déploie les profils pendant l'installation et les mises à jour de Secure Client (services client sécurisés). Les utilisateurs ne peuvent pas gérer ou modifier les profils.

Le fichier téléchargé sur le client est du format : *<profile\_name>.xml*.

Vous pouvez configurer un profil à l'aide de l'éditeur de profils Secure Client (services client sécurisés), un outil de configuration graphique pratique lancé par ASDM ou ISE. Le paquet de logiciels Secure Client (services client sécurisés) pour Windows comprend l'éditeur, qui s'active lorsque vous chargez le paquet

client sur le périphérique headend choisi et que vous le spécifiez comme image Secure Client (services client sécurisés).

Nous fournissons également une version autonome de l'éditeur de profils pour Windows que vous pouvez utiliser comme solution de rechange à l'éditeur de profils intégré à ASDM ou ISE. Si vous prédéployez le client, vous pouvez utiliser l'éditeur de profil autonome pour créer des profils pour le service VPN et d'autres modules que vous déployez sur les ordinateurs à l'aide de votre système de gestion de logiciels.

Pour en savoir plus sur Secure Client (services client sécurisés) et son éditeur de profils, consultez la version appropriée du [Guide de configuration de la solution de mobilité sécurisée Cisco AnyConnect](#).



#### Remarque

Le protocole Secure Client (services client sécurisés) est SSL par défaut. Pour activer IPsec IKEv2, vous devez configurer les paramètres IKEv2 sur l'ASA et configurer IKEv2 comme protocole principal dans le profil client. Le profil compatible IKEv2 doit être déployé sur l'ordinateur terminal ; sinon, le client tente de se connecter à l'aide de SSL.

### Procédure

- Étape 1** Utilisez l'éditeur de profil d'ASDM/ISE ou l'éditeur de profil autonome pour créer un profil.
- Étape 2** Chargez le fichier de profil dans la mémoire flash sur l'ASA à l'aide de tftp ou toute autre méthode.
- Étape 3** Utilisez la commande **anyconnect profiles** à partir du mode de configuration webvpn pour identifier le fichier en tant que profil client à charger dans la mémoire cache.

#### Exemple :

L'exemple suivant spécifie les fichiers sales\_hosts.xml et engineering\_hosts.xml en tant que profils :

```
asa1(config-webvpn)# anyconnect profiles sales
disk0:/sales_hosts.xml
asa1(config-webvpn)# anyconnect profiles engineering
disk0:/engineering_hosts.xml
```

Les profils sont maintenant disponibles pour les stratégies de groupe.

Affichez les profils chargés dans la mémoire cache à l'aide de la commande **dir cache:stc/profiles** :

```
hostname(config-webvpn)# dir cache:/stc/profiles

Directory of cache:stc/profiles/

0 ---- 774 11:54:41 Nov 22 2006 engineering.xml
0 ---- 774 11:54:29 Nov 22 2006 sales.xml

2428928 bytes total (18219008 bytes free)
hostname(config-webvpn)#
```

- Étape 4** Entrez le mode de configuration webvpn de la stratégie de groupe et spécifiez un profil client pour une stratégie de groupe avec la commande **anyconnect profiles** :

#### Exemple :

Vous pouvez saisir la commande `client profiles value` suivie d'un point d'interrogation (?) pour afficher les profils disponibles. Par exemple :

```
asa1(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages: engineering sales
```

L'exemple suivant configure la stratégie de groupe pour utiliser le profil `sales` avec le type de profil client `vpn` :

```
asa1(config-group-webvpn)# anyconnect profiles value sales type vpn
asa1(config-group-webvpn)#
```

## Activer la mise à niveau différée Secure Client (services client sécurisés)

La mise à niveau différée permet à l'utilisateur Secure Client (services client sécurisés) de retarder le téléchargement de la mise à niveau du client. Lorsqu'une mise à jour de client est disponible, Secure Client (services client sécurisés) ouvre une boîte de dialogue demandant à l'utilisateur s'il souhaite effectuer la mise à jour ou reporter la mise à niveau. Cette boîte de dialogue de mise à niveau ne s'affichera pas, sauf si AutoUpdate est défini sur *Enabled* (Activé) dans le paramètre de profil Secure Client (services client sécurisés).

La mise à niveau différée est activée en ajoutant des types d'attributs personnalisés et des valeurs nommées à l'ASA ; ensuite, référencez et configurez ces attributs dans une stratégie de groupe.

Les attributs personnalisés suivants prennent en charge la mise à niveau différée :

**Tableau 13 : Attributs personnalisés pour la mise à niveau différée**

| Type d'attribut personnalisé | Valeurs valides : | Valeur par défaut | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------|-------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DeferredUpdateAllowed        | true false        | faux              | La valeur true active la mise à jour différée. Si la mise à jour différée est désactivée (false), les paramètres ci-dessous sont ignorés.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| DeferredUpdateMinimumVersion | x.y.z             | 0.0.0             | Version minimale de Secure Client (services client sécurisés) à installer pour que les mises à jour soient reportables.<br><br>La vérification de version minimale s'applique à tous les modules activés sur la tête de réseau. Si un module activé (y compris le VPN) n'est pas installé ou ne répond pas à la version minimale, la connexion n'est pas admissible pour une mise à jour retardée.<br><br>Si cet attribut n'est pas spécifié, une invite de report s'affiche (ou est rejetée automatiquement), quelle que soit la version installée sur le terminal. |

| Type d'attribut personnalisé  | Valeurs valides :    | Valeur par défaut           | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------|----------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DeferredUpdateDismissTimeout  | 0-300 (secondes)     | none (Aucun)<br>(désactivé) | <p>Nombre de secondes pendant lesquelles l'invite de mise à niveau retardée s'affiche avant d'être rejetée automatiquement. Cet attribut s'applique uniquement lorsqu'une invite de mise à jour retardée doit s'afficher (l'attribut de version minimale est évalué en premier).</p> <p>Si cet attribut est manquant, la fonctionnalité de suppression automatique est désactivée et une boîte de dialogue s'affiche (le cas échéant) jusqu'à ce que l'utilisateur réponde.</p> <p>La définition de cet attribut à zéro permet de forcer le report ou la mise à niveau automatique en fonction des éléments suivants :</p> <ul style="list-style-type: none"> <li>• La version installée et la valeur de DeferredUpdateMinimumVersion.</li> <li>• La valeur de DeferredUpdateDismissResponse.</li> </ul> |
| DeferredUpdateDismissResponse | mise à jour reportée | mettre à jour               | Action à effectuer lorsque DeferredUpdateDismissTimeout se produit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Procédure

**Étape 1** Créez les types d'attributs personnalisés avec la commande **anyconnect-custom-attr** en mode de configuration webvpn :

```
[no] AnyConnect-custom-attr attr-type [description description]
```

**Exemple :**

L'exemple suivant montre comment ajouter les types d'attributs personnalisés DeferredUpdateAllowed et DeferredUpdateDismissTimeout :

```
hostame(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed
description Indicates if the deferred update feature is enabled or not
hostame(config-webvpn)# anyconnect-custom-attr DeferredUpdateDismissTimeout
```

**Étape 2** Ajoutez des valeurs nommées pour les attributs personnalisés avec la commande **anyconnect-custom-data** en mode de configuration globale. Pour les attributs avec des valeurs longues, vous pouvez fournir une entrée en double qui permet la concaténation. Cependant, avec une entrée de configuration en double, la boîte de dialogue de mise à niveau ne s'affiche pas, et un utilisateur ne peut pas reporter la mise à niveau ; au lieu de cela, la mise à niveau se produit automatiquement.

```
[no] AnyConnect-custom-data attr-type attr-name attr-value
```

**Exemple :**

L'exemple suivant montre comment ajouter une valeur nommée pour le type d'attribut personnalisé `DeferredUpdateDismissTimeout` et pour l'activation de `DeferredUpdateAllowed` :

```
hostname(config)# anyconnect-custom-data DeferredUpdateDismissTimeout
def-timeout 150
hostname(config)# anyconnect-custom-data DeferredUpdateAllowed
def-allowed true
```

### Étape 3

Ajoutez ou supprimez les valeurs nommées d'attribut personnalisé à une stratégie de groupe à l'aide de la commande **anyconnect-custom** :

- **anyconnect-custom attr-type value attr-name**
- **anyconnect-custom attr-type none**
- **no anyconnect-custom attr-type**

#### Exemple :

L'exemple suivant montre comment activer la mise à jour retardée pour la stratégie de groupe nommée `sales` et définir le délai d'expiration à 150 secondes :

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# anyconnect-custom DeferredUpdateAllowed
value def-allowed
hostname(config-group-policy)# anyconnect-custom DeferredUpdateDismissTimeout
value def-timeout
```

## Activer la conservation DSCP

En définissant un autre attribut personnalisé, vous pouvez contrôler le point de code de services différenciés (DSCP) sur les plateformes Windows ou OS X pour les connexions DTLS uniquement. L'activation de la conservation DSCP permet aux périphériques de hiérarchiser le trafic sensible à la latence ; le routeur tient compte de ce paramètre et marque le trafic prioritaire afin d'améliorer la qualité de la connexion sortante.

### Procédure

#### Étape 1

Créez les types d'attributs personnalisés avec la commande **anyconnect-custom-attr** en mode de configuration `webvpn` :

**[no] anyconnect-custom-attr DSCPPreservationAllowed description Définir le contrôle du point de code de services différenciés (DSCP) sur les plateformes Windows ou OS X pour les connexions DTLS uniquement.**

#### Étape 2

Ajoutez des valeurs nommées pour les attributs personnalisés avec la commande **anyconnect-custom-data** en mode de configuration globale :

**[no] anyconnect-custom-data DSCPPreservationAllowed true**

#### Remarque

Par défaut, Secure Client (services client sécurisés) effectue la conservation DSCP (true). Pour le désactiver, définissez l'attribut personnalisé sur false au niveau de la tête de réseau, puis relancez la connexion.

## Activer les fonctionnalités Secure Client (services client sécurisés) supplémentaires

Pour minimiser le temps de téléchargement, le client ne demande les téléchargements (à partir de l'ASA ou de l'ISE) que des modules principaux dont il a besoin. À mesure que des fonctionnalités supplémentaires deviennent disponibles pour le Secure Client (services client sécurisés), vous devez mettre à jour les clients distants pour qu'ils utilisent les fonctionnalités.

Pour activer de nouvelles fonctionnalités, vous devez spécifier les nouveaux noms de module à l'aide de la commande **anyconnect modules** à partir du mode de configuration de la stratégie de groupe webvpn ou du nom d'utilisateur webvpn :

**[no]anyconnect modules {none | value string}**

Séparez plusieurs chaînes par des virgules.

## Activer le démarrage avant la connexion

Le démarrage avant la connexion (SBL) permet l'exécution de scripts d'ouverture de session, la mise en cache des mots de passe, le mappage des lecteurs, et plus encore, pour le Secure Client (services client sécurisés) installé sur un PC Windows. Pour SBL, vous devez activer l'ASA afin qu'il télécharge le module qui permet l'identification et l'authentification graphiques (GINA) pour le Secure Client (services client sécurisés). La procédure suivante montre comment activer SBL :

### Procédure

**Étape 1** Activez l'ASA afin qu'il télécharge le module GINA pour la connexion VPN vers des groupes ou des utilisateurs précis au moyen de la commande **anyconnect modules vpngina** à partir des modes de configuration webvpn de la stratégie de groupe ou du nom d'utilisateur.

#### Exemple :

Dans l'exemple suivant, l'utilisateur entre dans le mode d'attributs de stratégie de groupe pour la stratégie de groupe *telecommuters*, entre dans le mode de configuration webvpn pour cette stratégie de groupe et précise la chaîne *vpngina* :

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#anyconnect modules value vpngina
```

**Étape 2** Récupérez une copie du fichier de profils clients (AnyConnectProfile.tmpl).

**Étape 3** Modifiez le fichier de profils pour préciser que SBL est activé. L'exemple ci-dessous montre la partie pertinente du fichier de profils (AnyConnectProfile.tmpl) pour Windows :

```
<Configuration>
 <ClientInitialization>
 <UseStartBeforeLogon>false</UseStartBeforeLogon>
```

```
</ClientInitialization>
```

La balise <UseStartBeforeLogon> détermine si le client utilise SBL. Pour activer SBL, remplacez *false* par *true*. L'exemple ci-dessous montre la balise avec SBL activé :

```
<ClientInitialization>
 <UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
```

#### Étape 4

Enregistrez les modifications apportées à AnyConnectProfile.tmpl et mettez à jour le fichier de profil du groupe ou de l'utilisateur sur l'ASA au moyen de la commande **profile** du mode de configuration webvpn. Par exemple :

```
asal(config-webvpn)#anyconnect profiles sales disk0:/sales_hosts.xml
```

## Traduction des langues pour les messages utilisateur Secure Client (services client sécurisés)

L'ASA fournit la traduction linguistique du portail et des écrans affichés aux utilisateurs qui amorcent des connexions VPN SSL sans client basées sur un navigateur, ainsi que l'interface affichée pour les utilisateurs du client VPN Cisco AnyConnect.

Cette section décrit comment configurer l'ASA pour traduire ces messages utilisateur.

### Comprendre la traduction linguistique

Les zones fonctionnelles et leurs messages visibles pour les utilisateurs distants sont organisés en domaines de traduction. Tous les messages affichés dans l'interface utilisateur de Cisco AnyConnect VPN Client se trouvent dans le domaine Secure Client (services client sécurisés).

Le progiciel pour l'ASA comprend un modèle de table de traduction pour le domaine Secure Client (services client sécurisés). Vous pouvez exporter le modèle, ce qui crée un fichier XML du modèle à l'URL que vous indiquez. Les champs de message de ce fichier sont vides. Vous pouvez modifier les messages et importer le modèle pour créer un nouvel objet de table de traduction qui réside dans la mémoire flash.

Vous pouvez également exporter une table de traduction existante. Le fichier XML créé affiche les messages que vous avez précédemment modifiés. La réimportation de ce fichier XML avec le même nom de langue crée une nouvelle version de l'objet de table de traduction, qui remplace les messages précédents. Les modifications apportées à la table de traduction du domaine Secure Client (services client sécurisés) sont immédiatement visibles par les utilisateurs Secure Client (services client sécurisés).

### Création de tableaux de traduction

La procédure suivante décrit comment créer des tables de traduction pour le domaine Secure Client (services client sécurisés) :

## Procédure

### Étape 1

Exportez un modèle de tableau de traduction vers un ordinateur avec la commande **export webvpn translation-table** à partir du mode d'exécution privilégié.

Dans l'exemple suivant, la commande **show import webvpn translation-table** affiche les modèles de tableau de traduction et les tableaux disponibles.

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect

PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
```

L'utilisateur exporte ensuite la table de traduction pour le domaine de traduction Secure Client (services client sécurisés). Le nom de fichier du fichier XML créé est nommé *client* et contient des champs de message vides :

```
hostname# export webvpn translation-table AnyConnect
template tftp://209.165.200.225/client
```

Dans l'exemple suivant, l'utilisateur exporte une table de traduction nommée *zh*, qui a été précédemment importée d'un modèle. *zh* est l'abréviation par Microsoft Internet Explorer pour la langue chinoise.

```
hostname# export webvpn translation-table customization
language zh tftp://209.165.200.225/chinese_client
```

### Étape 2

Modifier le fichier XML du tableau de traduction. L'exemple suivant montre une partie du modèle Secure Client (services client sécurisés). La fin de cette sortie comprend un champ d'ID de message (msgid) et un champ de chaîne de message (msgstr) pour le message *Connected*, qui s'affiche dans l'interface graphique Secure Client (services client sécurisés) lorsque le client établit une connexion VPN. Le modèle complet contient plusieurs paires de champs de message :

```
SOME DESCRIPTIVE TITLE.
Copyright (C) YEAR THE PACKAGE'S COPYRIGHT HOLDER
This file is distributed under the same license as the PACKAGE package.
FIRST AUTHOR <EMAIL@ADDRESS>, YEAR.
#
#, fuzzy
msgid ""
msgstr ""
"Project-Id-Version: PACKAGE VERSION\n"
"Report-Msgid-Bugs-To: \n"
"POT-Creation-Date: 2006-11-01 16:39-0700\n"
"PO-Revision-Date: YEAR-MO-DA HO:MI+ZONE\n"
```



```
"Last-Translator: FULL NAME <EMAIL@ADDRESS>\n"
"Language-Team: LANGUAGE <LL@li.org>\n"
"MIME-Version: 1.0\n"
"Content-Type: text/plain; charset=CHARSET\n"
"Content-Transfer-Encoding: 8bit\n"

#: C:\cygwin\home\<user>\cvc\main\Api\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\check\AgentIfc.cpp:22
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp~:20
#: C:\cygwin\home\<user>\cvc\main\Api\save\older\AgentIfc.cpp:22
msgid "Connected"
msgstr ""
```

Le msgid contient la traduction par défaut. Le msgstr qui suit msgid fournit la traduction. Pour créer une traduction, saisissez le texte traduit entre les guillemets de la chaîne msgstr. Par exemple, pour traduire le message « Connected » par une traduction en Espagnol, insérez le texte en Espagnol entre les guillemets :

```
msgid "Connected"
msgstr "Conectado"
```

Assurez-vous de sauvegarder le fichier.

### Étape 3

Importez la table de traduction à l'aide de la commande **import webvpn translation-table** à partir du mode d'exécution privilégié. Assurez-vous de préciser le nom de la nouvelle table de traduction avec l'abréviation de la langue compatible avec le navigateur.

Dans l'exemple suivant, le fichier XML est importé *es-us*, l'abréviation utilisée par Microsoft Internet Explorer pour l'Espagnol Parlé aux États-Unis.

```
hostname# import webvpn translation-table AnyConnect
language es-us tftp://209.165.200.225/client
hostname#
hostname# show import webvpn translation-table
Translation Tables' Templates:
AnyConnect
PortForwarder

customization
keepout
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
es-us AnyConnect
```

## Supprimer les tableaux de traduction

Si vous n'avez plus besoin d'un tableau de traduction, vous pouvez le supprimer.

## Procédure

### Étape 1 Répertoriez les tableaux de traduction existants.

Dans l'exemple suivant, la commande **show import webvpn translation-table** affiche les modèles de tableau de traduction et les tableaux disponibles. Plusieurs tableaux sont disponibles pour le français (fr), le japonais (ja) et le russe (ru).

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
 AnyConnect
 PortForwarder
 banners
 csd
 customization
 url-list
 webvpn
Translation Tables:
fr PortForwarder
fr AnyConnect
fr customization
fr webvpn
ja PortForwarder
ja AnyConnect
ja customization
ja webvpn
ru PortForwarder
ru customization
ru webvpn
```

### Étape 2 Supprimez le tableau de traduction indésirable.

**revert webvpn translation-table *translationdomain* language *language***

Où *translationdomain* correspond au domaine indiqué à droite dans la liste des tableaux de traduction ci-dessus, et *language* est le nom de langue à 2 caractères.

Vous devez supprimer chaque tableau individuellement. Vous ne pouvez pas supprimer tous les tableaux d'une langue donnée avec une seule commande.

Par exemple, pour supprimer le tableau de traduction française pour Secure Client (services client sécurisés):

```
ciscoasa# revert webvpn translation-table anyconnect language fr
ciscoasa#
```

## Configuration des fonctionnalités SSL avancées Secure Client (services client sécurisés)

La section suivante décrit les fonctionnalités avancées qui affinent les connexions VPN SSL Secure Client (services client sécurisés) :

## Activer le renouvellement

Lorsque l'ASA et le Secure Client (services client sécurisés) effectuent un renouvellement sur une connexion VPN SSL, ils renégocient les clés de chiffrement et les vecteurs d'initialisation, augmentant ainsi la sécurité de la connexion.

Pour permettre au client d'effectuer un renouvellement sur une connexion VPN SSL pour un groupe ou un utilisateur spécifique, utilisez la commande **AnyConnect ssl rekey** à partir des modes de stratégie de groupe ou de nom d'utilisateur webvpn.

```
[no]AnyConnect ssl rekey {method {new-tunnel | none | ssl} | time minutes}
```

- **method new-tunnel** spécifie que le client établit un nouveau tunnel pendant le renouvellement.
- **method ssl** spécifie que le client établit un nouveau tunnel pendant le renouvellement.
- **method none** désactive le renouvellement.
- **time minutes** spécifie le nombre de minutes à partir du début de la session ou du dernier renouvellement, jusqu'à ce que le renouvellement ait lieu, de 1 à 10080 (1 semaine).



### Remarque

La configuration de la méthode de renouvellement comme **ssl** ou **new-tunnel** spécifie que le client établit un nouveau tunnel pendant le renouvellement au lieu que la renégociation SSL ait lieu pendant le renouvellement. Consultez la référence de commande pour obtenir l'historique de la commande **AnyConnect ssl rekey**.

