ASDM, livre 3 : Guide de configuration d'ASDM Cisco Secure Firewall ASA, 7.19

Dernière modification : 2026-07-24

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

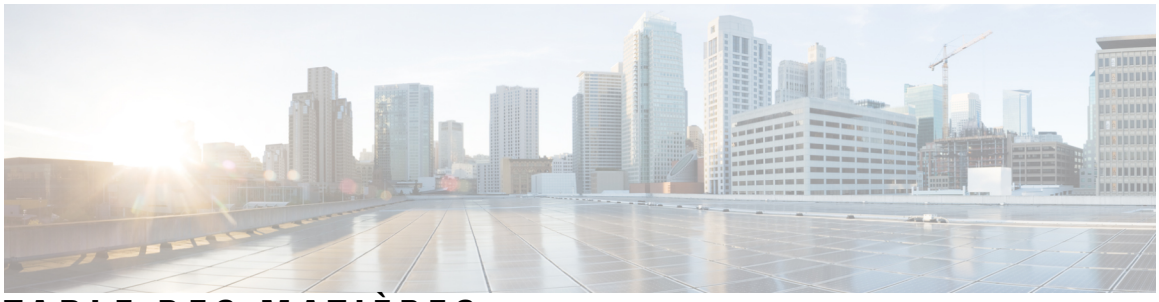


TABLE DES MATIÈRES

À propos de ce guide

Les rubriques suivantes expliquent comment utiliser ce guide.

Objectifs du document

L'objectif de ce guide est de vous aider à configurer VPN sur le Secure Firewall ASA à l'aide de Vous pouvez également configurer et superviser l'ASA à l'aide d'Adaptive Security Device Manager (ASDM), une application GUI Web. Ce guide ne couvre pas toutes les fonctionnalités, mais décrit uniquement les scénarios de configuration les plus 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/asadocs.

Conventions de document

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

Conventions de texte

Convention	Indication
boldface	Les commandes, les mots clés, les étiquettes de boutons, les noms de champ et le texte saisi par l'utilisateur s'affichent dans **boldface**. Pour les commandes basées sur des menus, le chemin complet vers la commande s'affiche.

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

Alertes adressées aux lecteurs

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

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

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

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

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

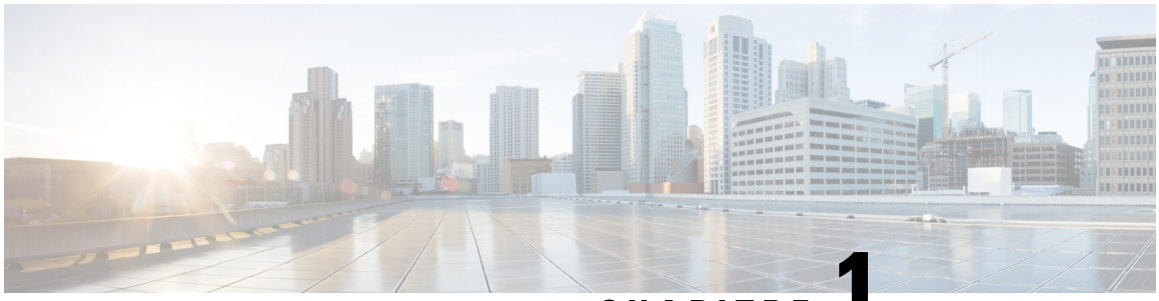
Avertissement **signifie que *le lecteur doit être averti.* Dans cette situation, vous pourriez effectuer une opération risquant d'entraîner des blessures corporelles.**

Communications, services et renseignements supplémentaires

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

Outil de recherche de bogues

L'outil de recherche de bogues de Cisco est un outil Web qui donne accès au système de suivi des bogues de Cisco, qui conserve une liste complète des défaillances et des vulnérabilités des produits et des logiciels Cisco. Cet outil vous fournit des informations détaillées sur les défaillances de vos produits et logiciels.



CHAPITRE 1

Assistants VPN

Présentation du VPN

L'ASA crée un réseau privé virtuel en établissant une connexion sécurisée sur un réseau TCP/IP (tel qu'Internet) que les utilisateurs voient comme une connexion privée. Il peut créer des connexions utilisateur unique à réseau local (LAN) et des connexions de réseau local (LAN) à réseau local (LAN).

La connexion sécurisée est appelée tunnel, et l'ASA utilise des protocoles de tunnellisation pour négocier les paramètres de sécurité, créer et gérer des tunnels, encapsuler des paquets, les transmettre ou les recevoir par le tunnel, et les désencapsuler. L'ASA fonctionne comme un point terminal de tunnel bidirectionnel : il peut recevoir des paquets simples, les encapsuler et les envoyer à l'autre extrémité du tunnel où ils sont désencapsulés et envoyés à leur destination finale. Il peut également recevoir des paquets encapsulés, les désencapsuler et les envoyer à leur destination finale.

L'assistant VPN vous permet de configurer les connexions de base entre les réseaux locaux et d'accès à distance et d'affecter des clés prépartagées ou des certificats numériques pour l'authentification. Utilisez ASDM pour modifier et configurer les fonctionnalités avancées.