Dans l'exemple suivant, le client est configuré pour renégocier avec SSL pendant le renouvellement, qui a lieu 30 minutes après le début de la session, pour la stratégie de groupe existante *sales* :

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl rekey method ssl
hostname(config-group-webvpn)# anyconnect ssl rekey time 30
```

## Configurer

La détection d'homologue mort (DPD) garantit que la passerelle ASA ou le client peut rapidement détecter une condition où l'homologue ne répond pas et que la connexion a échoué. Pour activer la détection d'homologue mort (DPD) et définir la fréquence à laquelle le Secure Client (services client sécurisés) ou la passerelle ASA exécute le DPD.



### Remarque

Lorsque la connexion est interrompue du côté client, l'ASA n'abandonne pas la session Secure Client (services client sécurisés) en raison de DPD ou de keepalive sans condition. DPD n'est déclenché par l'ASA que lorsqu'il y a un flux de données entre l'ASA et le client. Une fois que DPD est déclenché, il effectue trois tentatives pour chaque session enfant (SSL/DTLS) avant de les supprimer.

S'il n'y a pas de flux de données, le DPD n'est pas déclenché. L'ASA dispose d'un délai d'inactivité TCP codé en dur de 5 minutes qui ferme automatiquement les connexions de tunnel SSL/DTLS lorsqu'aucune donnée ni aucun paquet Keepalive ne circule pendant exactement 5 minutes, quel que soit le paramètre configuré de délai d'inactivité du VPN. Après la suppression des sessions enfants, la commande **vpn-idle-timeout** est uniquement responsable du contrôle de la durée maximale d'une session parente. Pour plus de détails sur les attributs DPD, keepalive et de temporisation, consultez la [FAQ AnyConnect – Tunnels, DPD et minuterie d'inactivité](#).

### Avant de commencer

- Cette fonctionnalité s'applique uniquement à la connectivité entre la passerelle ASA et le client SSL VPN Secure Client (services client sécurisés). Il ne fonctionne pas avec IPsec, car DPD est basé sur l'implémentation des normes qui ne permet pas le remplissage.
- Si vous activez DTLS, activez également la détection d'homologue mort (DPD). DPD permet à une connexion DTLS défaillante de revenir à TLS. Dans le cas contraire, la connexion se termine.
- Lorsque DPD est activé sur l'ASA, vous pouvez utiliser la fonction de MTU optimale (OMTU) pour trouver la plus grande MTU de point terminal à laquelle le client peut transmettre avec succès les paquets DTLS. Mettez en œuvre OMTU en envoyant un paquet DPD rempli jusqu'à la MTU maximale. Si un écho correct de la charge utile est reçu de la tête de réseau, la taille de la MTU est acceptée. Sinon, la MTU est réduite et la sonde est de nouveau envoyée jusqu'à ce que la MTU minimale autorisée pour le protocole soit atteinte.

### Procédure

#### Étape 1

Accédez à la stratégie de groupe souhaitée.

Entrez le mode de stratégie de groupe ou de nom d'utilisateur webvpn :

```
hostname(config)# group-policy group-policy-name attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)#
```

Ou

```
hostname# username username attributes
hostname(config-username)# webvpn
hostname (config-username-webvpn) #
```

#### Étape 2

Définir la détection côté passerelle.

Utilisez la commande **[no] anyconnect dpd-interval** {[gateway {secondes | none}}] .

La passerelle fait référence à l'ASA. Vous activez DPD et spécifiez l'intervalle auquel l'ASA attend tout paquet du client sur une plage comprise entre 30 (par défaut) et 3 600 secondes (1 heure). Une valeur de 300 est conseillée. Si aucun paquet n'est reçu dans cet intervalle, l'ASA effectue le test DPD avec trois tentatives au même intervalle. Si l'ASA ne reçoit pas de réponse du client, il interrompt le tunnel TLS/DTLS.

#### Remarque

La spécification **none** désactive les tests DPD effectués par l'ASA. Utilisez **no AnyConnect dpd-interval** pour supprimer cette commande de la configuration.

La spécification de **none** désactive le test DPD effectué par l'ASA. Utilisez la commande **no anyconnect dpd-interval** pour supprimer cette commande de la configuration.

#### Étape 3

Définir la détection côté client.

Utilisez la commande **[no] anyconnect dpd-interval** {[client {seconds | none}}] .

Le client fait référence à Secure Client (services client sécurisés). Vous activez DPD et spécifiez la fréquence à laquelle le client effectue le test DPD sur une plage de 30 (par défaut) à 3 600 secondes (1 heure). Une valeur de 30 secondes est conseillée.

La spécification de **client none** désactive le DPD effectué par le client. Utilisez la commande **no anyconnect dpd-interval** pour supprimer cette commande de la configuration.

### Exemple

L'exemple suivant définit la fréquence du DPD effectué par l'ASA à 30 secondes et celle du DPD effectué par le client à 10 secondes pour la stratégie de groupe existante *sales* :

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect dpd-interval gateway 30
hostname(config-group-webvpn)# anyconnect dpd-interval client 10
```

## Activer les messages keepalive

Vous pouvez ajuster la fréquence des messages keepalive pour vous assurer qu'une connexion VPN SSL à travers un proxy, un pare-feu ou un périphérique NAT demeure ouverte, même si ce périphérique limite la durée pendant laquelle la connexion peut rester inactive. L'ajustement de la fréquence garantit également que le client ne se déconnecte pas puis ne se reconnecte pas lorsque l'utilisateur distant n'exécute pas activement une application fondée sur des sockets, comme Microsoft Outlook ou Microsoft Internet Explorer.

Les messages keepalive sont activés par défaut. Si vous désactivez les messages keepalive, en cas de basculement, les sessions client VPN SSL ne sont pas transférées vers le périphérique en veille.

Pour définir la fréquence des messages keepalive, utilisez la commande **keepalive** à partir du mode de configuration de stratégie de groupe webvpn ou nom d'utilisateur webvpn : utilisez la forme **no** de la commande pour la supprimer de la configuration et faire hériter la valeur :

**[no] anyconnect ssl keepalive {none | secondes}**

- **none** Désactive les messages keepalive des clients.
- *secondes* permet au client d'envoyer des messages keepalive et précise la fréquence des messages dans une plage de 15 à 600 secondes.

Dans l'exemple suivant : l'ASA est configuré pour permettre au client d'envoyer des messages keepalive avec une fréquence de 300 secondes, soit 5 minutes, pour la stratégie de groupe existante *sales* :

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl keepalive 300
```

## Utiliser la compression

La compression augmente les performances des communications entre l'ASA et le client en réduisant la taille des paquets transférés pour les connexions à faible bande passante. Par défaut, la compression de toutes les connexions VPN SSL est activée sur l'ASA, à la fois au niveau global et pour des groupes ou des utilisateurs spécifiques.

**Remarque**

Lors de la mise en œuvre de la compression sur les connexions à large bande, vous devez prendre en compte le fait que la compression repose sur une connectivité sans perte. C'est la principale raison pour laquelle elle n'est pas activée par défaut sur les connexions à large bande.

La compression doit être activée globalement à l'aide de la commande **compression** en mode de configuration globale, puis elle peut être définie pour des groupes ou des utilisateurs spécifiques avec la commande **anyconnect ssl compression** en mode group-policy webvpn ou username webvpn.

**Modification globale de la compression**

Pour modifier les paramètres globaux de compression, utilisez la commande AnyConnect ssl **compression** à partir du mode de configuration globale. Pour supprimer la commande de la configuration, utilisez la forme **no** de la commande.

Dans l'exemple suivant, la compression est désactivée globalement pour toutes les connexions VPN SSL :

```
hostname(config)# no compression
```

**Modification de la compression pour les groupes et les utilisateurs**

Pour modifier la compression pour un groupe ou un utilisateur particulier, utilisez la commande AnyConnect ssl compression en mode group-policy webvpn ou username webvpn :

**[no] anyconnect ssl compression {deflate | none}**

Par défaut, pour les groupes et les utilisateurs, la compression SSL est définie sur *deflate* (activée).

Pour supprimer la commande **AnyConnect ssl compression** de la configuration et faire hériter la valeur du paramètre global, utilisez la forme **no** de la commande :

Dans l'exemple suivant, la compression est désactivée pour la stratégie de groupe sales :

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no anyconnect ssl compression none
```

**Ajuster la taille de la MTU**

Vous pouvez ajuster la taille de la MTU, de 576 à 1 406 octets, pour les connexions VPN SSL établies par le client au moyen de la commande **anyconnect mtu**, en mode de configuration group-policy webvpn ou username webvpn. :

**[no] anyconnect mtu size**

Cette commande affecte uniquement Secure Client (services client sécurisés). L'ancien client VPN SSL de Cisco () n'est pas en mesure de s'ajuster à différentes tailles de MTU. De plus, cette commande a une incidence sur les connexions client établies en SSL et sur celles établies en SSL avec DTLS.

La valeur par défaut pour cette commande dans la stratégie de groupe par défaut est **no anyconnect mtu**. La taille de la MTU est ajustée automatiquement en fonction de la MTU de l'interface utilisée par la connexion, moins le surdébit IP/UDP/DTLS.

Vous pouvez recevoir le message « Configuration MTU envoyée par la passerelle sécurisée trop petite », par exemple lors de l'exécution du module AnyConnect ISE Posture. Si vous saisissez **AnyConnect mtu 1200** avec **AnyConnect ssl df-bit-ignore disable**, vous pouvez éviter ces erreurs d'analyse du système.

### Exemple

L'exemple suivant configure la taille de la MTU à 1 200 octets pour la stratégie de groupe télétravailleurs :

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect mtu 1200
```

## Mettre à jour les images Secure Client (services client sécurisés)

Vous pouvez mettre à jour les images des clients sur l'ASA à tout moment en suivant cette procédure.



### Remarque

Pour une sécurité, une performance et une gestion optimales de votre infrastructure VPN, nous vous recommandons de supprimer régulièrement les images Secure Client (services client sécurisés) obsolètes de votre pare-feu, en ne conservant que les dernières versions requises pour éviter les conflits de configuration.

### Procédure

- Étape 1** Copiez les nouvelles images client dans l'ASA à l'aide de la commande **copy** du mode d'exécution privilégié ou à l'aide d'une autre méthode.
- Étape 2** Si les nouveaux fichiers image client portent les mêmes noms de fichier que les fichiers déjà chargés, entrez de nouveau la commande **anyconnect image** qui se trouve dans la configuration. Si les nouveaux noms de fichiers sont différents, désinstallez les anciens fichiers à l'aide de la commande d'image **[no]anyconnect image**. Utilisez ensuite la commande **anyconnect image** pour attribuer un ordre aux images et faire en sorte que l'ASA charge les nouvelles images.

## Activer l'accès VPN IPv6

Si vous souhaitez configurer l'accès IPv6, vous devez utiliser l'interface de ligne de commande. La version 9.0(x) de l'ASA ajoute la prise en charge des connexions VPN IPv6 à son interface externe à l'aide des protocoles SSL et IKEv2/IPsec.

Vous activez l'accès IPv6 à l'aide de la commande **ipv6 enable** dans le cadre de l'activation des connexions VPN SSL. Voici un exemple de connexion IPv6 qui active IPv6 sur l'interface externe :

```
hostname(config)# interface GigabitEthernet0/0
hostname(config-if)# ipv6 enable
```

Pour activer le VPN SSL IPv6, effectuez les actions générales suivantes :

1. Activez IPv6 sur l'interface externe.
2. Activez IPv6 et une adresse IPv6 sur l'interface interne.
3. Configurez un ensemble local d'adresses IPv6 pour les adresses IP attribuées aux clients.

#### 4. Configurez une passerelle par défaut de tunnel IPv6.

### Procédure

#### Étape 1 Configurer les interfaces :

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 192.168.0.1 255.255.255.0
 ipv6 enable ; Needed for IPv6.
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.0.1 255.255.0.0
 ipv6 address 2001:DB8::1/32 ; Needed for IPv6.
 ipv6 enable ; Needed for IPv6.
```

#### Étape 2 Configurer un « ensemble local ipv6 » (utilisé pour l'affectation d'adresses IPv6) :

```
ipv6 local pool ipv6pool 2001:DB8:1:1::5/32 100 ; Use your IPv6 prefix here
```

##### Remarque

Vous pouvez configurer l'ASA pour attribuer une adresse IPv4, une adresse IPv6 ou à la fois une adresse IPv4 et une adresse IPv6 à Secure Client (services client sécurisés) en créant des regroupements internes d'adresses sur l'ASA ou en attribuant une adresse dédiée à un utilisateur local sur l'ASA.

#### Étape 3 Ajouter l'ensemble d'adresses IPv6 à votre stratégie de groupe de tunnels (ou stratégie de groupe) :

```
tunnel-group YourTunGrp1 general-attributes ipv6-address-pool ipv6pool
```

##### Remarque

Vous devez également configurer un ensemble d'adresses IPv4 ici (à l'aide de la commande « address-ensemble »).

#### Étape 4 Configurer une passerelle par défaut de tunnel IPv6 :

```
ipv6 route inside ::/0 X:X:X:X::X tunneled
```

## SAML 2.0

L'ASA prend en charge SAML 2.0 afin que les utilisateurs VPN puissent saisir leurs informations d'authentification une seule fois lorsqu'ils accèdent à différentes applications SaaS en dehors du réseau privé.

Par exemple, une entreprise cliente a activé PingIdentity comme fournisseur d'identité (IdP) SAML et possède des comptes sur Rally, Salesforce, Oracle OEM, Microsoft ADFS, OneLogin ou Dropbox, pour lesquels l'authentification unique SAML 2.0 a été activée. Lorsque vous configurez l'ASA pour prendre en charge



SAML 2.0 SSO en tant que fournisseur de services (SP), les utilisateurs finaux peuvent se connecter une seule fois et avoir accès à tous ces services.

La prise en charge de SAML par AnyConnect a été ajoutée afin de permettre à un client AnyConnect 4.4 d'accéder à des applications basées sur SaaS au moyen de SAML 2.0. AnyConnect 4.6 a introduit une version améliorée de l'intégration SAML avec un navigateur intégré, qui a remplacé l'intégration au navigateur natif (externe) des versions précédentes. La nouvelle version améliorée avec navigateur intégré exigeait une mise à niveau vers AnyConnect 4.6 (ou version ultérieure) et ASA 9.7.1.24 (ou version ultérieure), 9.8.2.28 (ou version ultérieure) ou 9.9.2.1 (ou version ultérieure).

La version 9.17.1 d'ASA / version 7.17.1 d'ASDM a introduit la prise en charge du navigateur externe SAML pour AnyConnect VPN avec AnyConnect 4.10.04065 (ou version ultérieure). Lorsque vous utilisez SAML comme méthode d'authentification principale pour le profil de connexion VPN AnyConnect, vous pouvez choisir que le client Secure Client (services client sécurisés) utilise un navigateur local, au lieu du navigateur intégré à Secure Client (services client sécurisés) pour effectuer l'authentification Web. Grâce à cette fonctionnalité, Secure Client (services client sécurisés) prend en charge WebAuthN et toutes les autres options d'authentification Web basées sur SAML, telles que l'authentification unique, l'authentification biométrique ou d'autres méthodes améliorées qui ne sont pas offertes avec le navigateur intégré. Pour utiliser le navigateur externe SAML, vous devez effectuer la configuration décrite ici : [Configurer le navigateur du système d'exploitation par défaut pour l'authentification SAML](#), à la page 263.

L'ASA agit comme SP lorsque SAML est configuré comme méthode d'authentification pour un groupe de tunnels, qu'il s'agisse du groupe de tunnels par défaut ou de tout autre groupe. L'utilisateur VPN lance la connexion unique en accédant à un ASA activé ou au fournisseur d'identité de SAML. Chacun de ces scénarios est décrit ci-dessous.

### Authentification unique initiée par le SP SAML

Lorsque l'utilisateur final initie la connexion en accédant à l'ASA, le processus d'authentification se déroule comme suit :

1. Lorsque l'utilisateur VPN accède à un groupe de tunnels activé pour SAML ou le sélectionne, l'utilisateur final est redirigé vers le fournisseur d'identité SAML pour l'authentification. L'utilisateur est invité à s'authentifier, sauf s'il accède directement à l'URL de groupe, auquel cas la redirection est silencieuse.  
L'ASA génère une demande d'authentification SAML, que le navigateur redirige vers le fournisseur d'identité de SAML.
2. Le fournisseur d'identité invite l'utilisateur final à saisir ses informations d'authentification, puis l'utilisateur final se connecte. Les informations d'authentification saisies doivent satisfaire à la configuration d'authentification du fournisseur d'identité.
3. La réponse du fournisseur d'identité est renvoyée au navigateur et publiée sur l'URL de connexion de l'ASA. L'ASA vérifie la réponse pour terminer la connexion.

### SSL initié par le fournisseur d'identité SAML

Lorsque l'utilisateur initie la connexion en accédant au fournisseur d'identité, le processus d'authentification se déroule comme suit :

1. Un utilisateur final accède au fournisseur d'identité. Le fournisseur d'identité invite l'utilisateur final à saisir ses informations d'authentification conformément à sa configuration d'authentification. L'utilisateur final envoie ses informations d'authentification et se connecte au fournisseur d'identité.

2. En général, l'utilisateur final obtient une liste des services compatibles avec SAML qui ont été configurés avec le fournisseur d'identité. L'utilisateur final choisit l'ASA.
3. Une réponse SAML est renvoyée au navigateur et publiée sur l'URL de connexion de l'ASA. L'ASA vérifie la réponse pour terminer la connexion.

### Cercle de confiance

La relation de confiance entre l'ASA et le fournisseur d'identité SAML est établie au moyen de certificats configurés (points de confiance ASA).

La relation de confiance entre l'utilisateur final et le fournisseur d'identité SAML est établie par l'authentification configurée sur le fournisseur d'identité.

### Délai d'expiration SAML

Dans l'assertion SAML, il existe NotBefore et NotOnOrAfter comme suit :<saml:Conditions NotBefore="2015-03-10T19:47:41Z" NotOnOrAfter="2015-03-10T20:47:41Z">

Un délai d'expiration SAML configuré sur l'ASA remplacera NotOnOrAfter si la somme de NotBefore et du délai d'expiration est antérieure à NotOnOrAfter. Si NotBefore + le délai d'expiration est postérieur à NotOnOrAfter, NotOnOrAfter prend effet.

Le délai d'expiration doit être très court pour éviter que l'assertion ne soit réutilisée après l'expiration du délai. Vous devez synchroniser le serveur NTP (Network Time Protocol) de votre ASA avec le serveur NTP du fournisseur d'identité pour utiliser la fonctionnalité SAML.

### Prise en charge dans le réseau privé

L'identifiant du fournisseur de services basé sur SAML 2.0 est pris en charge dans un réseau privé. Lorsque le fournisseur d'identité SAML est déployé dans le nuage privé, l'ASA et les autres services compatibles avec SAML sont en position d'homologues et se trouvent tous dans le réseau privé. Avec l'ASA comme passerelle entre l'utilisateur et les services, l'authentification sur l'IdP est gérée avec une session webvpn anonyme restreinte, et tout le trafic entre l'IdP et l'utilisateur est traduit. Lorsque l'utilisateur se connecte, l'ASA modifie la session avec les attributs correspondants et stocke les sessions du fournisseur d'identité. Vous pouvez ensuite utiliser le fournisseur de services sur le réseau privé sans avoir à saisir de nouveau vos informations d'authentification.

L'attribut *NameID* du fournisseur d'identité SAML détermine le nom d'utilisateur et est utilisé pour l'autorisation, la comptabilité et la base de données des sessions VPN.



#### Remarque

Vous ne pouvez pas échanger d'informations d'authentification entre les réseaux privé et public. Si vous utilisez le même fournisseur d'identité pour les fournisseurs de services internes et externes, vous devez vous authentifier séparément. Le fournisseur d'identité interne uniquement ne peut pas être utilisé avec des services externes : le fournisseur d'identité externe uniquement ne peut pas être utilisé avec les fournisseurs de services dans le réseau privé.

## Directives et limites relatives à SAML 2.0

- ASA prend en charge les signatures suivantes pour l'authentification SAML :

- SHA1 avec RSA et HMAC
- SHA2 avec RSA et HMAC
- ASA prend en charge la liaison Redirect-POST SAML 2.0, qui est prise en charge par tous les fournisseurs d'identité SAML.
- L'ASA fonctionne uniquement comme fournisseur de service SAML. Il ne peut pas servir de fournisseur d'identité en mode passerelle ou en mode homologue.
- Cette fonctionnalité SAML SSO SP est une méthode d'authentification d'exclusion mutuelle. Elle ne peut pas être utilisée conjointement avec AAA et le certificat.
- Les fonctionnalités basées sur l'authentification par nom d'utilisateur/mot de passe, l'authentification de certificats et le KCD ne sont pas prises en charge. Par exemple, la fonction de préremplissage du nom d'utilisateur et du mot de passe, la connexion automatique basée sur un formulaire, la connexion automatique basée sur la substitution de macros, KCD SSO, etc.
- L'ASA prend en charge l'équilibrage de charges VPN avec l'authentification SAML AnyConnect.
- Lorsque vous utilisez Safari pour l'authentification SAML, assurez-vous de disposer de la mise à jour de Safari 14.1.2 ou ultérieure.
- Les administrateurs ASA doivent assurer la synchronisation de l'horloge entre l'ASA et le fournisseur d'identité SAML pour une gestion appropriée des déclarations d'authentification et un comportement correct du délai d'expiration.
- Les administrateurs ASA ont la responsabilité de maintenir un certificat de signature valide sur l'ASA et sur le fournisseur d'identité en tenant compte des éléments suivants :
  - Le certificat de signature du fournisseur d'identité est obligatoire lors de la configuration d'un fournisseur d'identité sur l'ASA.
  - L'ASA n'effectue pas de vérification de révocation sur le certificat de signature reçu du fournisseur d'identité.
- Dans les assertions SAML, il existe des conditions NotBefore et NotOnOrAfter . Le **délai d'expiration** configuré pour la SAML interagit avec ces conditions comme suit :
  - Le délai d'expiration remplace NotOnOrAfter si la somme de NotBefore et du délai d'expiration est antérieure à NotOnOrAfter.
  - Si NotBefore + le délai d'expiration est postérieur à NotOnOrWith, NotOnOrAfter prend effet.
  - Si l'attribut NotBefore est absent, l'ASA refuse la demande de connexion. Si l'attribut NotOnOrAfter est absent et que le délai d'expiration SAML n'est pas défini, l'ASA refuse la demande de connexion.
- L'ASA ne fonctionne pas avec Duo dans un déploiement utilisant SAML interne, ce qui oblige l'ASA à passer par le proxy pour que le client s'authentifie, en raison du changement de nom de domaine complet qui se produit lors de la demande/réponse pour l'authentification à deux facteurs (push, code, mot de passe).
- Les certificats de serveur non fiable ne sont pas autorisés dans le navigateur intégré.
- L'intégration SAML au navigateur intégré n'est pas prise en charge en modes CLI ou SBL.

- L'authentification SAML établie dans un navigateur Web n'est pas partagée avec AnyConnect, et inversement.
- Selon la configuration, diverses méthodes sont utilisées lors de la connexion à la tête de réseau avec le navigateur intégré. Par exemple, alors qu'AnyConnect peut préférer une connexion IPv4 à une connexion IPv6, le navigateur intégré peut préférer IPv6, ou inversement. De même, AnyConnect peut avoir recours à l'absence de proxy après avoir essayé de passer par un proxy et obtenu un échec, tandis que le navigateur intégré peut arrêter la navigation après avoir essayé de passer par un mandataire et obtenu un échec.
- Vous devez synchroniser le serveur NTP (Protocole de temps réseau) de votre ASA avec le serveur NTP du fournisseur d'identité pour utiliser la fonctionnalité SAML.
- L'assistant VPN sur ASDM ne prend actuellement pas en charge les configurations SAML.
- Vous ne pouvez pas accéder aux serveurs internes avec la SSO après vous être connecté à l'aide d'un fournisseur d'identité interne.
- L'attribut NameID du fournisseur d'identité SAML détermine le nom d'utilisateur de l'utilisateur et est utilisé pour l'autorisation, la comptabilité et la base de données des sessions VPN.
- SAML n'est pas pris en charge en mode multicontexte.
- Plusieurs attributs reçus avec une validation SAML ne sont pas pris en charge.
- Les Chromebook ne prennent pas en charge Secure Client SAML avec l'authentification par navigateur externe.
- Assurez-vous que le fournisseur d'identité comprend le paramètre d'état de relais dans la réponse SAML, tel qu'il a été reçu dans la demande SAML correspondante.

## Configurer un fournisseur d'identité (IdP) SAML 2.0

### Avant de commencer

Obtenez les URL de connexion et de déconnexion pour votre fournisseur SAML (IdP). Vous pouvez obtenir les URL sur le site Web du fournisseur, ou ils peuvent fournir ces informations dans un fichier de métadonnées.