Les quatre assistants VPN décrits dans cette section sont les suivants :

- Assistant VPN Secure Client, à la page 4

  Le module VPN AnyConnect de Cisco Secure Client fournit des connexions SSL ou IPsec (IKEv2) sécurisées à l'ASA pour les utilisateurs distants avec une tunnellisation VPN complète vers les ressources de l'entreprise. Sans client déjà installé, les utilisateurs distants saisissent dans leur navigateur l'adresse IP d'une interface configurée pour accepter les connexions VPN sans client. L'ASA 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 et reste ou se désinstalle (selon la configuration de l'ASA) lorsque la connexion s'interrompt. 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.

  L'assistant VPN Secure Client ne sera disponible que dans les contextes d'utilisateur lorsque l'ASA est en mode multi-contexte. Le stockage et la classe de ressources pour le contexte requis doivent être configurés à partir du contexte du système.

Le stockage par contexte est requis pour avoir les fichiers de paquet et de profil Cisco Secure Client. La classe de ressource est requise pour l'attribution de licence pour chaque contexte. La licence utilisée est Secure Client Premium.

Remarque Le reste de la configuration pour cet assistant reste la même que celle d'un contexte unique.

- Assistant d'accès à distance IPsec IKEv2, à la page 12

  IKEv2 permet aux clients VPN d'autres fournisseurs de se connecter aux appareils de sécurité adaptables Cisco. Cela améliore la sécurité et est conforme aux exigences d'accès à distance IPsec définies dans les mandats du gouvernement américain et du secteur public.

  L'assistant d'accès à distance IPSec IKEv2 ne sera disponible que dans les contextes d'utilisateur lorsque l'ASA est en mode multi-contexte. La classe de ressource pour le contexte requis doit être configurée à partir du contexte système pour l'attribution de licence. La licence utilisée est Secure Client Premium.

Remarque Le reste de la configuration pour cet assistant reste la même que celle d'un contexte unique.

- Assistant d'accès à distance IPsec IKEv1, à la page 7
- Assistant VPN de site à site IPsec, à la page 2

  Pour les connexions de réseau local à réseau local utilisant l'adressage IPv4 et IPv6, l'ASA prend en charge les tunnels VPN si les deux homologues sont ASA et si les deux réseaux internes ont des schémas d'adressage correspondants (IPv4 ou IPv6). Cela est également vrai si les deux réseaux internes homologues sont IPv6 et si le réseau externe est IPv6.

Assistant VPN de site à site IPsec

Un tunnel entre deux périphériques ASA s'appelle un tunnel de site à site et est bidirectionnel. Un tunnel VPN de site à site protège les données à l'aide du protocole IPsec.

Identification de l'appareil homologue.

- Peer IP Address (Adresse IP homologue) : configurez l'adresse IP de l'autre site (périphérique homologue).
- VPN Access Interface (Interface d'accès VPN) : sélectionnez l'interface à utiliser pour le tunnel de site à site.
- Crypto Map Type (Type de carte de chiffrement) : spécifiez le type de cartes qui sera utilisé pour cet homologue, statique ou dynamique.

Trafic à protéger

Cette étape vous permet d'identifier le réseau local et le réseau distant. Ces réseaux protègent le trafic à l'aide du chiffrement IPsec.

- Local Networks (Réseaux locaux) : identifiez l'hôte utilisé dans le tunnel IPsec.
- Remote Networks (Réseaux distants) : identifiez les réseaux utilisés dans le tunnel IPsec.

Sécurité

Cette étape vous permet de configurer les méthodes d'authentification auprès du périphérique homologue. Vous pouvez soit choisir la configuration simple et fournir une clé prépartagée. Ou vous pouvez choisir une configuration personnalisée pour des options plus avancées, comme suit :

- IKE Version (Version IKE) : cochez la case IKEv1 ou IKEv2 selon la version que vous souhaitez utiliser.
- Méthodes d'authentification IKE version 1
  - Pre-shared Key (Clé prépartagée : l'utilisation d'une clé prépartagée est un moyen rapide et facile de configurer la communication avec un nombre limité d'homologues distants et un réseau stable. Cela peut entraîner des problèmes d'évolutivité dans un grand réseau, car chaque homologue IPsec nécessite des informations de configuration pour chaque homologue avec lequel il établit des connexions sécurisées.

    Chaque paire d'homologues IPsec doit échanger des clés prépartagées pour établir des tunnels sécurisés. Utilisez une méthode sécurisée pour échanger la clé prépartagée avec l'administrateur du site distant.
  - Device Certificate (Certificat de périphérique) : cliquez sur cette option pour utiliser des certificats pour l'authentification entre l'ASA local et l'homologue IPsec distant.

    Vous pouvez gérer efficacement les clés de sécurité utilisées pour établir un tunnel IPsec avec des certificats numériques. Un certificat numérique contient des informations qui identifient un utilisateur ou un périphérique, tel qu'un nom, un numéro de série, une entreprise, un service ou une adresse IP. Un certificat numérique contient également une copie de la clé publique.