### Procédure

- 
- Étape 1** Créez un fournisseur d'identité SAML en mode de configuration webvpn et passez en sous-mode saml-idp sous webvpn.
- [no] saml idp idp-entityID**
- idp-entityID* : l'ID d'entité du fournisseur d'identité de SAML doit contenir de 4 à 128 caractères.
- Pour supprimer un fournisseur d'identité de SAML, utilisez la forme **no** de cette commande.
- Étape 2** Configurez les URL du fournisseur d'identité.
- url [sign-in | sign-out] value**

*value* : Il s'agit de l'URL pour la connexion au fournisseur d'identité ou de l'URL de redirection lors de la déconnexion du fournisseur d'identité. L'URL **sign-in** est requise, l'URL **sign-out** est facultative. La valeur de l'URL doit contenir de 4 à 500 caractères.

### Étape 3

(Facultatif) Configure l'URL de base du fournisseur de services SAML pour l'authentification VPN. Cette URL est utilisée dans les métadonnées SAML, qui sont fournies aux fournisseurs d'identité tiers, afin que les fournisseurs d'identité puissent rediriger les utilisateurs de points terminaux vers l'ASA.

#### **base-url** *URL*

Cette URL est fournie à des fournisseurs d'identité tiers pour rediriger les utilisateurs finaux vers l'ASA.

Lorsque **base-url** est configuré, nous l'utilisons comme URL de base pour les attributs AssertionConsumerService et SingleLogoutService dans **show saml metadata**.

Lorsque l'URL de base n'est pas configurée, l'URL est déterminée par le nom d'hôte et le nom de domaine de l'ASA. Par exemple, nous utilisons `https://ssl-vpn.cisco.com` lorsque le nom d'hôte est `ssl-vpn` et que le nom de domaine est `cisco.com`.

Une erreur se produit si ni l'URL de base ni le nom d'hôte/nom de domaine ne sont configurés lors de la saisie de **show saml metadata**.

### Étape 4

Configurez les trustpoints entre le fournisseur d'identité et le fournisseur (ASA).

#### **trustpoint** [**idp** | **sp**] *trustpoint-name*

**idp** : spécifie le trustpoint qui contient le certificat du fournisseur d'identité pour que l'ASA vérifie les assertions SAML.

**sp** : spécifie le trustpoint qui contient le certificat de l'ASA (SP) pour que le fournisseur d'identité vérifie la signature de l'ASA ou l'assertion SAML chiffrée.

*trustpoint-name* : doit être un trustpoint configuré précédemment.

### Étape 5

(Facultatif) Configurez le délai d'expiration SAML.

#### **timeout assertion** *timeout-in-seconds*

Si ce paramètre est spécifié, cette configuration remplace NotOnOrAfter si la somme de NotBefore et de timeout-in-seconds est antérieure à NotOnOrAfter.

Si ce paramètre n'est pas spécifié, NotBefore et NotOnOrAfter dans l'assertion sont utilisés pour déterminer la validité.

#### **Remarque**

Pour un groupe de tunnels avec un fournisseur d'identité SAML existant configuré, toutes les modifications apportées à l'interface de ligne de commande `saml idp` sous `webvpn` ne sont appliquées qu'au groupe de tunnels lorsque SAML est réactivé pour ce groupe de tunnels particulier. Après avoir configuré le délai d'expiration, le délai d'expiration mis à jour ne prend effet qu'après la réémission de l'interface de ligne de commande du fournisseur d'identité `saml` dans les attributs `webvpn` du groupe de tunnels.

### Étape 6

(Facultatif) Activez ou désactivez (paramètre par défaut) la signature dans la requête SAML.

#### **signature** <*value*>

#### **Remarque**

Avec la mise à niveau vers SSO 2.5.1, la méthode de signature par défaut passe de SHA1 à SHA256, et vous pouvez configurer la méthode de signature que vous préférez en entrant la *valeur* `rsa-sha1`, `rsa-sha256`, `rsa-sha384` ou `rsa-sha512`.

- Étape 7** (Facultatif) Pour définir l'indicateur déterminant que le fournisseur d'identité est un réseau interne, utilisez la commande **internal**. L'ASA fonctionnera ensuite en mode de passerelle.
- Étape 8** Utilisez **show webvpn saml idp** pour afficher la configuration.
- Étape 9** Utilisez **force re-authentication** pour que le fournisseur d'identité s'authentifie directement plutôt que de dépendre d'un contexte de sécurité précédent lorsqu'une demande d'authentification SAML se produit. Il s'agit du paramètre par défaut ; donc, pour désactiver, utilisez **no force re-authentication**.

### Exemple

L'exemple suivant configure un fournisseur d'identité nommé `salesforce_idp` et utilise des points de confiance préconfigurés :

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)#saml idp salesforce_idp

ciscoasa(config-webvpn-saml-idp)#url sign-in
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
ciscoasa(config-webvpn-saml-idp)#url sign-out
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect

ciscoasa(config-webvpn-saml-idp)#trustpoint idp salesforce_trustpoint
ciscoasa(config-webvpn-saml-idp)#trustpoint sp asa_trustpoint

ciscoasa(config)#show webvpn saml idp
saml idp salesforce_idp
url sign-in https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
url sign-out https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
trustpoint idp salesforce_trustpoint
trustpoint sp asa_trustpoint
```

La page Web suivante montre un exemple de la manière d'obtenir les URL pour OneLogin

<https://onelogin.zendesk.com/hc/en-us/articles/202767260-Configuring-SAML-for-Clarizen>

La page Web suivante est un exemple d'utilisation des métadonnées pour trouver les URL à partir de OneLogin.

[http://onlinehelp.tableau.com/current/online/en-us/saml\\_config\\_onelogin.htm](http://onlinehelp.tableau.com/current/online/en-us/saml_config_onelogin.htm)

### Prochaine étape

Appliquez l'authentification SAML aux profils de connexion, comme décrit dans [Configurer l'ASA en tant que fournisseur de services SAML 2.0](#), à la page 262.

## Configurer l'ASA en tant que fournisseur de services SAML 2.0

### Avant de commencer

Le fournisseur d'identité doit avoir été configuré précédemment. Consultez [Configurer un fournisseur d'identité \(IdP\) SAML 2.0](#), à la page 260.

## Procédure

- Étape 1** En sous-mode webvpn de groupe de tunnels, utilisez la commande `saml identity-provider` pour attribuer un fournisseur d'identité.
- saml identity-provider** *idp-entityID*
- idp-entityID* : doit être l'un des fournisseurs d'identité existants configurés précédemment.
- Pour désactiver SAML SP, utilisez la forme **no** de cette commande.
- Étape 2** Activez la méthode d'authentification SAML.
- authentication saml**

## Exemple

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

# Configurer le navigateur du système d'exploitation par défaut pour l'authentification SAML

Précisez si AnyConnect doit gérer ou non le processus d'authentification SSO à l'aide du navigateur natif de la plateforme (le navigateur par défaut du système d'exploitation) ou à l'aide du navigateur intégré dans AnyConnect.

Vous devez télécharger le progiciel de navigateur externe AnyConnect (par exemple, *external-ss0-4.10.04065-webdeploy-k9.pkg*) et le charger sur ASA. Vous pouvez ensuite choisir la méthode de connexion SAML (le navigateur intégré d'AnyConnect ou le navigateur par défaut du système d'exploitation) pour l'authentification SAML. Cet ensemble est un script qui permet au client VPN de lancer le navigateur Web du système d'exploitation par défaut à des fins d'authentification, et est indépendant du système d'exploitation, du navigateur et de la version du client VPN. Tant que la fonctionnalité est activée, la version du client VPN et le fichier de version du paquet de navigateur externe n'ont pas besoin de correspondre.

Choisir le navigateur du système d'exploitation par défaut active la connexion unique (SSO) entre votre authentification VPN et d'autres connexions d'entreprise. Choisissez cette option si vous souhaitez prendre en charge des méthodes d'authentification web, telles que l'authentification biométrique, qui ne peuvent pas être exécutées dans le navigateur intégré. Avant de sélectionner le navigateur du système d'exploitation, vous devez charger un paquet qui peut être exécuté dans le navigateur pour activer l'authentification Web.

## Procédure

- 
- Étape 1** En sous-mode webvpn, utilisez la commande AnyConnect external-browser-pkg pour activer l'authentification SAML AnyConnect à l'aide du navigateur par défaut du système d'exploitation.
- anyconnect external-browser-pkg path**
- Pour désactiver le navigateur par défaut du système d'exploitation pour l'authentification SAML, utilisez la forme **no** de cette commande.
- Étape 2** En sous-mode webvpn de groupe de tunnels, utilisez la commande external-browser pour activer l'authentification SAML AnyConnect à l'aide du navigateur par défaut du système d'exploitation.
- external-browser enable idp-entityID**
- Pour désactiver le navigateur par défaut du système d'exploitation pour l'authentification SAML, utilisez la forme **no** de cette commande.
- 

## Exemple

Cet exemple sélectionne le chemin d'accès au paquet de navigateur externe AnyConnect et active un navigateur externe (le navigateur par défaut du système d'exploitation) pour l'authentification SAML.

```
asa(config-webvpn)# anyconnect external-browser-pkg flashshow :
asa(config)# tunnel-group SAML webvpn-attributes
asa(config-tunnel-webvpn)# external-browser enable
asa(config-tunnel-webvpn)#
```

# Configurer l'authentification par certificat et SAML

Vous pouvez configurer l'authentification par certificat et l'authentification SAML pour les profils de connexion basés sur SAML afin de valider les ressources du client sans profilage pour une clé de fichier ou de registre particulière. Les authentifications basées sur SAML peuvent être liées à des ressources ou à des utilisateurs autorisés. Vous pouvez utiliser un seul certificat ou plusieurs certificats avec SAML pour l'authentification.

Lorsque Secure Client (services client sécurisés) amorce une connexion, l'ASA ou le FTD demandera et authentifie un ou plusieurs certificats du point terminal avant que l'authentification SAML ne soit effectuée.

Une fois l'authentification SAML terminée, le nom d'utilisateur de SAML et du certificat peut être

Une fois l'authentification SAML terminée, le nom d'utilisateur de SAML et du certificat peut être comparé avant de passer à la phase d'autorisation.

## Avant de commencer

Assurez-vous de configurer les paramètres SAML requis avant la configuration de l'authentification par certificat et SAML :



- Obtenez les URL de connexion et de déconnexion pour votre fournisseur SAML (IdP). Vous pouvez obtenir les URL sur le site Web du fournisseur, ou ils peuvent fournir ces informations dans un fichier de métadonnées.
- Configurez les paramètres du fournisseur d'identité SAML et du point de confiance. Voir la section [Configurer l'authentification par certificat et SAML](#), à la page 264.

### Procédure

- Étape 1** Pour configurer le certificat et l'authentification SAML, passez en mode d'attributs webvpn-attributs de groupe de tunnels en saisissant la commande suivante. L'invite change pour indiquer le changement de mode :
- ```
hostname(config)# tunnel-group tunnel-group-name webvpn-attributs
hostname(config-tunnel-webvpn)#
```
- Étape 2** Pour préciser la méthode d'authentification à utiliser, entrez la commande suivante :
- ```
hostname(config-tunnel-webvpn)#authentication authentication_method
```
- Par exemple : la commande suivante permet l'authentification SAML et par certificat :
- ```
hostname(config-tunnel-webvpn)#authentication saml certificate
```
- La commande suivante permet l'authentification par certificat et SAML :
- ```
hostname(config-tunnel-webvpn)#authentication certificate saml
```
- La commande suivante permet l'authentification par certificats multiples et SAML :
- ```
hostname(config-tunnel-webvpn)#authentication multiple-certificate saml
```
- Étape 3** Ajoutez ou modifiez un profil de connexion, puis sélectionnez les paramètres d'attributs du profil de connexion dans **Basic (De base)**.
- Étape 4** Pour préciser la méthode d'authentification pour l'authentification par certificat et SAML, sélectionnez SAML et certificat ou Plusieurs certificats et SAML dans la liste déroulante.

Exemple

L'exemple suivant configure plusieurs certificats et l'authentification SAML pour le profil de connexion sales_group :

```
ciscoasa(config)# tunnel-group sales_group webvpn
ciscoasa(config-tunnel-webvpn)#authentication multiple-certificate saml
```

Exemple de SAML 2.0 et OneLogin

Suivez cet exemple en utilisant votre fournisseur d'identité SAML 2.0 tiers à la place des informations et de la dénomination Onelogin.

1. Définissez la synchronisation de l'horloge entre le fournisseur d'identité et l'ASA (SP).

```
ciscoasa(config)# ntp server 209.244.0.4
```

2. Obtenez les métadonnées SAML du fournisseur d'identité en suivant les procédures fournies par votre fournisseur d'identité tiers.

3. Importez le certificat de signature du fournisseur d'identité dans un point de confiance.

```
ciscoasa(config)# crypto ca trustpoint onelogin
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# no ca-check
ciscoasa(config-ca-trustpoint)# crypto ca authenticate onelogin
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
quit
INFO: Certificate has the following attributes:
Fingerprint:      85de3781 07388f5b d92d9d14 1e22a549
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

4. Importez le certificat de signature PKCS12 du SP (ASA) dans un point de confiance

```
ciscoasa(config)# crypto ca import asa_saml_sp pkcs12 password
Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
quit
INFO: Import PKCS12 operation completed successfully
```

5. Ajoutez un fournisseur d'identité de SAML :

```
ciscoasa(config-webvpn)# saml idp https://app.onelogin.com/saml/metadata/462950
```

6. Configurez les attributs en sous-mode saml-idp :

Configurez l'URL de connexion et l'URL de déconnexion du fournisseur d'identité :

```
ciscoasa(config-webvpn-saml-idp)# url sign-in
https://ross.onelogin.com/trust/saml2/http-post/sso/462950
ciscoasa(config-webvpn-saml-idp)# url sign-out
https://ross.onelogin.com/trust/saml2/http-redirect/slo/462950
```

Configurez le point de confiance du fournisseur d'identité et le point de confiance du fournisseur de services (SP)

```
ciscoasa(config-webvpn-saml-idp)# trustpoint idp onelogin
ciscoasa(config-webvpn-saml-idp)# trustpoint sp asa_saml_sp
```

Configurez l'URL de base du VPN sans client, la signature de requête SAML et le délai d'expiration (timeout) de l'assertion SAML :

```
ciscoasa(config-webvpn-saml-idp)# base-url https://172.23.34.222
ciscoasa(config-webvpn-saml-idp)# signature
ciscoasa(config-webvpn-saml-idp)# timeout assertion 7200
```

7. Configurez un fournisseur d'identité pour un groupe de tunnels et activez l'authentification SAML.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

8. Affichez les métadonnées SAML SP de l'ASA :

Vous pouvez obtenir les métadonnées SAML SP de l'ASA à l'adresse https://172.23.34.222/saml/sp/metadata/cloud_idp_onelogin. Dans l'URL, `cloud_idp_onelogin` est le nom du groupe de tunnels.

9. Configurez un fournisseur de services SAML sur votre fournisseur d'identité tiers en suivant les procédures fournies par votre fournisseur d'identité tiers.

Dépannage de SAML 2.0

Utilisez la valeur **debug webvpn saml** pour déboguer le comportement de SAML 2.0. Les messages SAML suivants s'afficheront en fonction de la valeur :

- 8 : erreurs
- 16 : avertissements et erreurs
- 128 ou 255 : débogage, avertissements et erreurs

Surveiller les connexions Secure Client (services client sécurisés).

Pour afficher des renseignements sur les sessions actives, utilisez la commande **show vpn-sessiondb** :

Commande	Objectif
show vpn-sessiondb	Affiche des renseignements sur les sessions actives.
vpn-sessiondb logoff	Déconnecte les sessions VPN.
show vpn-sessiondb AnyConnect (afficher <code>vpn-sessiondb AnyConnect</code>)	Améliore le résumé des sessions VPN pour afficher les renseignements sur les sessions OSPFv3.
show vpn-sessiondb ratio encryption (afficher <code>vpn-sessiondb ratio encryption</code>)	Affiche le nombre de tunnels et les pourcentages pour les algorithmes de suite B (comme AES-GCM-128, AES-GCM-192, AES-GCM-256, AES-GMAC-128, etc.).

**Remarque AnyConnect Parent Tunnel** (Tunnel parent AnyConnect)

Les tunnels parents AnyConnect n'ont pas d'adresses IP attribuées.

Il s'agit de la session principale créée pendant la négociation afin d'établir le jeton de session nécessaire si une reconnexion s'impose en raison de problèmes de connectivité réseau ou d'une mise en veille prolongée. En fonction du mécanisme de connexion, Cisco Adaptive Security Appliance (ASA) répertorie la session comme sans client (lancement Web via le portail) ou parent (autonome AnyConnect).

AnyConnect parent représente la session lorsque le client n'est pas activement connecté. En pratique, il fonctionne comme un témoin, puisqu'il s'agit d'une entrée de base de données sur l'ASA qui correspond à la connexion d'un client particulier. Si le client est mis en veille ou en veille prolongée, les tunnels (protocoles IPsec/Internet Key Exchange [IKE]/Transport Layer Security [TLS]/Datagram Transport Layer Security [DTLS]) sont démontés, mais le Parent reste en place jusqu'à ce que le délai d'inactivité ou la durée maximale de connexion prenne effet. Cela permet à l'utilisateur de se reconnecter sans devoir se réauthentifier.

Exemple

Le champ Inactivity (Inactivité) affiche le temps écoulé depuis qu'une session Secure Client (services client sécurisés) a perdu la connectivité. Si la session est active, 00:00m:00s s'affiche dans ce champ.

```
hostname# show vpn-sessiondb

Session Type: SSL VPN Client

Username       : lee
Index          : 1
Protocol       : SSL VPN Client
Hashing        : SHA1
TCP Dst Port   : 443
Bytes Tx       : 20178
Pkts Tx        : 27
Client Ver     : Cisco STC 1.1.0.117
Client Type    : Internet Explorer
Group          : DfltGrpPolicy
Login Time     : 14:32:03 UTC Wed Mar 20 2007
Duration       : 0h:00m:04s
Inactivity     : 0h:00m:04s
Filter Name    :

hostname# vpn-sessiondb logoff
INFO: Number of sessions of type "" logged off : 1

hostname# vpn-sessiondb logoff name tester
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "tester" logged off : 1
```

Déconnecter les sessions VPN AnyConnect

Pour déconnecter toutes les sessions VPN, utilisez la commande **vpn-sessiondb logoff** en mode de configuration globale :

L'exemple suivant déconnecte toutes les sessions VPN :

```
hostname# vpn-sessiondb logoff
INFO: Number of sessions of type "" logged off : 1
```

Vous pouvez déconnecter les sessions individuelles en utilisant l'argument du nom ou l'argument de l'index :

```
vpn-sessiondb logoff name name
```

```
vpn-sessiondb logoff index index
```

Les sessions qui ont été inactives le plus longtemps sont marquées comme inactives (et sont automatiquement déconnectées) de sorte que la capacité de licence n'est pas atteinte et que les nouveaux utilisateurs peuvent se connecter. Si la session reprend ultérieurement, elle est supprimée de la liste inactive.

Vous pouvez trouver à la fois le nom d'utilisateur et le numéro d'index (établi par l'ordre des images client) dans la sortie de la commande **show vpn-sessiondb anyconnect**. Les exemples suivants montrent le nom d'utilisateur *lee* et le numéro d'index *1*.

```
hostname# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username      : lee                      Index      : 1
Assigned IP   : 192.168.246.1          Public IP   : 10.139.1.2
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : RC4 AES128             Hashing     : SHA1
Bytes Tx      : 11079                  Bytes Rx    : 4942
Group Policy  : EngPolicy               Tunnel Group : EngGroup
Login Time    : 15:25:13 EST Fri Jan 28 2011
Duration      : 0h:00m:15s
Inactivity    : 0h:00m:00s
NAC Result    : Unknown
VLAN Mapping  : N/A                    VLAN        : none
```

L'exemple suivant met fin à la session en utilisant l'option **name** de la commande **vpn-session-db logoff** :

```
hostname# vpn-sessiondb logoff name lee
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "lee" logged off : 1

hostname#
```

Historique des fonctionnalités pour les connexions Secure Client (services client sécurisés)

Le tableau suivant présente l'historique des versions de cette fonctionnalité.

Tableau 14 : Historique des fonctionnalités pour les connexions Secure Client (services client sécurisés)

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Connexions Secure Client (services client sécurisés)	7.2(1)	Les commandes suivantes ont été introduites ou modifiées : <code>authentication eap-proxy</code> , <code>authentication ms-chap-v1</code> , <code>authentication ms-chap-v2</code> , <code>authentication pap</code> , <code>tunnel hello l2tp</code> , <code>vpn-tunnel-protocol l2tp-ipsec</code>

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
IPsec IKEv2	v 8.4(1)	IKEv2 a été ajouté pour prendre en charge les connexions IPsec IKEv2 pour le Secure Client (services client sécurisés) et LAN à LAN.



CHAPITRE 10

Secure Client (services client sécurisés) Analyse de l'hôte

Le module de posture AnyConnect Secure Client (services client sécurisés) permet d'identifier le système d'exploitation, l'anti-programme malveillant et le logiciel de pare-feu installés sur l'hôte. L'application HostScan recueille ces informations. L'évaluation de la posture nécessite l'installation de HostScan sur l'hôte.

- [Préalables pour la posture HostScan/Secure Firewall](#), à la page 271
- [Licences pour HostScan](#), à la page 271
- [Proiciel HostScan](#), à la page 272
- [Installer ou mettre à niveau HostScan/Secure Firewall Posture](#), à la page 272
- [Activer ou désactiver HostScan](#), à la page 273
- [Afficher la version de HostScan/Secure Firewall Posture activée sur l'ASA](#), à la page 274
- [Désinstaller HostScan/Secure Firewall Posture](#), à la page 274
- [Attribuer des modules de fonctionnalité Secure Client \(services client sécurisés\) aux stratégies de groupe](#), à la page 275
- [Documentation associée à HostScan/Secure Firewall Posture](#), à la page 276

Préalables pour la posture HostScan/Secure Firewall

L'Secure Client (services client sécurisés) avec le module Secure Firewall Posture/HostScan nécessite au minimum les composants ASA suivants :

- ASA 8.4
- ASDM 6.4

Vous devez installer Secure Firewall Posture/HostScan pour utiliser la fonction d'authentification SCEP.

Reportez-vous à [Plateformes VPN prises en charge, série Cisco ASA](#) pour connaître les systèmes d'exploitation pris en charge pour l'installation de Secure Firewall Posture/HostScan.

Licences pour HostScan

Voici les exigences de licence Secure Client (services client sécurisés) pour HostScan :

- AnyConnect Apex

- AnyConnect VPN seulement

Proiciel HostScan

Vous pouvez charger le package HostScan sur l'ASA en tant que package autonome : **hostscan-version.pkg**. Ce fichier contient le logiciel HostScan ainsi que la bibliothèque et les tableaux d'assistance de HostScan.

Installer ou mettre à niveau HostScan/Secure Firewall Posture

Utilisez cette procédure pour installer ou mettre à niveau le logiciel HostScan ou Secure Firewall Posture et l'activer à l'aide de l'interface de ligne de commande de l'ASA.

Avant de commencer



Remarque

Si vous tentez d'effectuer une mise à niveau vers HostScan version 4.6.x ou ultérieure à partir d'une version 4.3.x ou d'une version antérieure, vous recevrez un message d'erreur en raison du fait que toutes les politiques DAP existantes d'AV/AS/FW et les scripts LUA que vous avez établis précédemment sont incompatibles avec HostScan 4.6.x ou version ultérieure.

Il existe une procédure de migration unique qui doit être effectuée pour adapter votre configuration. Cette procédure implique de quitter cette boîte de dialogue afin de migrer votre configuration pour qu'elle soit compatible avec HostScan 4.4.x avant d'enregistrer cette configuration. Abandonnez cette procédure et consultez le [Secure Client \(services client sécurisés\) guide de migration HostScan de la version 4.3.x à la version 4.6.x](#) pour obtenir des instructions détaillées. En résumé, la migration implique la navigation vers la page de politique DAP d'ASDM pour passer en revue et supprimer manuellement les attributs incompatibles d'AV/AS/FW, puis de passer en revue et de réécrire les scripts LUA.

- Au niveau de l'interface de ligne de commande de l'ASA, entrez en mode de configuration globale. En mode de configuration globale, l'ASA affiche cette invite : `hostname(config)#`
- Chargez le fichier `secure-firewall-posture-version-k9.pkg` sur l'ASA. Si vous utilisez la version HostScan 4.x, vous devez charger le fichier `hostscan_version-k9.pkg`.

Procédure

Étape 1 Entrez en mode de configuration webvpn.

Exemple :

```
hostname(config)# webvpn
```

Étape 2 Ouvrez ASDM et choisissez **Configuration > Remote Access VPN (VPN d'accès à distance) > Posture (for Secure Firewall) (Posture [pour Secure Firewall]) > Posture Image (Image Posture)**. Si vous utilisez la version HostScan 4.x, le chemin d'accès sera **Configuration > Remote Access VPN (VPN d'accès à distance) > Secure Desktop Manager (Gestionnaire Secure Desktop) > HostScan Image (Image HostScan)**.

Étape 3 Précisez le chemin d'accès au paquet que vous souhaitez désigner comme image HostScan/Secure Firewall Posture. Vous pouvez préciser un progiciel autonome ou le progiciel Secure Client (services client sécurisés).

hostscan image path

Exemple :

Si vous utilisez la version HostScan 4.x,

```
ASAName (webvpn) #hostscan image disk0:/hostscan_4.10.06081.pkg
```

Si vous utilisez la version Secure Firewall Posture 5.x,

```
ASAName (webvpn) #hostscan image disk0:/secure-firewall-posture5.0.00556.pkg
```

Étape 4 Activez l'image HostScan/Secure Firewall Posture que vous avez désignée à l'étape précédente.

Exemple :

```
ASAName (webvpn) #hostscan enable
```

Étape 5 Enregistrez la configuration en cours d'exécution dans la mémoire flash. Après avoir enregistré avec succès la nouvelle configuration dans la mémoire flash, vous recevez le message [OK].

Exemple :

```
hostname (webvpn) # write memory
```

Étape 6

Activer ou désactiver HostScan

Ces commandes activent ou désactivent une image HostScan installée à l'aide de l'interface de ligne de commande de l'ASA.

Avant de commencer

Au niveau de l'interface de ligne de commande de l'ASA, entrez en mode de configuration globale. En mode de configuration globale, l'ASA affiche cette invite : `hostname(config)#`

Procédure

Étape 1 Entrez en mode de configuration webvpn.

Exemple :

```
webvpn
```

Étape 2 Activez l'image autonome HostScan si elle n'a pas été désinstallée de l'ASA.

```
hostscan enable
```

Étape 3 Désactivez HostScan pour tous les progiciels HostScan installés.

Remarque

Avant de désinstaller l'image HostScan activée, vous devez d'abord désactiver HostScan à l'aide de cette commande.

no hostscan enable

Afficher la version de HostScan/Secure Firewall Posture activée sur l'ASA

Utilisez cette procédure pour déterminer la version de HostScan/Secure Firewall Posture activée à l'aide de l'interface de ligne de commande de l'ASA.

Avant de commencer

Connectez-vous à l'ASA et passez en mode d'exécution privilégié. En mode d'exécution privilégié, l'ASA affiche cette invite : hostname#

Procédure

Affichez la version de HostScan/Secure Firewall Posture activée sur l'ASA.

show webvpn hostscan

Désinstaller HostScan/Secure Firewall Posture

La désinstallation du package HostScan/Secure Firewall Posture le retire de l'affichage dans l'interface ASDM et empêche l'ASA de le déployer, même lorsqu'il est activé. La désinstallation de HostScan/Secure Firewall Posture ne supprime pas le paquet de la mémoire flash.

Avant de commencer

Connectez-vous à l'ASA et passez en mode de configuration globale. En mode de configuration globale, l'ASA affiche cette invite : hostname(config)#

Procédure**Étape 1**

Entrez en mode de configuration webvpn.

webvpn

Étape 2

Désactivez l'image HostScan/Secure Firewall Posture que vous souhaitez désinstaller.

no hostscanenable**Étape 3**

Précisez le chemin d'accès à l'image HostScan/Secure Firewall Posture que vous souhaitez désinstaller. Un progiciel autonome peut avoir été désigné comme progiciel HostScan/Secure Firewall Posture.

no hostscan image path**Exemple :**

Si vous utilisez la version HostScan 4.x,

```
ASAName (webvpn) #hostscan image disk0:/hostscan_4.10.06081-k9.pkg
```

Si vous utilisez la version 5.x de Secure Firewall Posture,

```
ASAName (webvpn) #hostscan image disk0:/secure-firewall-posture-5.0.00556-k9.pkg
```

Étape 4

Enregistrez la configuration en cours dans la mémoire flash. Après l'enregistrement réussi de la nouvelle configuration dans la mémoire flash, le message [OK] s'affiche.

write memory

Attribuer des modules de fonctionnalité Secure Client (services client sécurisés) aux stratégies de groupe

Cette procédure associe les modules de fonctionnalité Secure Client (services client sécurisés) à une stratégie de groupe. Lorsque les utilisateurs VPN se connectent à l'ASA, l'ASA télécharge et installe ces modules de fonctionnalité Secure Client (services client sécurisés) sur leur ordinateur terminal.

Avant de commencer

Au niveau de l'interface de ligne de commande de l'ASA, entrez en mode de configuration globale. En mode de configuration globale, l'ASA affiche cette invite : `hostname(config)#`

Procédure**Étape 1**

Ajoute une stratégie de groupe interne pour Network Client Access (Accès client réseau)

group-policy name internal**Exemple :**

```
hostname (config) # group-policy PostureModuleGroup internal
```

Étape 2

Modifiez la nouvelle stratégie de groupe. Après avoir saisi la commande, vous recevez une invite pour le mode de configuration de la stratégie de groupe, `hostname(config-group-policy)#`.

group-policy name attributes**Exemple :**

```
hostname (config) # group-policy PostureModuleGroup attributes
```

Étape 3 Entrez le mode de configuration webvpn de stratégie de groupe. Après avoir saisi la commande, l'ASA renvoie cette invite : `hostname(config-group-webvpn)#`

webvpn

Étape 4 Configurez la stratégie de groupe pour télécharger les modules de fonctionnalité Secure Client (services client sécurisés) pour tous les utilisateurs du groupe.

AnyConnect modules value *Secure Firewall Module Name*

La valeur de la commande AnyConnect modules peut contenir une ou plusieurs des valeurs suivantes : Lorsque vous spécifiez plusieurs modules, séparez les valeurs par une virgule :

valeur	Secure Firewall Module/Feature Name
dart	Secure Client DART (Diagnostics and Reporting Tool)
vpngina	Secure Client SBL (Start Before Logon)
posture	Secure Firewall Posture/HostScan
nam	Secure Client Network Access Manager
none	Utilisé seul, supprime tous les modules AnyConnect de la stratégie de groupe.
profileMgmt	Secure Client Management Tunnel VPN

Exemple :

```
hostname(config-group-webvpn)# anyconnect modules value websecurity,telemetry,posture
```

Pour supprimer l'un des modules, envoyez de nouveau la commande en précisant uniquement les valeurs du module que vous souhaitez conserver. Par exemple, cette commande supprime le module websecurity :

```
hostname(config-group-webvpn)# anyconnect modules value telemetry,posture
```

Étape 5 Enregistrez la configuration en cours d'exécution dans la mémoire flash.

Après avoir enregistré avec succès la nouvelle configuration dans la mémoire flash, vous recevez le message [OK], puis l'ASA vous renvoie à l'invite `hostname(config-group-webvpn)#`.

write memory

Documentation associée à HostScan/Secure Firewall Posture

Une fois que HostScan/Secure Firewall Posture a collecté les informations de posture sur l'ordinateur terminal, vous devrez comprendre des sujets tels que la configuration des politiques d'accès dynamique et l'utilisation d'expressions LUA pour exploiter ces informations.

Ces sujets sont traités en détail dans les documents suivants : [Guides de configuration de Cisco Adaptive Security Device Manager](#). Consultez également le [guide d'administration de Cisco Secure Client](#) (y compris

AnyConnect) de Cisco pour obtenir plus d'informations sur le fonctionnement de HostScan/Secure Firewall Posture avec Secure Client (services client sécurisés).



CHAPITRE 11

Virtual Tunnel Interface

Ce chapitre décrit comment configurer un tunnel VTI.

- [À propos des Virtual Tunnel Interfaces \(Interfaces de tunnel virtuel\), à la page 279](#)
- [Lignes directrices pour les interfaces Virtual Tunnel Interfaces, à la page 280](#)
- [Créer un tunnel VTI, à la page 283](#)
- [Historique des fonctionnalités de Virtual Tunnel Interface, à la page 292](#)

À propos des Virtual Tunnel Interfaces (Interfaces de tunnel virtuel)

ASA prend en charge une interface logique appelée Virtual Tunnel Interface (VTI). Comme alternative au VPN basé sur les politiques, vous pouvez créer un tunnel VPN entre les homologues à l'aide des VTI. Les VTI prennent en charge le VPN basé sur le routage avec des profils IPsec associés à l'extrémité de chaque tunnel. Vous pouvez utiliser des routes dynamiques ou statiques. Le trafic sortant du VTI est chiffré et envoyé à l'homologue, et la SA associée déchiffre le trafic entrant vers le VTI.

Avec une interface VTI, il n'est plus nécessaire de configurer des listes d'accès aux cartes de chiffrement statiques et de les mapper aux interfaces. Vous n'avez plus à suivre tous les sous-réseaux distants ni à les inclure dans l'ACL de la carte de chiffrement. Les déploiements deviennent plus simples, et le fait de disposer d'une VTI statique qui prend en charge un VPN fondé sur le routage avec un protocole de routage dynamique répond également à de nombreuses exigences d'un nuage privé virtuel.

VTI statique

Vous pouvez utiliser des configurations VTI statiques pour une connectivité de site à site dans laquelle un tunnel est toujours actif entre deux sites. Pour un VTI statique, vous devez définir une interface physique comme source de tunnel. Vous pouvez associer un maximum de 1 024 VTI par périphérique. Pour créer une interface VTI statique, consultez [Ajouter une interface VTI, à la page 287](#).

VTI dynamique

Le VTI dynamique fournit une connectivité hautement sécurisée et évolutive pour les VPN de site à site. Le VTI dynamique facilite la configuration des homologues pour les déploiements en étoile dans les grandes entreprises. Un seul VTI dynamique peut remplacer plusieurs configurations de VTI statique sur le concentrateur. Vous pouvez ajouter de nouveaux satellites à un concentrateur sans modifier la configuration du concentrateur. Le VTI dynamique remplace les cartes de chiffrement dynamiques et la méthode dynamique

en étoile pour établir les tunnels. Dans le centre de gestion, le VTI dynamique prend uniquement en charge la topologie concentrateur-étoile.

Le VTI dynamique utilise un modèle virtuel pour l'instanciation et la gestion dynamiques des interfaces IPsec. Le modèle virtuel génère dynamiquement l'interface d'accès virtuelle qui est unique pour chaque session VPN. Le VTI dynamique prend en charge plusieurs associations de sécurité IPsec et accepte plusieurs sélecteurs IPsec proposés par l'étoile. Le VTI dynamique prend également en charge les sites distants dynamiques DHCP. Pour créer une interface VTI dynamique, consultez [Ajouter une interface VTI dynamique, à la page 290](#).

Comment un ASA crée un tunnel VTI dynamique pour une session VPN

1. Créez un modèle virtuel sur l'ASA (**interface virtual-Template *template_number* type tunnel**).
Vous pouvez utiliser ce modèle pour plusieurs sessions VPN.
2. Associez ce modèle à un groupe de tunnels. Vous pouvez associer un modèle virtuel à plusieurs groupes de tunnels.
3. Le site distant initie une demande de tunnel auprès du concentrateur.
4. Le concentrateur authentifie le site distant.
5. L'ASA utilise le modèle virtuel pour créer dynamiquement une interface d'accès virtuelle sur le concentrateur pour la session VPN avec le site distant.
6. Le concentrateur établit un tunnel VTI dynamique avec le site distant à l'aide de l'interface d'accès virtuelle.
7. Configurez l'option de `ikev2 route set interface` afin d'annoncer l'adresse IP de l'interface VTI au moyen des échanges IKEv2. Cette option permet la joignabilité en monodiffusion entre les interfaces VTI afin que BGP ou la surveillance des chemins fonctionne à travers le tunnel.
8. À la fin de la session VPN, le tunnel se déconnecte et le concentrateur supprime l'interface d'accès virtuelle correspondante.

Lignes directrices pour les interfaces Virtual Tunnel Interfaces

Mode contexte et mise en grappe

- Pris en charge en mode unique uniquement.
- Aucune prise en charge de mise en grappe.

Mode pare-feu

Pris en charge en mode routé uniquement.

Prise en charge de BGP IPv4 et IPv6

Prend en charge le routage BGP IPv4 et IPv6 sur un VTI.

Prise en charge d'EIGRP

Prend en charge le routage EIGRP IPv4 et IPv6 sur un VTI.

Prise en charge d'OSPF IPv4 et IPv6

Prend en charge le routage OSPF IPv4 et IPv6 sur un VTI.

Prise en charge d'IPv6

- Vous pouvez configurer des VTI dotés d'adresses IPv6.
- La source et la destination du tunnel d'un VTI peuvent toutes deux avoir des adresses IPv6.
- Les combinaisons suivantes d'adresse IP de VTI (ou de version IP des réseaux internes) sur des versions d'IP publique sont prises en charge :
 - IPv6 sur IPv6
 - IPv4 sur IPv6
 - IPv4 sur IPv4
 - IPv6 sur IPv4
- Seules les adresses IPv6 statiques sont prises en charge comme source et destination du tunnel.
- L'interface source du tunnel peut avoir des adresses IPv6, et vous pouvez préciser laquelle utiliser comme point de terminaison du tunnel. Si vous ne précisez rien, la première adresse IPv6 globale de la liste est utilisée par défaut comme point de terminaison du tunnel.
- Vous pouvez préciser le mode de tunnel comme IPv6. Lorsque ce mode est précisé, le trafic IPv6 peut être acheminé par tunnel par le VTI. Cependant, pour un même VTI, le mode de tunnel peut être soit IPv4, soit IPv6.

Directives de configuration générale

- Si vous utilisez des cartes de chiffrement dynamiques et des VTI dynamiques dans vos VPN LAN-à-LAN, seuls les tunnels VTI dynamiques seront établis. Ce comportement se produit car les cartes de chiffrement et les VTI dynamiques tentent d'utiliser le groupe de tunnels par défaut.

Nous vous recommandons d'effectuer l'une des opérations suivantes :

- Migrez vos VPN LAN-à-LAN vers des VTI dynamiques.
- Utiliser des cartes de chiffrement statiques avec leurs propres groupes de tunnels.
- Les VTI ne sont configurables qu'en mode IPsec. La terminaison des tunnels GRE sur un ASA n'est pas prise en charge.
- Vous pouvez utiliser des routes IPv4 statiques, BGP, OSPF ou EIGRP pour le trafic qui utilise l'interface de tunnel.
- Pour les VTI statiques et dynamiques, assurez-vous de ne pas utiliser l'interface borrow IP comme adresse IP source du tunnel pour une interface VTI.
- La MTU pour les VTI est définie automatiquement en fonction de l'interface physique sous-jacente. Cependant, si vous modifiez la MTU de l'interface physique après l'activation du VTI, vous devez désactiver et réactiver le VTI pour utiliser le nouveau paramètre de MTU.

- Pour le VTI dynamique, l'interface d'accès virtuel hérite de la MTU de l'interface source du tunnel configurée. Si vous ne précisez pas l'interface source du tunnel, l'interface d'accès virtuel hérite de la MTU de l'interface source sur laquelle l'ASA accepte la demande de session VPN.
- Pour les VTI statiques, vous pouvez configurer un maximum de 1 024 VTI sur un périphérique. Lors du calcul du nombre de VTI, tenez compte des éléments suivants :
 - Incluez les sous-interfaces Nameif pour dériver le nombre total de VTI qui peuvent être configurées sur le périphérique.
 - Vous ne pouvez pas configurer nameif sur les interfaces membres d'un canal de port. Par conséquent, le nombre de tunnels est réduit par le nombre d'interfaces du canal de port principal seulement et non par aucune de ses interfaces membres.
 - Même si une plateforme prend en charge plus de 1 024 interfaces, le nombre de VTI est limité au nombre de VLAN configurables sur cette plateforme. Par exemple, si un modèle prend en charge 500 VLAN, le nombre de tunnels correspond à 500 moins le nombre d'interfaces physiques configurées.
- Pour les VTI dynamiques, le nombre maximal d'interfaces d'accès virtuelles créées dynamiquement peut être de 1 024 ou de la limite totale d'interfaces de la plateforme, selon la valeur la plus faible.
- Le VTI prend en charge les versions IKEv1 et IKEv2 et utilise IPsec pour envoyer et recevoir des données entre la source et la destination du tunnel.
- Si la NAT doit être appliquée, les paquets IKE et ESP sont encapsulés dans l'en-tête UDP.
- Les associations de sécurité IKE et IPsec seront rachetées en permanence, quel que soit le trafic de données dans le tunnel. Cela garantit que les tunnels VTI sont toujours actifs.
- Le nom du groupe de tunnels doit correspondre à ce que l'homologue envoie comme identité IKEv1 ou IKEv2.
- Pour IKEv1 dans les groupes de tunnels site à site, vous pouvez utiliser des noms autres que des adresses IP si la méthode d'authentification du tunnel repose sur des certificats numériques et/ou si l'homologue est configuré en mode agressif.
- Les configurations du VTI et de la carte de chiffrement peuvent coexister sur la même interface physique, à condition que l'adresse homologue configurée dans la carte de chiffrement et la destination du tunnel pour le VTI soient différentes.
- Les règles d'accès peuvent être appliquées sur une interface VTI pour contrôler le trafic via VTI.
- Le ping ICMP est pris en charge entre interfaces VTI.
- Si l'équipement homologue d'un tunnel VPN site à site IKEv2 envoie des charges utiles de requête de configuration IKEv2, l'ASA ne peut pas établir de tunnel IKEv2 avec cet équipement. Vous devez désactiver la requête config-exchange sur l'équipement homologue pour permettre à l'ASA d'établir un tunnel VPN avec celui-ci.
- Les VTI dynamiques prennent en charge la haute disponibilité (HA) et IKEv2.

Paramètres d'usine

- Par défaut, tout le trafic passant par VTI est chiffré.

- Par défaut, le niveau de sécurité pour les interfaces VTI est 0. Ce niveau de sécurité ne peut pas être modifié.

Limitations des VTI

L'ASA rejette les trames et paquets contenant des Security Group Tags (SGT) après le déchiffrement du VTI.

Le VTI dynamique ne prend pas en charge :

- ECMP et VRF
- Mise en grappes
- IKEv1
- Qualité de service

Pour les VTI dynamiques, si aucune source de tunnel n'est spécifiée, IKEv2 est activé sur toutes les interfaces de l'équipement, sauf celles dédiées à la gestion (management-only) et au basculement (failover).

Créer un tunnel VTI

Pour configurer un tunnel VTI, créez une proposition IPsec (ensemble de transformation). Vous devrez créer un profil IPsec qui fait référence à la proposition IPsec, suivi d'une interface VTI à laquelle le profil IPsec est associé. Configurez l'homologue distant avec des paramètres de proposition IPsec et de profil IPsec identiques. La négociation SA commencera lorsque tous les paramètres du tunnel seront configurés.



Remarque

Pour l'ASA qui fait partie des deux domaines VPN VTI et qui présente une contiguïté BGP sur l'interface physique :

Lorsqu'un changement d'état est déclenché en raison de la vérification de l'intégrité de l'interface, les routes de l'interface physique seront supprimées jusqu'à ce que la contiguïté BGP soit rétablie avec le nouvel homologue actif. Ce comportement ne s'applique pas aux interfaces logiques VTI.

Des listes de contrôle d'accès peuvent être appliquées à une interface VTI pour contrôler le trafic qui passe par le VTI. Pour autoriser tous les paquets provenant d'un tunnel IPsec sans vérifier les ACL des interfaces source et destination, saisissez la commande `sysopt connection permit-vpn` en mode de configuration globale.

Vous pouvez utiliser la commande suivante pour autoriser le trafic IPsec à travers l'ASA sans vérifier les ACL :

hostname(config)# sysopt connection permit-vpn

Lorsqu'une interface externe et une interface VTI ont toutes deux un niveau de sécurité de 0, si une ACL est appliquée à l'interface VTI, elle ne sera pas atteinte si `same-security-traffic` n'est pas configuré.

Pour configurer cette fonctionnalité, utilisez la commande **same-security-traffic** en mode de configuration globale avec son argument **intra-interface**.

Pour en savoir plus, consultez [Permettre le trafic intra-interface \(hairpinning\)](#), à la page 72.

Procédure

-
Étape 1	Ajouter une proposition IPsec (ensembles de transformations)
Étape 2	Ajouter un profil IPsec.
Étape 3	Ajouter un tunnel VTI.
-

Ajouter une proposition IPsec (ensembles de transformations)

Un ensemble de transformation est nécessaire pour sécuriser le trafic dans un tunnel VTI. Utilisé comme partie intégrante du profil IPsec, il s'agit d'un ensemble de protocoles et d'algorithmes de sécurité qui protège le trafic du VPN.

Avant de commencer

- Vous pouvez utiliser soit une clé prépartagée, soit des certificats pour authentifier la session IKE associée à un VTI. IKEv2 permet des méthodes d'authentification et des clés dissymétriques. Pour IKEv1 et IKEv2, vous devez configurer la clé prépartagée dans le groupe de tunnels utilisé pour le VTI.
- Pour l'authentification fondée sur des certificats au moyen d'IKEv1, vous devez préciser le point de confiance à utiliser du côté de l'initiateur. Pour le répondeur, vous devez configurer le point de confiance dans la commande tunnel-group. Pour IKEv2, vous devez configurer, dans la commande tunnel-group, le point de confiance à utiliser pour l'authentification, tant pour l'initiateur que pour le répondeur.

Procédure

Ajoutez un ensemble de transformation IKEv1 ou une proposition IPsec IKEv2 pour établir l'association de sécurité.

Ajouter un ensemble de transformation IKEv1 :

crypto ipsec ikev1 transform-set {transform-set-name | chiffrement | authentication}

Exemple :

```
ciscoasa(config)#crypto ipsec ikev1 transform-set SET1 esp-aes esp-sha-hmac
```

Le *chiffrement* spécifie quelle méthode de chiffrement protège les flux de données IPsec :

- esp-aes : utilise AES avec une clé de 128 bits.
- esp-aes-192 : utilise AES avec une clé de 192 bits.
- esp-aes-256 : utilise AES avec une clé de 256 bits.
- esp-null : pas de chiffrement.

L'*authentification* spécifie la méthode d'authentification pour protéger les flux de données IPsec :

- esp-md5-hmac : utilise MD5/HMAC-128 comme algorithme de hachage.

- `esp-sha-hmac` : utilise SHA/HMAC-160 comme algorithme de hachage.
- `esp-none` : aucune authentification HMAC.

Ajouter une proposition IPsec IKEv2.

Remarque

Pour la plateforme IOS, utilisez la commande **no config-exchange request** dans le mode de configuration du profil IKEv2 pour désactiver les options d'échange de configuration. Consultez <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c2.html#wp3456426280> pour de plus amples renseignements.

- Précisez un nom pour la proposition IPsec :

crypto ipsec ikev2 ipsec-proposal *nom de la proposition IPsec*

Exemple :

```
ciscoasa(config)#crypto ipsec ikev2 ipsec-proposal SET1
```

- Précisez les paramètres de sécurité en mode de configuration crypto IPsec ikev2 ipsec-proposal :

protocol esp {encryption {aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | null} | integrity {sha-1 | sha-256 | sha-384 | sha-512 | null}}

Exemple :

```
ciscoasa(config-ipsec-proposal)#protocol esp encryption aes aes-192
```

Ajouter un profil IPsec

Un profil IPsec contient les protocoles et les algorithmes de sécurité requis dans l'ensemble de proposition ou de transformation IPsec auquel il fait référence. Cela garantit un chemin de communication logique et sécurisé entre deux homologues VPN VTI de site à site.

Procédure

Étape 1 Définissez un nom pour le profil :

crypto ipsec profile *nom*

Exemple :

```
ciscoasa(config)#crypto ipsec profile PROFILE1
```

Étape 2 Définissez la proposition IKEv1 ou IKEv2. Vous pouvez choisir un ensemble de transformation IKEv1 ou une proposition IKEv2 IPsec.

a) Définissez l'ensemble de transformation IKEv1.

- Pour définir la proposition IKEv1, saisissez la commande suivante dans le sous-mode de commande `crypto ipsec profile` :

set ikev1 transform set *set_name*

Dans cet exemple, SET1 est l'ensemble de propositions IKEv1 créé précédemment.

```
ciscoasa(config-ipsec-profile)#set ikev1 transform-set SET1
```

b) Définissez la proposition IKEv2.

- Pour définir la proposition IKEv2, saisissez la commande suivante dans le sous-mode de commande de profil crypto ipsec :

```
set ikev2 ipsec-proposal IPsec_proposal_name
```

Dans cet exemple, SET1 est la proposition IKEv2 IPsec créée précédemment.

```
ciscoasa(config-ipsec-profile)#set ikev2 ipsec-proposal SET1
```

Étape 3 (Facultatif) Précisez la durée de l'association de sécurité :

```
set security-association lifetime {seconds number | kilobytes {number | unlimited}}
```

Exemple :

```
ciscoasa(config-ipsec-profile)#set security-association lifetime
seconds 120 kilobytes 10000
```

Étape 4 (Facultatif) Configurez la fin du tunnel VTI pour qu'elle agisse uniquement en tant que répondeur :

responder-only

- Vous pouvez configurer une extrémité du tunnel VTI pour qu'elle fonctionne uniquement en tant que répondeur. L'extrémité configurée en mode répondeur uniquement n'initie ni le tunnel ni le renouvellement de clés.
- Si vous utilisez IKEv2, définissez une durée de vie de l'association de sécurité supérieure à la valeur de durée de vie définie dans le profil IPsec à l'extrémité initiatrice. Cela vise à faciliter un renouvellement de clés réussi par l'extrémité initiatrice et à garantir que les tunnels restent opérationnels.
- Si vous utilisez IKEv1, IOS doit toujours être en mode de répondeur uniquement, car IOS ne prend pas en charge le mode de canal continu. L'ASA devient l'initiateur de la session et du renouvellement de clés.
- Si la configuration du renouvellement de clés à l'extrémité initiatrice est inconnue, supprimez le mode répondeur uniquement afin de rendre l'établissement de la SA bidirectionnel, ou configurez une durée de vie IPsec infinie à l'extrémité en mode répondeur uniquement afin d'éviter l'expiration.

Étape 5 (Facultatif) Précisez le groupe de PFS. La confidentialité de transmission parfaite (PFS) génère une clé de session unique pour chaque échange chiffré. Cette clé de session unique protège l'échange contre tout déchiffrement ultérieur. Pour configurer PFS, vous devez sélectionner l'algorithme de dérivation de clé Diffie-Hellman à utiliser lors de la génération de la clé de session PFS. Les algorithmes de dérivation de clé génèrent des clés d'association de sécurité IPsec. Chaque groupe a un module de taille différent. Un module plus élevé offre une sécurité élevée, mais nécessite plus de temps de traitement. Vous devez avoir des groupes Diffie-Hellman correspondants sur les deux homologues.

```
set pfs { group14 }
```

Exemple :

```
ciscoasa(config-ipsec-profile)# set pfs group14
```

Étape 6 (Facultatif) Précisez un point de confiance qui définit le certificat à utiliser lors de l'initialisation d'une connexion de tunnel VTI.

set trustpoint *nom*

Exemple :

```
ciscoasa(config-ipsec-profile)#set trustpoint TPVTI
```

Étape 7 (Facultatif) Activez l'injection de route inverse (RRI) pour ce profil IPsec et définissez la route inverse comme dynamique.

set reverse-route [*dynamique*]

Exemple :

```
ciscoasa(config-ipsec-profile)#set reverse-route dynamic
```

Ajouter une interface VTI

Pour créer une nouvelle interface VTI et établir un tunnel VTI, procédez comme suit :



Remarque

Implémentez l'IP SLA pour vous assurer que le tunnel reste opérationnel lorsqu'un routeur dans le tunnel actif n'est pas disponible. Consultez la section Configurer le suivi de route statique dans le Guide de configuration des opérations générales ASA dans <http://www.cisco.com/go/asa-config>.

Procédure

- Étape 1** Créez une nouvelle interface de tunnel :
- interface tunnel** *tunnel_interface_number*
- Précisez un ID de tunnel, dans une plage de 0 à 10 413. Jusqu'à 10 413 interfaces VTI sont prises en charge.
- Exemple :**
- ```
ciscoasa(config)#interface tunnel 100
```
- Étape 2** Saisissez le nom de l'interface VTI.
- Saisissez la commande suivante dans le sous-mode de commande **interface tunnel** :
- nameif** *interface name*
- Exemple :**
- ```
ciscoasa(config-if)#nameif vti
```
- Étape 3** Saisissez l'adresse IP de l'interface VTI.
- ip address** *IP address mask*
- Exemple :**
- ```
ciscoasa(config-if)#ip address 192.168.1.10 255.255.255.254
```
- Étape 4** Saisissez une adresse IPv4 ou IPv6 pour une interface dont hérite le modèle virtuel.

Vous pouvez choisir n'importe quelle interface physique ou une adresse de boucle avec retour configurée sur le périphérique. Toutes les interfaces d'accès virtuelles clonées à partir du modèle virtuel auront la même adresse IP.

**ip unnumbered** *interface-name*

**ipv6 unnumbered** *interface-name*

**Exemple :**

```
ciscoasa(config-if)#ip unnumbered loopback1
```

**Étape 5** Spécifiez l'interface source du tunnel.

**tunnel source interface** *interface\_name*

L'interface source peut être une interface physique ou une interface de boucle.

**Exemple :**

```
ciscoasa(config-if)#tunnel source interface outside
```

**Étape 6** Spécifiez l'adresse IP de destination du tunnel.

**tunnel destination** *ip\_address*

**Exemple :**

```
ciscoasa(config-if)#tunnel destination 10.1.1.1
```

**Étape 7** Configurez le tunnel avec le mode tunnel IPsec IPv4.

**tunnel mode ipsec** *ipv4*

**Exemple :**

```
ciscoasa(config-if)#tunnel mode ipsec ipv4
```

**Étape 8** Attribuez le profil IPsec au tunnel.

**tunnel protection ipsec** *IPsec profile*

**Exemple :**

```
ciscoasa(config-if)#tunnel protection ipsec Profile1
```

**Étape 9** Attribuez un sélecteur de trafic pour l'interface VTI statique.

**tunnel protection policy** *acl\_name*

La liste d'accès peut contenir un ou plusieurs sélecteurs de liste. Si vous ne configurez pas cette commande, l'interface VTI statique propose des sélecteurs any-any, ce qui est le comportement par défaut.

**Exemple :**

```
ciscoasa(config)# access-list Spoke-to-Hub extended permit ip 209.165.200.225 255.255.255.224 any
ciscoasa(config-if)# tunnel protection ipsec policy Spoke-to-Hub
```

---

**Exemple**

Exemple de configuration d'un tunnel VTI (avec IKEv2) entre l'ASA et un périphérique IOS :



ASA :

```
crypto ikev2 policy 1
 encryption aes-gcm-256
 integrity null
 group 21
 prf sha512
 lifetime seconds 86400
!
crypto ipsec ikev2 ipsec-proposal gcm256
 protocol esp encryption aes-gcm-256
 protocol esp integrity null
!
crypto ipsec profile asa-vti
 set ikev2 ipsec-proposal gcm256
!
interface Tunnel 100
 nameif vti
 ip address 10.10.10.1 255.255.255.254
 tunnel source interface [asa-source-nameif]
 tunnel destination [router-ip-address]
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile asa-vti
!
tunnel-group [router-ip-address] ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
!
crypto ikev2 enable [asa-interface-name]
```

IOS :

```
!
crypto ikev2 proposal asa-vti
 encryption aes-gcm-256
 prf sha512
 group 21
!
crypto ikev2 policy asa-vti
 match address local [router-ip-address]
 proposal asa-vti
!
crypto ikev2 profile asa-vti
 match identity remote address [asa-ip-address] 255.255.255.255
 authentication local pre-share key cisco
 authentication remote pre-share key cisco
 no config-exchange request
!
crypto ipsec transform-set gcm256 esp-gcm 256
!
crypto ipsec profile asa-vti
 set ikev2-profile asa-vti
 set transform-set gcm256
!
interface tunnel 100
```

```
ip address 10.10.10.0 255.255.255.254
tunnel mode ipsec ipv4
tunnel source [router-interface]
tunnel destination [asa-ip-address]
tunnel protection ipsec profile asa-vti
!
```

## Ajouter une interface VTI dynamique

Pour créer un modèle virtuel pour le VTI dynamique :



### Remarque

Implémentez l'IP SLA pour vous assurer que le tunnel reste opérationnel lorsqu'un routeur dans le tunnel actif n'est pas disponible. Consultez « Configure Static Route Tracking » (Configurer le suivi de route statique) dans le Guide de configuration des opérations générales ASA dans <http://www.cisco.com/go/asa-config>.

### Avant de commencer

Assurez-vous d'avoir configuré un profil IPsec et une interface IP non numérotée.

### Procédure

#### Étape 1

Créez un nouveau modèle virtuel :

**interface virtual-Template** *template\_number* **type tunnel**

*template\_number* est le numéro unique du modèle virtuel. La plage est comprise entre 1 et 10 413.

Le modèle d'interface ne doit pas être à l'état d'arrêt. Voici les paramètres obligatoires pour le modèle virtuel :

- Nom d'interface
- Mode de tunnel IPsec
- Profil IPsec du tunnel

#### Exemple :

```
ciscoasa(config)#interface virtual-Template 101 type tunnel
```

#### Étape 2

Précisez le nom de l'interface de modèle virtuel VTI dynamique.

Saisissez la commande suivante en mode de configuration **interface** :

**nameif** *interface\_name*

L'ASA crée dynamiquement des interfaces d'accès virtuelles en tant que *<Virtual\_Template\_name>\_va<n>*. Par exemple, si le nom du modèle virtuel est dVTI101, les interfaces d'accès virtuelles seront dVTI101\_va1, dVTI101\_va2, etc. Si vous souhaitez modifier un modèle virtuel, vous devez l'arrêter à l'aide de la commande **shutdown**.

#### Exemple :

```
ciscoasa(config-if)#nameif dVTI101
```

**Étape 3** Configurez une adresse IPv4 ou IPv6 d'une interface dont le modèle virtuel hérite.

**ip unnumbered** *interface-name*

**ipv6 unnumbered** *interface-name*

Le modèle virtuel peut hériter de l'adresse IP de n'importe quelle interface physique ou d'une adresse de boucle configurée sur le périphérique. Toutes les interfaces d'accès virtuelles clonées à partir du modèle virtuel auront la même adresse IP.

**Exemple :**

```
ciscoasa(config-if)#ip unnumbered loopback1
```

**Étape 4** (Facultatif) Précisez l'interface source du tunnel.

**tunnel source interface** *interface\_name*

L'interface source peut être une interface physique ou une interface de boucle.

L'ASA accepte les demandes de session VPN uniquement de l'interface configurée comme adresse IP source du tunnel. Si vous ne spécifiez pas cette interface, l'ASA accepte les demandes de session VPN reçues de n'importe quelle interface. L'interface d'accès virtuel hérite de la MTU de l'interface source du tunnel configurée. Si vous n'activez pas l'option ci-dessus, l'interface d'accès virtuel hérite de la MTU de l'interface source de laquelle l'ASA accepte la demande de session VPN.

**Exemple :**

```
ciscoasa(config-if)#tunnel source interface outside1
```

**Étape 5** Précisez le mode de protection du tunnel comme IPv4 ou IPv6.

**tunnel mode ipsec** {*ipv4* | *ipv6*}

**Exemple :**

```
ciscoasa(config-if)#tunnel mode ipsec ipv4
```

**Étape 6** Attribuez un profil IPsec au tunnel.

**tunnel protection ipsec profile** *ipsec\_profile*

Ce profil IPsec configure les paramètres IPsec/IKE requis pour négocier l'échange.

**Exemple :**

```
ciscoasa(config-if)#tunnel protection ipsec profile Profile1
```

**Étape 7** Associez le modèle virtuel à un groupe de tunnels.

**tunnel-group** *tunnel\_group\_name* **type** *type*

**tunnel-group** *tunnel\_group\_name* **ipsec-attributes**

**virtual-template** *template\_number*

Vous pouvez associer le même modèle virtuel à plusieurs groupes de tunnels. L'ASA utilise le modèle virtuel pour créer des interfaces d'accès virtuelles individuelles pour chaque session VPN.

**Exemple :**

```
ciscoasa(config)#tunnel-group DVTI_spoke1 type ipsec-l2l
ciscoasa(config)#tunnel-group DVTI_spoke1 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#virtual-template 101
```

**Étape 8** Activez le routage dynamique pour le groupe de tunnels.

**tunnel-group** *tunnel\_group\_name* **ipsec-attributes**

**ikev2 route accept any**

**ikev2 route set interface**

La commande **ikev2 route accept any** permet à l'ASA d'accepter toutes les adresses IP d'interface de tunnel reçues lors des échanges IKEv2. Par défaut, cette option est activée.

La commande **ikev2 route set interface** permet à l'ASA d'envoyer l'adresse IP de l'interface du tunnel pendant les échanges IKEv2. Cette option permet la connectivité en monodiffusion entre les interfaces VTI pour que BGP fonctionne sur le tunnel.

Le routage dynamique est activé pour les groupes de tunnels à l'aide de BGP/OSPF/EIGRP. Après avoir configuré le modèle virtuel, vous devez configurer une politique de routage pour acheminer le trafic VTI dynamique entre les périphériques sur le tunnel VTI. Vous devez également configurer une règle de contrôle d'accès pour autoriser le trafic chiffré.

**Exemple :**

```
ciscoasa(config)#tunnel-group DVTI_spoke1 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#ikev2 route set interface
ciscoasa(config-tunnel-ipsec)#ikev2 route accept any
```

## Historique des fonctionnalités de Virtual Tunnel Interface

| Nom de la caractéristique                                                    | Versions | Renseignements sur les fonctionnalités                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prise en charge de Dynamic Virtual Tunnel Interface                          | 9.19(1)  | Vous pouvez créer un VTI dynamique et l'utiliser pour configurer un VPN de site à site basé sur le routage dans une topologie en étoile. Le VTI dynamique facilite la configuration des homologues pour les déploiements en étoile dans les grandes entreprises. Un seul VTI dynamique peut remplacer plusieurs configurations de VTI statique sur le concentrateur. Vous pouvez ajouter de nouveaux satellites à un concentrateur sans modifier la configuration du concentrateur.<br><br>Commandes nouvelles/modifiées : <b>interface virtual-Template, ip unnumbered, ipv6 unnumbered, tunnel protection ipsec policy</b> |
| Prise en charge du routage OSPF IPv4 et IPv6                                 | 9.19(1)  | Prend en charge le protocole de routage OSPF IPv4 et IPv6 sur un VTI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Prise en charge d'EIGRP                                                      | 9.19(1)  | Prend en charge le protocole de routage EIGRP IPv4 et IPv6 sur un VTI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Prise en charge de l'interface loopback pour les VTI statiques et dynamiques | 9.19(1)  | Vous pouvez désormais définir une interface de bouclage comme interface source pour un VTI. La possibilité d'hériter de l'adresse IP d'une interface de bouclage au lieu d'une adresse IP configurée de manière statique a également été ajoutée. L'interface de boucle avec retour permet de résoudre les échecs de chemin. Si une interface tombe en panne, vous pouvez accéder à toutes les interfaces grâce à l'adresse IP attribuée à l'interface de boucle avec retour.<br><br>Commandes nouvelles/modifiées : <b>tunnel source interface, ip unnumbered, ipv6 unnumbered</b>                                          |

| Nom de la caractéristique                                                          | Versions | Renseignements sur les fonctionnalités                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prise en charge de l'ID de tunnel local                                            | 9.17(1)  | <p>L'ASA prend en charge un ID de tunnel local unique qui permet à l'ASA d'avoir plusieurs tunnels IPsec derrière une NAT pour se connecter à Cisco Umbrella Secure Internet Gateway (SIG). L'identité locale est utilisée pour configurer une identité unique par tunnel IKEv2, au lieu d'une identité globale pour tous les tunnels.</p> <p>Commandes nouvelles ou modifiées : <b>local-identity-from-cryptomap</b></p>                                                                                                                                                                                                                                                                                                                                                                           |
| Prise en charge d'IPv6 sur VTI statique                                            | 9.16(1)  | <p>L'ASA prend en charge les adresses IPv6 dans les configurations Virtual Tunnel Interfaces (VTI).</p> <p>Une interface source de tunnel VTI peut avoir une adresse IPv6, que vous pouvez configurer pour l'utiliser comme terminal du tunnel. Si l'interface source du tunnel a plusieurs adresses IPv6, vous pouvez spécifier l'adresse à utiliser, sinon la première adresse globale IPv6 de la liste est utilisée par défaut.</p> <p>Le mode du tunnel peut être IPv4 ou IPv6, mais il doit être identique au type d'adresse IP configuré sur VTI pour que le tunnel soit actif. Une adresse IPv6 peut être attribuée à l'interface source ou de destination du tunnel dans un VTI.</p> <p>Commandes nouvelles/modifiées : <b>tunnel source interface, tunnel destination, tunnel mode</b></p> |
| Prise en charge de 1024 interfaces VTI par périphérique                            | 9.16(1)  | <p>Le nombre de VTI maximum à configurer sur un périphérique est passé de 100 à 1 024.</p> <p>Même si une plateforme prend en charge plus de 1 024 interfaces, le nombre de VTI est limité au nombre de VLAN configurables sur cette plateforme. Par exemple, l'ASA 5510 prend en charge 100 VLAN, le nombre de tunnels serait donc de 100 moins le nombre d'interfaces physiques configurées.</p> <p>Commandes nouvelles ou modifiées : aucune</p>                                                                                                                                                                                                                                                                                                                                                 |
| Prise en charge du serveur relais DHCP sur VTI                                     | 9.14(1)  | <p>L'ASA permet de configurer les interfaces VTI comme interfaces de connexion du serveur relais DHCP.</p> <p>Nous avons modifié les commandes suivantes : <b>dhcprelay server ip_address vti_ifc_name</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Prise en charge d'IKEv2, de l'authentification par certificat et de l'ACL dans VTI | 9.8(1)   | <p>Virtual Tunnel Interface (VTI) prend désormais en charge BGP (VTI statique). Vous pouvez désormais utiliser IKEv2 en modes autonome et à haute disponibilité. Vous pouvez utiliser l'authentification par certificat en configurant un point de confiance dans le profil IPsec. Vous pouvez également appliquer des listes d'accès sur le VTI à l'aide des commandes access-group pour filtrer le trafic d'entrée.</p> <p>Nous avons introduit la commande suivante dans le mode de configuration du profil IPsec : <b>set trustpoint</b>.</p>                                                                                                                                                                                                                                                   |
| Prise en charge de l'interface de tunnel virtuel (VTI)                             | 9.7(1)   | <p>L'ASA est enrichi d'une nouvelle interface logique appelée Virtual Tunnel Interface (VTI), utilisée pour représenter un tunnel VPN vers un homologue. Ces interfaces prennent en charge le VPN basé sur le routage avec des profils IPsec associés à chaque extrémité du tunnel. Avec une interface VTI, vous n'avez plus besoin de configurer des listes d'accès aux cartes de chiffrement statiques et de les mapper aux interfaces.</p> <p>Nous avons introduit les commandes suivantes : <b>crypto ipsec profile, interface tunnel, responder-only, set ikev1 transform-set, set pfs, set security-association lifetime, tunnel destination, tunnel mode ipsec, tunnel protection ipsec profile, tunnel source interface</b>.</p>                                                            |





## CHAPITRE 12

# Configurer un serveur AAA externe pour le VPN

- À propos des serveurs AAA externes, à la page 295
- Lignes directrices relatives à l'utilisation de serveurs AAA externes, à la page 296
- Configurer l'authentification de plusieurs certificats, à la page 296
- Configurer l'autorisation avec LDAP pour le VPN, à la page 298
- Exemples d'autorisation d'accès à distance Active Directory/LDAP, à la page 313

## À propos des serveurs AAA externes

Cet ASA peut être configuré pour utiliser un serveur LDAP, RADIUS ou TACACS+ externe afin de prendre en charge l'authentification, l'autorisation et la comptabilité (AAA) pour l'ASA. Le serveur AAA externe applique les autorisations et les attributs configurés. Avant de configurer l'ASA pour utiliser un serveur externe, vous devez configurer le serveur AAA externe avec les attributs d'autorisation ASA appropriés et, à partir d'un sous-ensemble de ces attributs, attribuer des autorisations spécifiques aux utilisateurs individuels.

## Comprendre l'application des politiques aux attributs d'autorisation

L'ASA prend en charge plusieurs méthodes d'application des attributs d'autorisation d'utilisateur, également appelés droits ou autorisations d'utilisateur, aux connexions VPN. Vous pouvez configurer l'ASA pour obtenir les attributs utilisateur de n'importe quelle combinaison de :

- une politique d'accès dynamique (DAP) sur l'ASA
- un serveur d'authentification et/ou d'autorisation RADIUS ou LDAP externe
- une stratégie de groupe sur l'ASA

Si l'ASA reçoit des attributs de toutes les sources, les attributs sont évalués, fusionnés et appliqués à la politique d'utilisateur. En cas de conflit entre les attributs, les attributs du DAP prévalent.

L'ASA applique les attributs dans l'ordre suivant :

1. Attributs DAP sur l'ASA : introduits dans la version 8.0(2), ces attributs prévalent sur tous les autres. Si vous définissez un signet ou une liste d'URL dans DAP, il remplace un signet ou une liste d'URL définis dans la stratégie de groupe.
2. Attributs de l'utilisateur sur le serveur AAA externe : le serveur renvoie ces attributs une fois l'authentification ou l'autorisation de l'utilisateur réussie. Ne les confondez pas avec les attributs définis

pour les utilisateurs individuels dans la base de données AAA locale sur l'ASA (comptes d'utilisateurs dans ASDM).

3. Stratégie de groupe configurée sur l'ASA : si un serveur RADIUS renvoie la valeur de l'attribut de classe RADIUS IETF-Class-25 (*OU=group-policy*) pour l'utilisateur, l'ASA place l'utilisateur dans la stratégie de groupe du même nom et applique les attributs de la stratégie de groupe qui ne sont pas renvoyés par le serveur.

Pour les serveurs LDAP, n'importe quel nom d'attribut peut être utilisé pour définir la stratégie de groupe pour la session. La carte d'attributs LDAP que vous configurez sur l'ASA associe l'attribut LDAP à l'attribut Cisco IETF-Radius-Class.

4. Stratégie de groupe affectée par le profil de connexion (appelé *tunnel-group* dans le CLI) : le profil de connexion contient les paramètres préliminaires pour la connexion et comprend une stratégie de groupe par défaut appliquée à l'utilisateur avant l'authentification. Tous les utilisateurs se connectant à l'ASA appartiennent initialement à ce groupe, qui fournit tous les attributs manquants dans le DAP, les attributs utilisateur renvoyés par le serveur, ou la stratégie de groupe attribuée à l'utilisateur.
5. Stratégie de groupe par défaut (*DfltGrpPolicy*) : les attributs par défaut du système fournissent les valeurs manquantes dans le DAP, les attributs d'utilisateur, la stratégie de groupe, ou le profil de connexion.

## Lignes directrices relatives à l'utilisation de serveurs AAA externes

Les ASA appliquent les attributs LDAP en fonction du nom de l'attribut, et non de l'ID numérique. Les attributs RADIUS sont appliqués par ID numérique, et non par nom.

Pour ASDM version 7.0, les attributs LDAP comprennent le préfixe *cVPN3000*. Pour les versions 7.1 et ultérieures d'ASDM, ce préfixe a été supprimé.

Les attributs LDAP sont un sous-ensemble des attributs Radius, qui sont répertoriés dans le chapitre Radius.

## Configurer l'authentification de plusieurs certificats

Vous pouvez désormais valider plusieurs certificats par session au moyen des protocoles client Secure Client (services client sécurisés) SSL et IKEv2. Par exemple, vous pouvez vous assurer que le nom d'émetteur du certificat de machine correspond à une autorité de certification particulière et, par conséquent, que le périphérique est un périphérique émis par l'entreprise.

L'option de certificats multiples permet l'authentification de certificat de la machine et de l'utilisateur au moyen de certificats. Sans cette option, vous ne pourriez authentifier par certificat que la machine ou l'utilisateur, mais pas les deux.



### Remarque

Étant donné que l'authentification par certificats multiples nécessite un certificat d'ordinateur et un certificat utilisateur (ou deux certificats utilisateur), vous ne pouvez pas utiliser le démarrage Secure Client (services client sécurisés) avant la connexion (SBL) avec cette fonctionnalité.



L'option de préremplissage du nom d'utilisateur permet d'analyser un champ du deuxième certificat (utilisateur) et de l'utiliser pour l'authentification AAA subséquente dans une connexion authentifiée par AAA et certificat. Le nom d'utilisateur, pour le préremplissage principal comme secondaire, est toujours extrait du deuxième certificat (utilisateur) reçu du client.

À partir de la version 9.14(1), l'ASA vous permet de préciser de quel certificat doivent provenir les noms d'utilisateur principal et secondaire lors de la configuration de l'authentification à certificats multiples et de l'utilisation de l'option de préremplissage du nom d'utilisateur pour l'authentification ou l'autorisation. Pour plus de renseignements, consultez [Configurer plusieurs noms d'utilisateur de certificat, à la page 297](#)

Avec l'authentification par certificats multiples, deux certificats sont authentifiés : le deuxième certificat (utilisateur) reçu du client est celui à partir duquel sont analysés les noms d'utilisateur principal et secondaire de pre-fill et de username-from-certificate.

Vous pouvez également configurer l'authentification par certificats multiples avec SAML.

Les attributs d'authentification webvpn existants sont modifiés pour inclure une option d'authentification à certificats multiples :

```
tunnel-group <name> webvpn-attributes
authentication {aaa [certificate | multiple-certificate] | multiple-certificate [aaa | saml]
 | saml [certificate | multiple-certificate]}
```

Avec l'authentification à certificats multiples, vous pouvez prendre des décisions de politique en fonction des champs d'un certificat utilisé pour authentifier cette tentative de connexion. Les certificats utilisateur et machine reçus du client lors de l'authentification à certificats multiples sont chargés dans DAP afin de permettre la configuration de politiques fondées sur les champs du certificat. Pour ajouter l'authentification par certificats multiples à l'aide des Dynamic Access Policies (DAP) afin de pouvoir définir des règles pour autoriser ou refuser les tentatives de connexion, consultez la section *Ajouter plusieurs certificats d'authentification à DAP* dans la version appropriée du [Guide de configuration ASDM du VPN ASA](#).

## Configurer plusieurs noms d'utilisateur de certificat

Une nouvelle commande a été introduite dans l'ASA 9.14(1) pour configurer le certificat que l'ASA doit utiliser comme nom d'utilisateur principal et secondaire pour l'authentification ou l'autorisation. Vous pouvez préciser s'il faut utiliser le certificat machine envoyé en SSL ou en IKE (premier certificat) ou le certificat utilisateur envoyé par le client (deuxième certificat) pour obtenir les paramètres d'authentification et d'autorisation. Cette option est disponible et peut être configurée pour tous les groupes de tunnels, quel que soit le type d'authentification (**aaa**, **certificat** ou **certificat multiple (multiple-certificate)**). Cependant, la configuration ne prend effet que pour l'authentification par certificats multiples (**multi-certificat (multiple-certificate)** ou **aaa authentification de certificats multiples (aaa multiple-certificate)**). Lorsque l'option n'est pas utilisée pour l'authentification de plusieurs certificats, le deuxième certificat est utilisé par défaut pour l'authentification ou l'autorisation.

### Procédure

- 
- Étape 1** Précisez s'il faut utiliser le nom d'utilisateur principal du premier ou du deuxième certificat :
- username-from-certificate-choice {first-certificate | second-certificate}**
- Étape 2** Précisez s'il faut utiliser le nom d'utilisateur secondaire du premier ou du deuxième certificat :
- secondary-username-from-certificate-choice {first-certificate | second-certificate}**

**Exemple :**

```
tunnel-group tgl webvpn-attributes
authentication aaa multiple-certificate
pre-fill-username client
secondary-pre-fill-username client
tunnel-group tgl type remote-access
tunnel-group tgl general-attributes
secondary-authentication-server-group LOCAL
username-from-certificate-choice first-certificate
secondary-username-from-certificate-choice first-certificate
```

## Configurer l'autorisation avec LDAP pour le VPN

Lorsque l'authentification de l'utilisateur LDAP pour l'accès VPN a réussi, l'ASA interroge le serveur LDAP, qui renvoie les attributs LDAP. Ces attributs comprennent généralement des données d'autorisation qui s'appliquent à la session VPN.

Il peut arriver que vous ayez besoin de l'autorisation d'un serveur de répertoire LDAP distinct du mécanisme d'authentification. Par exemple, si vous utilisez un serveur SDI ou de certificat pour l'authentification, aucune information d'autorisation n'est renvoyée. Pour les autorisations d'utilisateur dans ce cas, vous pouvez interroger un répertoire LDAP après une authentification réussie, ce qui effectue l'authentification et l'autorisation en deux étapes.

Pour configurer l'autorisation d'utilisateur du VPN à l'aide de LDAP, procédez comme suit.

**Procédure****Étape 1**

Créez un groupe de serveurs AAA.

```
aaa-server server_group protocol {kerberos | ldap | nt | radius | sdi | tacacs+}
```

**Exemple :**

```
hostname(config)# aaa-server servergroup1 protocol ldap
hostname(config-aaa-server-group)
```

**Étape 2**

Créez un groupe de tunnels d'accès à distance IPsec nommé remotegrp.

```
tunnel-group groupname
```

**Exemple :**

```
hostname(config)# tunnel-group remotegrp
```

**Étape 3**

Associez le groupe de serveurs et le groupe de tunnels.

```
tunnel-group groupname general-attributes
```

**Exemple :**

```
hostname(config)# tunnel-group remotegrp general-attributes
```

#### Étape 4

Affecte un nouveau groupe de tunnels à un groupe de serveurs AAA précédemment créé pour l'autorisation.  
***authorization-server-group group-tag***

**Exemple :**

```
hostname(config-general)# authorization-server-group ldap_dir_1
```

#### Exemple

L'exemple suivant montre les commandes pour activer l'autorisation utilisateur avec LDAP. L'exemple crée ensuite un groupe de tunnels d'accès à distance IPsec nommé RAVPN et affecte ce nouveau groupe de tunnels au groupe de serveurs AAA LDAP précédemment créé pour l'autorisation :

```
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# authorization-server-group (inside) LDAP
hostname(config-general)#
```

Après avoir terminé ce travail de configuration, vous pouvez configurer des paramètres d'autorisation LDAP supplémentaires tels que un mot de passe de répertoire, un point de départ pour la recherche dans un répertoire et la portée d'une recherche dans le répertoire en saisissant les commandes suivantes :

```
hostname(config)# aaa-server LDAP protocol ldap
hostname(config-aaa-server-group)# aaa-server LDAP (inside) host 10.0.2.128
hostname(config-aaa-server-host)# ldap-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-group-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-login-dn AD\cisco
hostname(config-aaa-server-host)# ldap-login-password cisco123
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)# server-type microsoft
```

## Définir la configuration LDAP ASA

Cette section décrit comment définir la syntaxe de l'attribut LDAP AV-pair et comprend les renseignements suivants :

- [Attributs Cisco pris en charge pour l'autorisation LDAP, à la page 300](#)
- [Syntaxe des attributs AV Pair Cisco, à la page 311](#)
- [Exemples d'ACL à l'aide de paires Cisco-AV, à la page 312](#)

**Remarque**

L'ASA applique les attributs LDAP en fonction du nom de l'attribut, et non de l'ID numérique. Les attributs RADIUS, en revanche, sont appliqués selon l'ID numérique, et non selon le nom.

L'autorisation désigne le processus d'application d'autorisations ou d'attributs. Un serveur LDAP défini comme serveur d'authentification ou d'autorisation applique les autorisations ou les attributs s'ils sont configurés.

Pour ASA Version 7.0, les attributs LDAP comprennent le préfixe cVPN3000. Pour les versions logicielles 7.1 et ultérieures, ce préfixe a été supprimé.

## Attributs Cisco pris en charge pour l'autorisation LDAP

Cette section fournit une liste complète des attributs (voir ) pour les ASA 5500, les concentrateurs VPN 3000 et les PIX série 500. Le tableau comprend des renseignements sur la prise en charge d'attributs pour le concentrateur VPN 3000 et les PIX série 500 afin de vous aider à configurer les réseaux avec une combinaison de ces périphériques.

**Tableau 15 : Attributs Cisco pris en charge par l'ASA pour l'autorisation LDAP**

| Nom de l'attribut                               | VPN 3000 | ASA | PIX | Syntaxe/Type  | Valeur unique ou valeurs multiples | Valeurs possibles                                                                                  |
|-------------------------------------------------|----------|-----|-----|---------------|------------------------------------|----------------------------------------------------------------------------------------------------|
| Heures d'accès                                  | O        | O   | O   | Chaîne        | Unique                             | Nom de la plage temporelle (par exemple, heures de travail)                                        |
| Autoriser le mode d'extension de réseau         | O        | O   | O   | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                                        |
| Délai d'expiration de l'utilisateur authentifié | O        | O   | O   | nombre entier | Unique                             | 1 à 35 791 394 minutes                                                                             |
| Authorization-Required                          | O        |     |     | nombre entier | Unique                             | 0 = Non<br>1 = Oui                                                                                 |
| Authorization-Type                              | O        |     |     | nombre entier | Unique                             | 0 = Aucun<br>1 = RADIUS<br>2 = LDAP                                                                |
| Banner1                                         | O        | O   | O   | Chaîne        | Unique                             | Chaîne de bannière pour les clients VPN SSL sans client, les clients VPN SSL et les clients IPsec. |
| Banner2                                         | O        | O   | O   | Chaîne        | Unique                             | Chaîne de bannière pour les clients VPN SSL sans client, les clients VPN SSL et les clients IPsec. |

| Nom de l'attribut                   | VPN 3000 | ASA | PIX | Syntaxe/Type  | Valeur unique ou valeurs multiples | Valeurs possibles                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------|----------|-----|-----|---------------|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco-AV-Pair                       | O        | O   | O   | Chaîne        | Multi                              | Une chaîne d'octets au format suivant :<br>[Préfixe] [Action] [Protocole] [Source]<br>[Masque générique de la source]<br>[Destination] [Masque générique de la destination] [Établi] [Log] [Opérateur]<br>[Port]<br><br>Pour en savoir plus, consultez la section <a href="#">Syntaxe des attributs de paires Cisco-AV</a> .                                                                      |
| Cisco-IP-Phone-Bypass               | O        | O   | O   | nombre entier | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                                                                                                                                                                                                                                                       |
| Cisco-LEAP-Bypass                   | O        | O   | O   | nombre entier | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                                                                                                                                                                                                                                                       |
| Client-Intercept-DHCP-Configure-Msg | O        | O   | O   | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                                                                                                                                                                                                                                                       |
| Client-Type-Version-Limiting        | O        | O   | O   | Chaîne        | Unique                             | Chaîne du numéro de version du client VPN IPsec                                                                                                                                                                                                                                                                                                                                                   |
| Intervalle de confiance             | O        | O   | O   | nombre entier | Unique                             | 10 - 300 secondes                                                                                                                                                                                                                                                                                                                                                                                 |
| DHCP-Network-Scope                  | O        | O   | O   | Chaîne        | Unique                             | Adresse IP                                                                                                                                                                                                                                                                                                                                                                                        |
| Champ DN                            | O        | O   | O   | Chaîne        | Unique                             | Valeurs possibles : UID, OU, O, CN, L, SP, C, EA, T, N, GN, SN, I, GENQ, DNQ, SER et use-entire-name.                                                                                                                                                                                                                                                                                             |
| Firewall-ACL-In                     |          | O   | O   | Chaîne        | Unique                             | ID de la liste d'accès                                                                                                                                                                                                                                                                                                                                                                            |
| Firewall-ACL-Out                    |          | O   | O   | Chaîne        | Unique                             | ID de la liste d'accès                                                                                                                                                                                                                                                                                                                                                                            |
| Politique de groupe                 |          | O   | O   | Chaîne        | Unique                             | Définit la politique de groupe pour la session VPN d'accès à distance. Pour les versions 8.2 et ultérieures, utilisez cet attribut au lieu de IETF-Radius-Class. Vous pouvez utiliser l'un des formats suivants : <ul style="list-style-type: none"> <li>• nom de la stratégie de groupe</li> <li>• OU = nom de la stratégie de groupe</li> <li>• OU = nom de la stratégie de groupe :</li> </ul> |

| Nom de l'attribut             | VPN 3000 | ASA | PIX | Syntaxe/Type  | Valeur unique ou valeurs multiples | Valeurs possibles                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------|----------|-----|-----|---------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IE-Proxy-Bypass-Local         |          |     |     | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                                                                                                                                                                                                                                                                  |
| IE-Proxy-Exception-List       |          |     |     | Chaîne        | Unique                             | Une liste des domaines DNS. Les entrées doivent être séparées par la séquence de nouvelle ligne (\n).                                                                                                                                                                                                                                                                                                        |
| IE-Proxy-Method               | O        | O   | O   | nombre entier | Unique                             | 1 = Ne pas modifier les paramètres du proxy<br>2 = Ne pas utiliser de proxy<br>3 = Détecter automatiquement<br>4 = Utiliser le paramètre de l'ASA                                                                                                                                                                                                                                                            |
| IE-Proxy-Server               | O        | O   | O   | nombre entier | Unique                             | Adresse IP                                                                                                                                                                                                                                                                                                                                                                                                   |
| IETF-Radius-Class             | O        | O   | O   |               | Unique                             | Définit la politique de groupe pour la session VPN d'accès à distance. Pour les versions 8.2 et ultérieures, utilisez l'attribut Group-Policy au lieu de IETF-Radius-Class. Vous pouvez utiliser l'un des formats suivants : <ul style="list-style-type: none"> <li>• nom de la stratégie de groupe</li> <li>• OU = nom de la stratégie de groupe</li> <li>• OU = nom de la stratégie de groupe :</li> </ul> |
| IETF-Radius-Filter-Id         | O        | O   | O   | Chaîne        | Unique                             | Nom de la liste d'accès défini sur l'ASA. Le paramètre s'applique aux clients d'accès à distance VPN IPsec et SSL VPN.                                                                                                                                                                                                                                                                                       |
| IETF-Radius-Filter-IP-Address | O        | O   | O   | Chaîne        | Unique                             | Une adresse IP. Le paramètre s'applique aux clients d'accès à distance VPN IPsec et SSL VPN.                                                                                                                                                                                                                                                                                                                 |
| IETF-Radius-Filter-IP-Mask    | O        | O   | O   | Chaîne        | Unique                             | Un masque d'adresse IP. Le paramètre s'applique aux clients d'accès à distance VPN IPsec et SSL VPN.                                                                                                                                                                                                                                                                                                         |
| IETF-Radius-Idle-Timeout      | O        | O   | O   | nombre entier | Unique                             | Secondes                                                                                                                                                                                                                                                                                                                                                                                                     |

| Nom de l'attribut                     | VPN 3000 | ASA | PIX | Syntaxe/Type  | Valeur unique ou valeurs multiples | Valeurs possibles                                                                                                                                                                |
|---------------------------------------|----------|-----|-----|---------------|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IETF-RADIUS-Service-Type              | O        | O   | O   | nombre entier | Unique                             | 1 = Login<br>2 = Framed<br>5 = Remote access<br>6 = Administrative<br>7 = Invite de commande NAS                                                                                 |
| IETF-RADIUS-Session-Timeout           | O        | O   | O   | nombre entier | Unique                             | Secondes                                                                                                                                                                         |
| IKE-Keep-Alives                       | O        | O   | O   | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                                      |
| IPsec-Allow-Passwd-Stored             | O        | O   | O   | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                                      |
| IPsec-Authentication                  | O        | O   | O   | nombre entier | Unique                             | 0 = None<br>1 = RADIUS<br>2 = LDAP (autorisation uniquement)<br>3 = domaine NT<br>4 = SDI (RSA)<br>5 = Interne<br>6 = RADIUS avec expiration<br>7 = Kerberos ou Active Directory |
| IPsec-Auth-On-Rekey                   | O        | O   | O   | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                                      |
| IPsec-Backup-Server-List              | O        | O   | O   | Chaîne        | Unique                             | Adresses de serveurs (délimitées par des espaces)                                                                                                                                |
| IPsec-Backup-Servers                  | O        | O   | O   | Chaîne        | Unique                             | 1 = Utiliser la liste configurée sur le client<br>2 = Désactivé et effacer la liste des clients<br>3 = Utiliser la liste des serveurs de sauvegarde                              |
| IPsec-Client-Firewall-Filter-Name     | O        |     |     | Chaîne        | Unique                             | Spécifie le nom du filtre à envoyer au client en tant que politique de pare-feu.                                                                                                 |
| IPsec-Client-Firewall-Filter-Optional | O        | O   | O   | nombre entier | Unique                             | 0 = Obligatoire<br>1 = Facultatif                                                                                                                                                |

| Nom de l'attribut            | VPN 3000 | ASA | PIX | Syntaxe/Type  | Valeur unique ou valeurs multiples | Valeurs possibles                                                                                                                                          |
|------------------------------|----------|-----|-----|---------------|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPsec-Default-Domain         | O        | O   | O   | Chaîne        | Unique                             | Spécifie le nom de domaine par défaut unique à envoyer au client (1 à 255 caractères).                                                                     |
| IPsec-ExtAuthOnReq           |          | O   | O   | Chaîne        | Unique                             | Chaîne                                                                                                                                                     |
| IPsec-IKE-Peer-ID-Check      | O        | O   | O   | nombre entier | Unique                             | 1 = Obligatoire<br>2 = Si pris en charge par le certificat de l'homologue<br>3 = Ne pas vérifier                                                           |
| IPsec-IP-Compression         | O        | O   | O   | nombre entier | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                |
| IPsec-Mode-Config            | O        | O   | O   | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                |
| IPsec-Over-UDP               | O        | O   | O   | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                |
| IPsec-Over-UDP-Port          | O        | O   | O   | nombre entier | Unique                             | 4001 à 49 151 ; la valeur par défaut est 10 000.                                                                                                           |
| IPsec-Quick-Flow-Capability  | O        | O   | O   | nombre entier | Unique                             | 0 = Aucun<br>1 = Politique définie par le pare-feu distant « Are-You-There » (AYT)<br>2 = Politique CPP poussée vers le client<br>4 = Politique du serveur |
| IPsec-Sec-association        | O        |     |     | Chaîne        | Unique                             | Nom de l'association de sécurité                                                                                                                           |
| IPsec-Split-DNS-Names        | O        | O   | O   | Chaîne        | Unique                             | Spécifie la liste des noms de domaine secondaires à envoyer au client (1 à 255 caractères).                                                                |
| IPsec-Split-Tunneling-Policy | O        | O   | O   | nombre entier | Unique                             | 0 = Tunneliser tout le trafic<br>1 = Tunnelisation fractionnée<br>2 = Réseau local autorisé                                                                |
| IPsec-Split-Tunnel-List      | O        | O   | O   | Chaîne        | Unique                             | Spécifie le nom du réseau ou de la liste de contrôle d'accès qui décrit la liste d'inclusion du tunnel fractionné.                                         |



| Nom de l'attribut     | VPN 3000 | ASA | PIX | Syntaxe/Type  | Valeur unique ou valeurs multiples | Valeurs possibles                                                                                                                     |
|-----------------------|----------|-----|-----|---------------|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| IPsec-Tunnel-Type     | O        | O   | O   | nombre entier | Unique                             | 1 = Site à site<br>2 = Accès à distance                                                                                               |
| L2TP-Encryption       | O        |     |     | nombre entier | Unique                             | Bitmap :<br>1 = Chiffrement requis<br>2 = 40 bits<br>4 = 128 bits<br>8 = Stateless-Req<br>15 = 40/128-Encr/Stateless-Req              |
| L2TP-MPCCompression   | O        |     |     | nombre entier | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                           |
| MS-Client-Subnet-Mask | O        | O   | O   | Chaîne        | Unique                             | Une adresse IP                                                                                                                        |
| PFS-Required          | O        | O   | O   | Booléen       | Unique                             | 0 = Non<br>1 = Oui                                                                                                                    |
| Port-Forwarding-Name  | O        | O   |     | Chaîne        | Unique                             | Nom de chaîne de caractères (par exemple, « Corporate-Apps »)                                                                         |
| PPTP-Encryption       | O        |     |     | Integer       | Unique                             | Bitmap :<br>1 = Chiffrement requis<br>2 = 40 bits<br>4 = 128 bits<br>8 = Stateless-Req<br>Exemple :<br>15 = 40/128-Encr/Stateless-Req |
| PPTP-MPCCompression   | O        |     |     | nombre entier | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                           |
| Primary-DNS           | O        | O   | O   | Chaîne        | Unique                             | Une adresse IP                                                                                                                        |
| Primary-WINS          | O        | O   | O   | Chaîne        | Unique                             | Une adresse IP                                                                                                                        |
| Privilege-Level       |          |     |     | nombre entier | Unique                             | Pour les noms d'utilisateur, 0 à 15                                                                                                   |

| Nom de l'attribut                     | VPN 3000 | ASA | PIX | Syntaxe/Type  | Valeur unique ou valeurs multiples | Valeurs possibles                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------|----------|-----|-----|---------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Required-Client-Firewall-Vendor-Code  | O        | O   | O   | nombre entier | Unique                             | 1 = Cisco Systems (avec le client intégré Cisco)<br>2 = Zone Labs<br>3 = NetworkICE<br>4 = Sygate<br>5 = Cisco Systems (avec Cisco Intrusion Prevention Security Agent)                                                                                                                                                                                         |
| Required-Client-Firewall-Description  | O        | O   | O   | Chaîne        | Unique                             | —                                                                                                                                                                                                                                                                                                                                                               |
| Required-Client-Firewall-Product-Code | O        | O   | O   | nombre entier | Unique                             | Produits Cisco Systems :<br>1 = Cisco Intrusion Prevention Security Agent ou Cisco Integrated Client (CIC)<br>Produits de Zone Labs :<br>1 = Zone Alarm<br>2 = Zone AlarmPro<br>3 = Zone Labs Integrity<br>Produit NetworkICE :<br>1 = BlackIce Defender/Agent<br>Produits Sygate :<br>1 = Personal Firewall<br>2 = Personal Firewall Pro<br>3 = Security Agent |
| Require-HW-Client-Auth                | O        | O   | O   | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                                                                                                                                                                                                                     |
| Require-Individual-User-Auth          | O        | O   | O   | nombre entier | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                                                                                                                                                                                                                     |
| Secondary-DNS                         | O        | O   | O   | Chaîne        | Unique                             | Une adresse IP                                                                                                                                                                                                                                                                                                                                                  |
| Secondary-WINS                        | O        | O   | O   | Chaîne        | Unique                             | Une adresse IP                                                                                                                                                                                                                                                                                                                                                  |
| SEP-Card-Attribution                  |          |     |     | nombre entier | Unique                             | Non utilisé                                                                                                                                                                                                                                                                                                                                                     |
| Connexions simultanées                | O        | O   | O   | nombre entier | Unique                             | De 0 à 2 147 483 647                                                                                                                                                                                                                                                                                                                                            |

| Nom de l'attribut                                   | VPN 3000 | ASA | PIX | Syntaxe/Type  | Valeur unique ou valeurs multiples | Valeurs possibles                                                                                                                                                                                                      |
|-----------------------------------------------------|----------|-----|-----|---------------|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Strip-Realm                                         | O        | O   | O   | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                                                                            |
| TACACS-Authtype                                     | O        | O   | O   | nombre entier | Unique                             | —                                                                                                                                                                                                                      |
| TACACS-Privilege-Level                              | O        | O   | O   | nombre entier | Unique                             | —                                                                                                                                                                                                                      |
| Tunnel-Group-Lock                                   |          | O   | O   | Chaîne        | Unique                             | Nom du groupe de tunnels ou « none » (aucun)                                                                                                                                                                           |
| Tunneling-Protocoles                                | O        | O   | O   | nombre entier | Unique                             | 1 = PPTP<br>2 = L2TP<br>4 = IPSec (IKEv1)<br>8 = L2TP/IPSec<br>16 = WebVPN<br>32 = SVC<br>64 = IPsec (IKEv2)<br>8 et 4 sont mutuellement exclusifs<br>(0 à 11, 16 à 27, 32 à 43, 48 à 59 sont des valeurs autorisées). |
| Use-Client-Address                                  | O        |     |     | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                                                                            |
| User-Auth-Server-Name                               | O        |     |     | Chaîne        | Unique                             | Adresse IP ou nom d'hôte                                                                                                                                                                                               |
| Port du serveur d'authentification de l'utilisateur | O        | O   | O   | nombre entier | Unique                             | Numéro de port pour le protocole de serveur                                                                                                                                                                            |
| User-Auth-Server-Secret                             | O        |     |     | Chaîne        | Unique                             | Mot de passe du serveur                                                                                                                                                                                                |
| WebVPN-ACL-Filters                                  |          | O   |     | Chaîne        | Unique                             | Nom de liste d'accès de type Web                                                                                                                                                                                       |
| WebVPN-Apply-ACL-Filter                             | O        | O   |     | nombre entier | Unique                             | 0 = Désactivé<br>1 = Activé<br><br>Avec la version 8.0 et les versions ultérieures, cet attribut n'est pas requis.                                                                                                     |

| Nom de l'attribut                           | VPN 3000 | ASA | PIX | Syntaxe/Type  | Valeur unique ou valeurs multiples | Valeurs possibles                                                                                                                                                                                                                                                                                            |
|---------------------------------------------|----------|-----|-----|---------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WebVPN-Client-Support-Enable                | O        | O   |     | nombre entier | Unique                             | 0 = Désactivé<br>1 = Activé<br><br>Avec la version 8.0 et les versions ultérieures, cet attribut n'est pas requis.                                                                                                                                                                                           |
| WebVPN-Enable-functions                     |          |     |     | nombre entier | Unique                             | Non utilisé — obsolète                                                                                                                                                                                                                                                                                       |
| WebVPN-Exchange-Server-Address              |          |     |     | Chaîne        | Unique                             | Non utilisé — obsolète                                                                                                                                                                                                                                                                                       |
| WebVPN-Exchange-Server-NETBIOS-Name         |          |     |     | Chaîne        | Unique                             | Non utilisé — obsolète                                                                                                                                                                                                                                                                                       |
| WebVPN-File-Access-Enable                   | O        | O   |     | nombre entier | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                                                                                                                                                                  |
| WebVPN-File-Download-Enable                 | O        | O   |     | nombre entier | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                                                                                                                                                                  |
| WebVPN-File-Server-Enable                   | O        | O   |     | nombre entier | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                                                                                                                                                                  |
| WebVPN-Forward-Ports                        |          | O   |     | Chaîne        | Unique                             | Nom de la liste de transfert de port                                                                                                                                                                                                                                                                         |
| WebVPN-Homepage                             | O        | O   |     | Chaîne        | Unique                             | Une URL telle que <a href="http://www.exemple.com">http://www.exemple.com</a>                                                                                                                                                                                                                                |
| WebVPN-Mac-Stub-URL                         | O        | O   |     | Chaîne        | Unique                             | Consultez le guide de déploiement du VPN SSL pour obtenir des exemples à l'URL suivante :<br><br><a href="http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html">http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html</a> |
| WebVPN-Mac-Stub-URL2                        | O        | O   |     | Chaîne        | Unique                             | Consultez le guide de déploiement du VPN SSL pour obtenir des exemples à l'URL suivante :<br><br><a href="http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html">http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html</a> |
| WebVPN-Port-Forwarding-Auto-Download-Enable | O        | O   |     | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                                                                                                                                                                                                                                                  |

| Nom de l'attribut                           | VPN 3000 | ASA | PIX | Syntaxe/Type  | Valeur unique ou valeurs multiples | Valeurs possibles                                                                  |
|---------------------------------------------|----------|-----|-----|---------------|------------------------------------|------------------------------------------------------------------------------------|
| WebVPN-PortForwarding-Enable                | O        | O   |     | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                        |
| WebVPN-PortForwarding-Exchange-Proxy-Enable | O        | O   |     | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                        |
| WebVPN-PortForwarding-HTTP-Proxy-Enable     | O        | O   |     | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                        |
| WebVPN-Subgr-OS-Name                        | O        | O   |     | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                        |
| WebVPN-SVC-Client-IPD                       | O        | O   |     | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                        |
| WebVPN-SVC-Compression                      | O        | O   |     | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                        |
| WebVPN-SVC-Enable                           | O        | O   |     | Booléen       | Unique                             | 0 = Désactivé<br>1 = Activé                                                        |
| WebVPN-SVC-Global-DHD                       | O        | O   |     | nombre entier | Unique                             | 0 = Désactivé<br>n = Valeur de détection d'homologue mort en secondes (30 à 3 600) |
| WebVPN-SVC-keepalive                        | O        | O   |     | nombre entier | Unique                             | 0 = Désactivé<br>n = Valeur de keepalive en secondes (15 - 600)                    |
| WebVPN-SVC-Keep-Enable                      | O        | O   |     | nombre entier | Unique                             | 0 = Désactivé<br>1 = Activé                                                        |
| WebVPN-SVC-Proxy-Auth                       | O        | O   |     | nombre entier | Unique                             | 0 = Aucun<br>1 = SSL<br>2 = Nouveau tunnel<br>3 = Any (défini sur SSL)             |
| WebVPN-SVC-Proxy-Period                     | O        | O   |     | nombre entier | Unique                             | 0 = Désactivé<br>n = période de nouvelle tentative en minutes (4 - 10080)          |

| Nom de l'attribut   | VPN 3000 | ASA | PIX | Syntaxe/Type  | Valeur unique ou valeurs multiples | Valeurs possibles           |
|---------------------|----------|-----|-----|---------------|------------------------------------|-----------------------------|
| WebVPN-SVC-ACL-Ente | O        | O   |     | nombre entier | Unique                             | 0 = Désactivé<br>1 = Activé |
| WebVPN-URL-Ente     | O        | O   |     | nombre entier | Unique                             | 0 = Désactivé<br>1 = Activé |
| WebVPN-URL-List     |          | O   |     | Chaîne        | Unique                             | Nom de la liste d'URL       |

## Types d'URL pris en charge dans les listes de contrôle d'accès

L'URL peut être une URL partielle, contenir des caractères génériques pour le serveur ou inclure un port.

Les types d'URL suivants sont pris en charge.

|                |          |                 |           |
|----------------|----------|-----------------|-----------|
| toutes les URL | https:// | post://         | ssh://    |
| cifs://        | ica://   | rdp://          | telnet:// |
| citrix://      | imap4:// | rdp2://         | vnc://    |
| citrixs://     | ftp://   | smart-tunnel:// |           |
| http://        | pop3://  | smtp://         |           |

## Lignes directrices relatives à l'utilisation des paires Cisco-AV

- Utilisez les entrées de paire Cisco-AV avec le préfixe ip:inac1# pour appliquer les listes d'accès pour les tunnels distants IPsec et SSL VPN Client (SVC).
- Utilisez les entrées de paire Cisco-AV avec le préfixe webvpn:inac1# pour appliquer les listes d'accès aux tunnels sans client du VPN SSL (en mode navigateur).
- Pour les listes de contrôle d'accès de type Web, vous ne spécifiez pas la source, car l'ASA est la source.

Tableau 16 : Jetons pris en charge par l'ASA

| Jeton               | Champ de syntaxe   | Description                                                                                                                                                                                          |
|---------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip:inac1# Num =     | S.O. (identifiant) | (Où Num est un entier unique.) Introduit toutes les listes de contrôle d'accès basées sur des paires AV. Applique les listes d'accès pour les tunnels distants IPsec et SSL VPN (SVC).               |
| webvpn:inac1# Num = | S.O. (identifiant) | (Où Num est un entier unique.) Introduit toutes les listes de contrôle d'accès SSL sans client basées sur des paires AV. Applique les listes d'accès pour les tunnels sans client (mode navigateur). |
| deny (Refuser)      | Action             | Refuse l'action. (Par défaut)                                                                                                                                                                        |

| Jeton              | Champ de syntaxe | Description                                                                                                              |
|--------------------|------------------|--------------------------------------------------------------------------------------------------------------------------|
| permit (Autoriser) | Action           | Autorise l'action.                                                                                                       |
| ICMP               | Protocole        | Internet Control Message Protocol (ICMP)                                                                                 |
| 1                  | Protocole        | Internet Control Message Protocol (ICMP)                                                                                 |
| IP                 | Protocole        | Protocole Internet (IP)                                                                                                  |
| 0                  | Protocole        | Protocole Internet (IP)                                                                                                  |
| TCP                | Protocole        | protocole TCP (Transmission Control Protocol)                                                                            |
| 6                  | Protocole        | protocole TCP (Transmission Control Protocol)                                                                            |
| UDP                | Protocole        | Protocole de datagrammes utilisateur (UDP)                                                                               |
| 17                 | Protocole        | Protocole de datagrammes utilisateur (UDP)                                                                               |
| Tous               | Nom d'hôte       | La règle s'applique à tout hôte.                                                                                         |
| hôte               | Nom d'hôte       | Toute chaîne alphanumérique qui dénote un nom d'hôte.                                                                    |
| se connecter       | Journal          | Lorsque l'événement se produit, un message de journal de filtre s'affiche. (Identique à permit and log ou deny and log.) |
| lt                 | Opérateur        | Valeur inférieure à                                                                                                      |
| gt                 | Opérateur        | Valeur supérieure à                                                                                                      |
| eq                 | Opérateur        | Égal à la valeur                                                                                                         |
| neq                | Opérateur        | Non égal à la valeur                                                                                                     |
| plage              | Opérateur        | Plage inclusive. Doit être suivi de deux valeurs.                                                                        |

## Syntaxe des attributs AV Pair Cisco

La paire AV Cisco (Attribute Value) (numéro d'identifiant 26/9/1) peut être utilisée pour appliquer les listes d'accès d'un serveur RADIUS (comme Cisco ACS) ou d'un serveur LDAP par l'intermédiaire d'un mappage d'attributs LDAP.

La syntaxe de chaque règle Cisco-AV-Pair est la suivante :

*[Préfixe] [Action] [Protocole] [Source] [Masque générique de la source] [Destination] [Masque générique de la destination] [Établi] [Log] [Opérateur] [Port]*

**Tableau 17 : Règles de syntaxe des attributs d'AV-Pair**

| Champ  | Description                                                                  |
|--------|------------------------------------------------------------------------------|
| Action | Action à effectuer si la règle correspond à deny (refus) ou permit (permis). |

| Champ                                        | Description                                                                                                                                                                                                                                                                                            |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Destination                                  | Réseau ou hôte qui reçoit le paquet. Précisez-le comme une adresse IP, un nom d'hôte ou le mot-clé <b>any</b> . Si vous utilisez une adresse IP, le masque de caractère générique source doit suivre.                                                                                                  |
| Masque de caractère générique de destination | Le masque de caractère générique qui s'applique à l'adresse de destination.                                                                                                                                                                                                                            |
| Journal                                      | Génère un message de journal FILTER. Vous devez utiliser ce mot-clé pour générer des événements de niveau de gravité 9.                                                                                                                                                                                |
| Opérateur                                    | Opérateurs logiques : supérieur à, inférieur à, égal à, différent de.                                                                                                                                                                                                                                  |
| Port                                         | Le nombre d'un port TCP ou UDP dans la plage de 0 à 65 535.                                                                                                                                                                                                                                            |
| Préfixe                                      | Un identifiant unique pour l'AV pair (par exemple : <code>ip:inacl#1=</code> pour les listes d'accès standard ou <code>webvpn:inacl# =</code> pour les listes d'accès VPN SSL sans client). Ce champ ne s'affiche que lorsque le filtre a été envoyé en tant que paire AV.                             |
| Protocole                                    | Numéro ou nom d'un protocole IP. Il s'agit d'un entier dans la plage de 0 à 255 ou de l'un des mots-clés suivants : <b>icmp</b> , <b>igmp</b> , <b>ip</b> , <b>tcp</b> , <b>udp</b> .                                                                                                                  |
| Source                                       | Réseau ou hôte qui envoie le paquet. Précisez-le comme une adresse IP, un nom d'hôte ou le mot-clé <b>any</b> . Si vous utilisez une adresse IP, le masque de caractère générique source doit suivre. Ce champ ne s'applique pas au VPN SSL sans client, car l'ASA a le rôle de la source ou du proxy. |
| Masque de caractère générique source         | Le masque de caractère générique qui s'applique à l'adresse source. Ce champ ne s'applique pas au VPN SSL sans client, car l'ASA a le rôle de la source ou du proxy.                                                                                                                                   |

## Exemples d'ACL à l'aide de paires Cisco-AV

Cette section présente des exemples de paires AV Cisco et décrit l'effet d'autorisation ou de refus qui en résulte.



### Remarque

Chaque numéro d'ACL dans `inacl#` doit être unique. Cependant, ils n'ont pas besoin d'être séquentiels (par exemple, 1, 2, 3, 4). Autrement dit, ils peuvent être 5, 45, 135.

Tableau 18 : Exemples de paires AV Cisco et de l'effet d'autorisation ou de refus correspondant

| Exemple de paire AV Cisco                                                      | Effet d'autorisation ou de refus                                                                                                                 |
|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ip:inacl#1=deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log</code> | Permet le trafic IP entre les deux hôtes à l'aide d'un client VPN IPsec ou SSL à tunnel complet.                                                 |
| <code>ip:inacl#2=permit TCP any host 10.160.0.1 eq 80 log</code>               | Autorise le trafic TCP de tous les hôtes vers l'hôte spécifié sur le port 80 uniquement, au moyen d'un client VPN IPsec ou SSL à tunnel complet. |



| Exemple de paire AV Cisco                                                                                                                                                            | Effet d'autorisation ou de refus                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| webvpn:inac1#1=permit url<br>http://www.example.comwebvpn:inac1#2=deny url<br>smtp://serverwebvpn:inac1#3=permit url cifs://server/share                                             | Autorise le trafic VPN SSL sans client vers l'URL spécifiée, refuse le trafic SMTP vers un serveur précis et autorise l'accès au partage de fichiers (CIFS) sur le serveur spécifié.                                                                 |
| webvpn:inac1#1=permit tcp 10.86.1.2 eq 2222 logwebvpn:inac1#2=deny tcp 10.86.1.2 eq 2323 log                                                                                         | Refuse l'accès Telnet et autorise l'accès SSH sur les ports non par défaut 2323 et 2222, respectivement, ou d'autres flux de trafic d'application utilisant ces ports pour le VPN SSL sans client.                                                   |
| webvpn:inac1#1=permit url<br>ssh://10.86.1.2webvpn:inac1#35=permit tcp 10.86.1.5 eq 22<br>logwebvpn:inac1#48=deny url<br>telnet://10.86.1.2webvpn:inac1#100=deny tcp 10.86.1.6 eq 23 | Autorise l'accès SSH du VPN SSL sans client au port par défaut 22 et refuse respectivement l'accès Telnet au port 23. Cet exemple suppose que vous utilisez des modules d'extension Telnet ou SSH Java appliqués par ces listes de contrôle d'accès. |

## Exemples d'autorisation d'accès à distance Active Directory/LDAP

Cette section présente des exemples de procédures pour configurer l'authentification et l'autorisation sur l'ASA à l'aide du serveur Microsoft Active Directory. Elle comprend les rubriques suivantes :

- [Appliquer la politique aux attributs basés sur l'utilisateur, à la page 313](#)
- [Appliquer l'affectation d'adresse IP statique pour les tunnels Secure Client \(services client sécurisés\), à la page 315](#)
- [Appliquer l'autorisation ou le refus d'accès entrant, à la page 317](#)
- [Appliquer les règles d'heures de connexion et d'heure du jour, à la page 319](#)

D'autres exemples de configuration disponibles sur Cisco.com comprennent les notes techniques suivantes.

- [ASA/PIX : exemple de mappage des clients VPN aux stratégies de groupe de VPN à l'aide de la configuration LDAP](#)
- [PIX/ASA 8.0 : utiliser l'authentification LDAP pour attribuer une stratégie de groupe à la connexion](#)

## Appliquer la politique aux attributs basés sur l'utilisateur

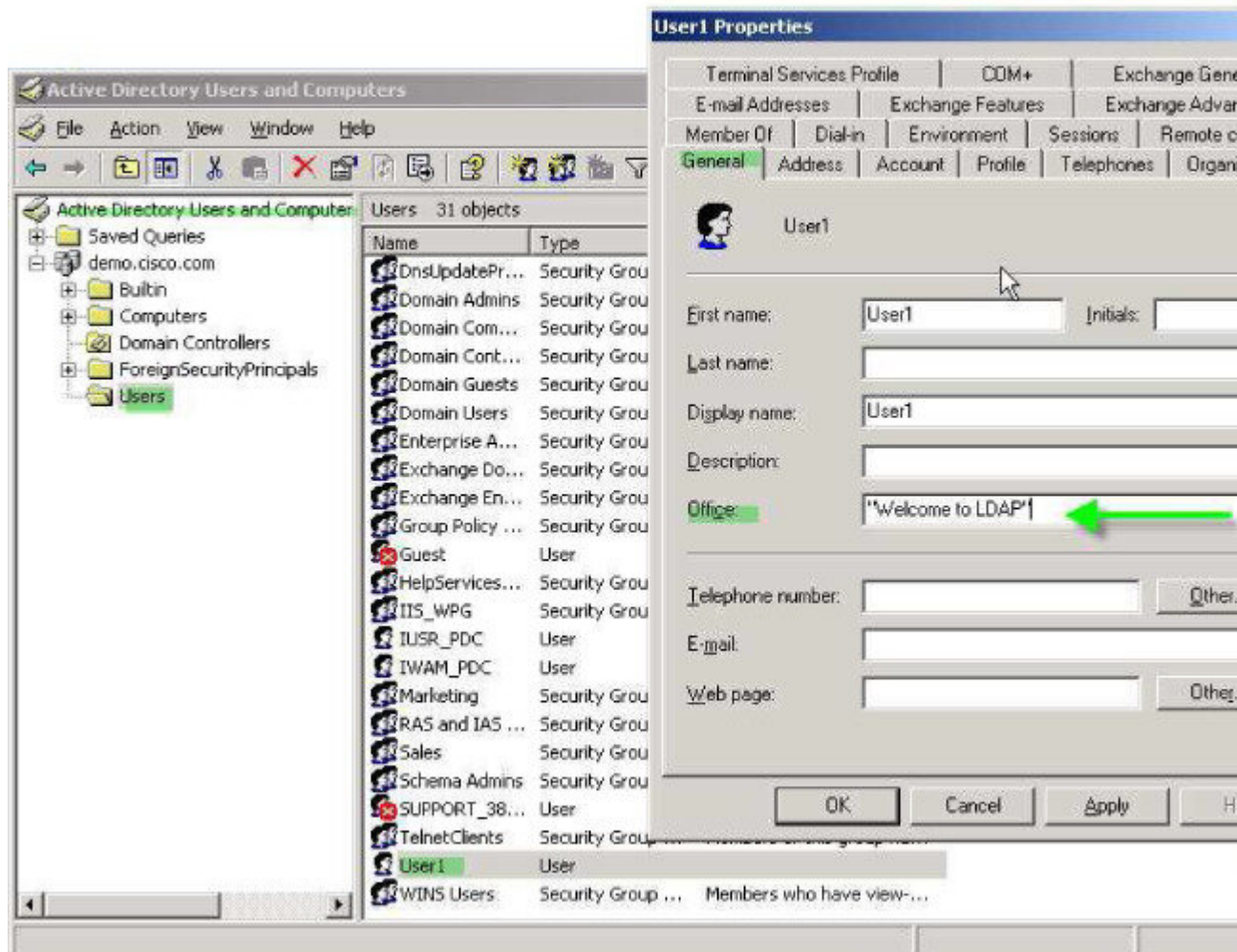
Cet exemple affiche une bannière simple à l'utilisateur, indiquant comment vous pouvez mapper n'importe quel attribut LDAP standard à un attribut spécifique au fournisseur (VSA) bien connu, et vous pouvez mapper un ou plusieurs attributs LDAP à un ou plusieurs attributs LDAP de Cisco. Il s'applique à tout type de connexion, y compris le client VPN IPsec et Secure Client (services client sécurisés).

Pour appliquer une bannière simple à un utilisateur configuré sur un serveur LDAP AD, utilisez le champ Office sous l'onglet General (Général) pour saisir le texte de la bannière. Ce champ utilise l'attribut nommé physicalDeliveryOfficeName. Sur l'ASA, créez une carte d'attributs qui associe physicalDeliveryOfficeName à l'attribut Cisco Banner1.

Lors de l'authentification, l'ASA récupère la valeur de `physicalDeliveryOfficeName` du serveur, associe la valeur à l'attribut `Cisco Banner1` et affiche la bannière à l'utilisateur.

## Procédure

- Étape 1** Cliquez avec le bouton droit sur le nom d'utilisateur, ouvrez la boîte de dialogue Propriétés puis l'onglet **General (Général)** et saisissez le texte de la bannière dans le champ Office (Bureau), qui utilise l'attribut AD/LDAP `physicalDeliveryOfficeName`.



- Étape 2** Créez une correspondance d'attributs LDAP sur l'ASA.  
Créez la carte Banner et faites correspondre l'attribut AD/LDAP `physicalDeliveryOfficeName` à l'attribut Cisco `Banner1` :

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

**Étape 3** Associez la carte d'attributs LDAP au serveur AAA.

Entrez en mode de configuration de l'hôte du serveur AAA pour l'hôte 10.1.1.2 dans le groupe de serveurs AAA MS\_LDAP et associez la carte d'attributs Banner que vous avez créée précédemment :

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

**Étape 4** Testez l'application de la bannière.

---

## Appliquer l'affectation d'adresse IP statique pour les tunnels Secure Client (services client sécurisés)

Cet exemple s'applique aux clients de tunnel complet, tels que le client IPsec et les clients VPN SSL.

Pour appliquer les affectations d'adresses IP statiques Secure Client (services client sécurisés), configurez l'utilisateur Web1 Secure Client (services client sécurisés) pour qu'il reçoive une adresse IP statique, saisissez l'adresse dans le champ Assign Static IP Address (Attribuer une adresse IP statique) de l'onglet Dial-in (Accès distant) sur le serveur LDAP AD (ce champ utilise l'attribut msRADIUSFramedIPAddress), puis créez une carte d'attributs qui mappe cet attribut à l'attribut Cisco IETF-Radius-Framed-IP-Address.

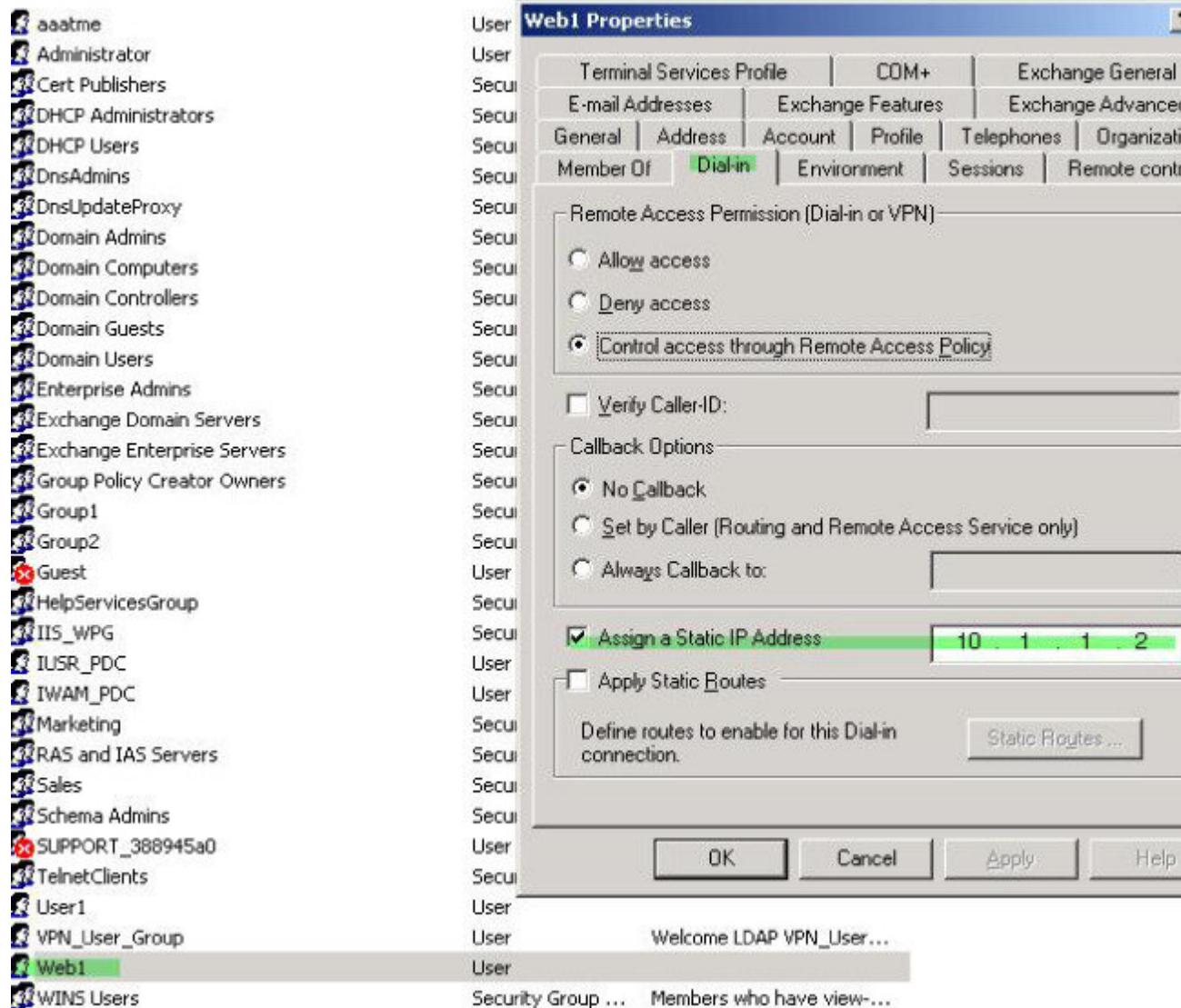
Lors de l'authentification, l'ASA récupère la valeur de msRADIUSFramedIPAddress du serveur, la mappe à l'attribut Cisco IETF-Radius-Framed-IP-Address et fournit l'adresse statique à Web1.

### Procédure

---

**Étape 1** Cliquez avec le bouton droit sur le nom d'utilisateur, ouvrez la boîte de dialogue Properties (Propriétés), puis l'onglet **Dial-in (Accès distant)**, cochez la case **Assign Static IP Address (Attribuer une adresse IP statique)** et saisissez l'adresse IP 10.1.1.2.

## Appliquer l'affectation d'adresse IP statique pour les tunnels Secure Client (services client sécurisés)



**Étape 2** Créez une mise en correspondance d'attributs pour la configuration LDAP affichée.

Mappez l'attribut AD msRADIUSFramedIPAddress utilisé par le champ d'adresse statique avec l'attribut Cisco IETF-Radius-Framed-IP-Address :

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

**Étape 3** Associez la carte d'attributs LDAP au serveur AAA.

Entrez en mode de configuration d'hôte de serveur AAA pour l'hôte 10.1.1.2 dans le groupe de serveurs AAA MS\_LDAP, puis associez la carte d'attributs static\_address que vous avez créée précédemment :

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

```
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

**Étape 4** Vérifiez que la commande **vpn-address-assignment** est configurée pour spécifier AAA en affichant cette partie de la configuration :

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa << Make sure this is configured >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

**Étape 5** Établissez une connexion à l'ASA avec le Secure Client (services client sécurisés). Observez que l'utilisateur reçoit l'adresse IP configurée sur le serveur et mappée à l'ASA.

**Étape 6** Utilisez la commande **show vpn-sessiondb svc** pour afficher les détails de la session et vérifier l'adresse attribuée :

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username : web1 Index : 31
Assigned IP : 10.1.1.2 Public IP : 10.86.181.70
Protocol : Clientless SSL-Tunnel DTLS-Tunnel
Encryption : RC4 AES128 Hashing : SHA1
Bytes Tx : 304140 Bytes Rx : 470506
Group Policy : VPN_User_Group Tunnel Group : Group1_TunnelGroup
Login Time : 11:13:05 UTC Tue Aug 28 2007
Duration : 0h:01m:48s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

## Appliquer l'autorisation ou le refus d'accès entrant

Cet exemple crée une mise en correspondance d'attributs LDAP qui précise les protocoles de tunnellation autorisés par l'utilisateur. Vous associez les paramètres d'autorisation d'accès et de refus d'accès de l'onglet Dial-in à l'attribut Cisco Tunneling-Protocol, qui prend en charge les valeurs de bitmap suivantes :

| Valeur | Protocole de tunnellation                                              |
|--------|------------------------------------------------------------------------|
| 1      | PPTP                                                                   |
| 2      | L2TP                                                                   |
| 4      | IPsec (IKEv1)                                                          |
| 8      | L2TP/IPsec                                                             |
| 16     | SSL sans client                                                        |
| 32     | Client SSL—Secure Client (services client sécurisés) ou client VPN SSL |
| 64     | IPsec (IKEv2)                                                          |

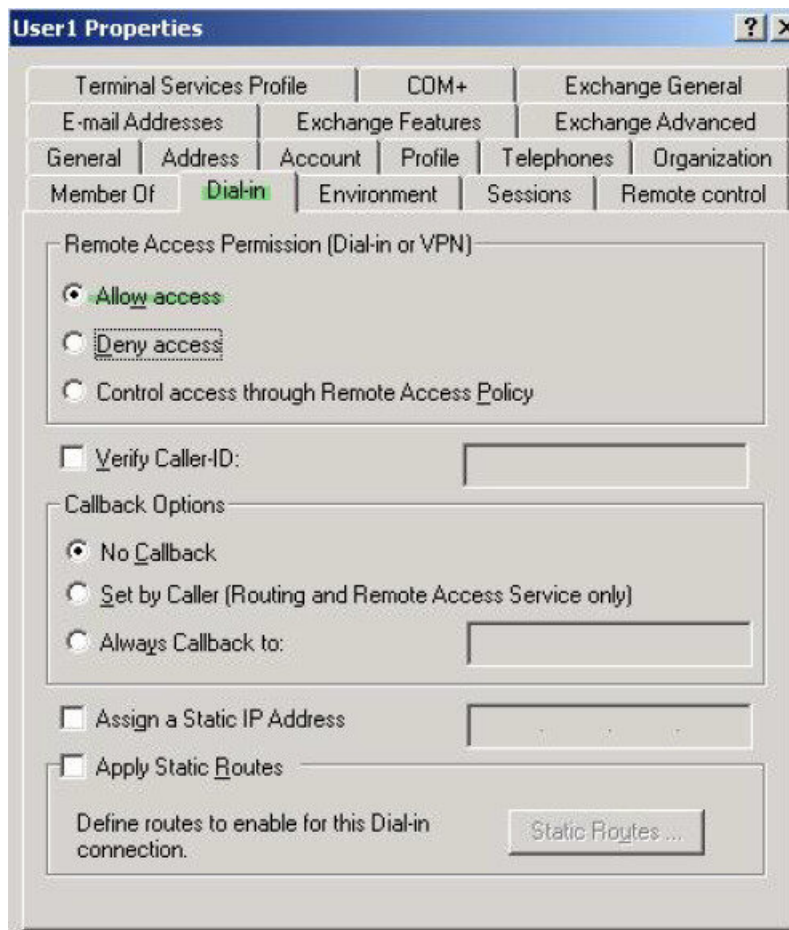
- <sup>1</sup> (1) IPsec et L2TP sur IPsec ne sont pas pris en charge simultanément. Par conséquent, les valeurs 4 et 8 s'excluent mutuellement.
- <sup>2</sup> (2) Voir note 1.

Utilisez cet attribut pour créer une condition Allow Access (TRUE) ou Deny Access (FALSE) pour les protocoles et appliquer la méthode pour laquelle l'utilisateur est autorisé à accéder.

Consultez la note technique [ASA/PIX : Mappage des clients VPN avec les stratégies de groupe VPN à l'aide de l'exemple de configuration LDAP](#) pour obtenir un autre exemple d'application de l'autorisation d'accès par numérotation ou de refus d'accès.

## Procédure

- Étape 1** Cliquez avec le bouton droit sur le nom d'utilisateur, ouvrez la boîte de dialogue des propriétés, puis l'onglet **Dial-in**, et cliquez sur le bouton radio Allow Access (autoriser l'accès).



### Remarque

Si vous choisissez l'option Contrôle de l'accès par la stratégie d'accès à distance, aucune valeur n'est renvoyée par le serveur et les autorisations appliquées sont basées sur les paramètres de stratégie de groupe internes de l'ASA.

**Étape 2** Créez une mise en correspondance d'attributs pour autoriser une connexion IPsec et Secure Client (services client sécurisés), mais refuser une connexion SSL sans client.

a) Créez la carte `tunneling_protocols` :

```
hostname(config)# ldap attribute-map tunneling_protocols
```

b) Mappez l'attribut AD `msNPAllowDialin` utilisé par le paramètre Allow Access (autoriser l'accès) avec l'attribut Cisco Tunneling-Protocols (protocoles de tunnellation) :

```
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
```

c) Ajoutez des valeurs de carte :

```
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

**Étape 3** Associez la carte d'attributs au serveur AAA.

a) Passez en mode de configuration d'hôte de serveur aaa pour l'hôte 10.1.1.2 dans le groupe de serveurs AAA `MS_LDAP` :

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

b) Associez la carte d'attributs `tunneling_protocols` que vous avez créée :

```
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

**Étape 4** Vérifiez que la carte d'attributs fonctionne comme configurée.

Essayez les connexions à l'aide du protocole SSL sans client, l'utilisateur doit être informé qu'un mécanisme de connexion non autorisée est la raison de l'échec de la connexion. Le client IPsec doit se connecter, car IPsec est un protocole de tunnellation autorisé en fonction de la carte d'attributs.

## Appliquer les règles d'heures de connexion et d'heure du jour

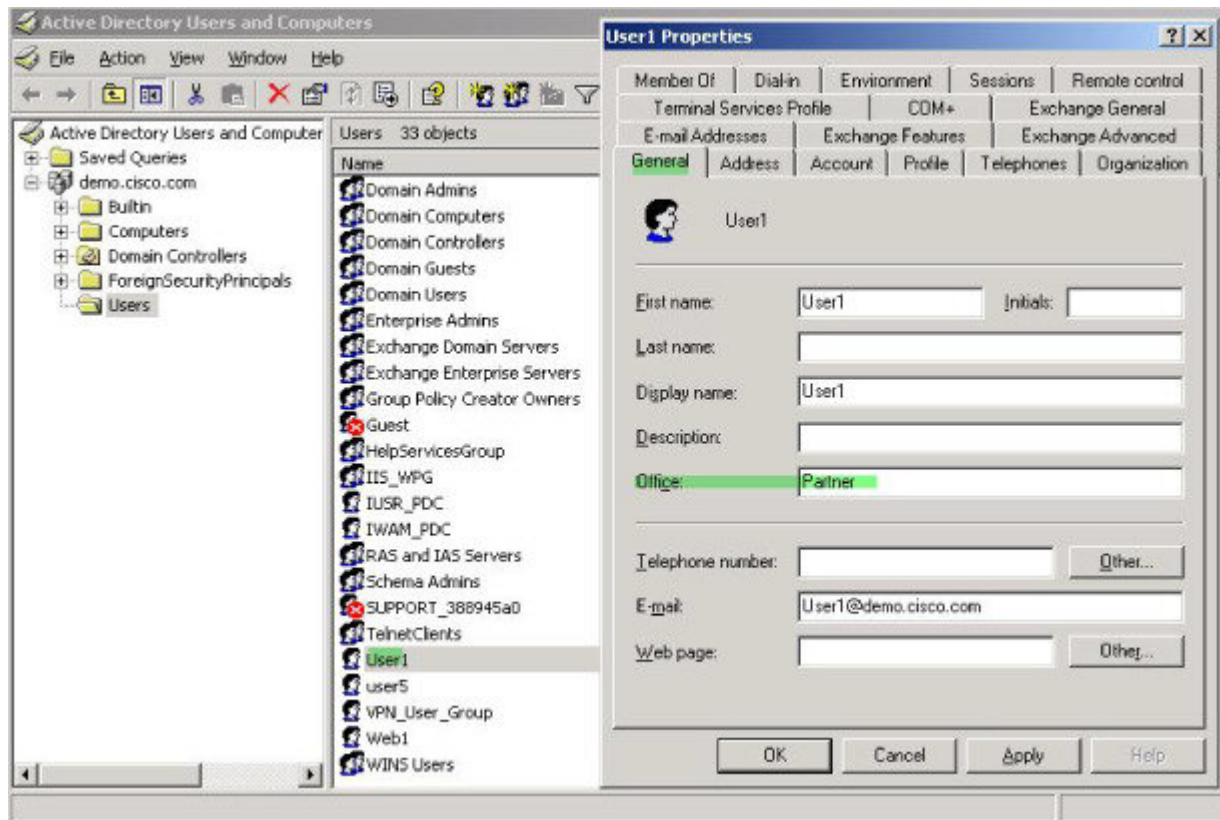
L'exemple suivant montre comment configurer et appliquer les heures pendant lesquelles un utilisateur SSL sans client (comme un partenaire commercial) est autorisé à accéder au réseau.

Sur le serveur AD, utilisez le champ Office (Bureau) pour saisir le nom du partenaire, qui utilise l'attribut `physicalDeliveryOfficeName`. Nous créons ensuite une carte d'attributs sur l'ASA pour faire correspondre cet attribut à l'attribut Cisco Access-Hours. Lors de l'authentification, l'ASA récupère la valeur de `physicalDeliveryOfficeName` et l'associe à Access-Hours.

### Procédure

**Étape 1** Sélectionnez l'utilisateur, cliquez avec le bouton droit sur **Properties (Propriétés)** puis ouvrez l'onglet **General (Général)** :





## Étape 2 Créer une carte d'attributs.

Créez la carte d'attributs `access_hours` et faites correspondre l'attribut AD `physicalDeliveryOfficeName` utilisé par le champ `Office` à l'attribut Cisco Access-Hours.

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

## Étape 3 Associez la carte d'attributs LDAP au serveur AAA.

Entrez dans le mode de configuration de l'hôte du serveur aaa pour l'hôte 10.1.1.2 du groupe de serveurs AAA MS\_LDAP et associez la carte d'attributs `access_hours` que vous avez créée.

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

## Étape 4 Configurez les plages de temps pour chaque valeur autorisée sur le serveur.

Configurez les heures d'accès du partenaire de 9 h à 17 h du lundi au vendredi :

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```



## 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.