    Lorsque deux homologues veulent communiquer, ils échangent des certificats et signent numériquement des données pour s'authentifier mutuellement. Lorsque vous ajoutez un nouvel homologue au réseau, il s'enregistre auprès d'une autorité de certification, et aucun des autres homologues ne nécessite de configuration supplémentaire.
- Méthodes d'authentification IKE version 2
  - Local Pre-shared Key (Clé prépartagée locale) : spécifiez les méthodes d'authentification et les algorithmes de chiffrement IPsec IKEv2.
  - Local Device Certificate (Certificat de périphérique local) : authentifie l'accès VPN au moyen du périphérique de sécurité.
  - Remote Peer Pre-shared Key (Clé prépartagée de l'homologue distant) : saisissez une clé prépartagée pour l'authentification entre l'ASA local et l'homologue IPsec distant.
  - Remote Peer Certificate Authentication (Authentification du certificat de l'homologue distant) : lorsque cette option est cochée, le périphérique homologue est autorisé à utiliser le certificat pour s'authentifier auprès de ce périphérique.

- Encryption Algorithms (Algorithmes de chiffrement) : cet onglet vous permet de choisir les types d'algorithmes de chiffrement utilisés pour protéger les données.
  - IKE Policy (Politique IKE) : spécifiez les méthodes d'authentification IKEv1/IKEv2.
  - IPsec Proposal (Proposition IPsec) : spécifiez les algorithmes de chiffrement IPsec.
- Confidentialité de transmission parfaite
  - Enable Perfect Forwarding Secrecy (PFS) (Activer la confidentialité persistante [PFS]) : spécifiez s'il faut utiliser la confidentialité persistante et la taille des nombres à utiliser pour générer les clés IPsec de phase :2. PFS est un concept cryptographique dans lequel chaque nouvelle clé n'est liée à aucune clé précédente. Dans les négociations IPsec, les clés de phase 2 sont basées sur les clés de phase 1, sauf si le protocole PFS est activé. PFS utilise des techniques Diffie-Hellman pour générer les clés.

    PFS garantit qu'une clé de session dérivée d'un ensemble de clés publiques et privées à long terme ne sera pas compromise si l'une des clés privées est compromise à l'avenir.

    Le protocole PFS doit être activé des deux côtés de la connexion.
  - Groupe Diffie-Hellman : sélectionnez l'identifiant du groupe Diffie-Hellman que les deux homologues IPsec utilisent pour obtenir un secret partagé sans le transmettre l'un à l'autre. La valeur par défaut est Group 14 (Diffie-Hellman 2048 bits).

Exemption NAT

- Exempter l'hôte/le réseau côté ASA de la traduction d'adresses : utiliser la liste déroulante pour choisir un hôte ou un réseau à exclure de la traduction d'adresses.

Assistant VPN Secure Client

Utilisez cet assistant pour configurer l'ASA afin qu'il accepte les connexions VPN du module VPN AnyConnect du client AnyConnect. Cet assistant configure les protocoles IPsec (IKEv2) ou SSL VPN pour un accès complet au réseau. L'ASA télécharge automatiquement le module VPN AnyConnect du client VPN Cisco Secure Client sur le périphérique de l'utilisateur final lorsqu'une connexion VPN est établie.

Identification du profil de connexion

L'identification du profil de connexion est utilisée pour identifier l'ASA auprès des utilisateurs de l'accès à distance :

- Connection Profile Name (Nom du profil de connexion) : fournissez un nom que les utilisateurs d'accès à distance utiliseront pour les connexions VPN.
- VPN Access Interface (Interface d'accès VPN) : choisissez une interface à laquelle les utilisateurs d'accès à distance accéderont pour les connexions VPN.

Protocoles VPN

Précisez le protocole VPN autorisé pour ce profil de connexion.

La valeur par défaut est SSL Secure Client. Si vous activez IPsec comme protocole de tunnel VPN pour le profil de connexion, vous devez également créer et déployer un profil client avec IPsec activé à l'aide de l'éditeur de profils d'ASDM, puis déployer le profil.

Si vous prédéployez le Secure Client au lieu d'utiliser le lancement Web, la première connexion client utilise SSL et reçoit le profil client de l'ASA pendant la session. Pour les connexions ultérieures, le client utilise le protocole spécifié dans le profil, soit SSL ou IPsec. Si vous prédéployez le profil avec IPsec précisé pour le client, la première connexion client utilise IPsec. Pour en savoir plus sur le prédéploiement d'un profil client avec IPsec activé, consultez le *guide d'administration AnyConnect Secure Mobility Client.*

- SSL
- IPsec (IKE v2)
- Device Certificate (Certificat de périphérique) : identifie l'ASA auprès des clients d'accès à distance. Certaines fonctionnalités Secure Client (comme la fonctionnalité permanente et IPsec/IKEv2) nécessitent un certificat de périphérique valide sur l'ASA.
- Manage (Gérer) : choisir **Manage** (Gérer) ouvre la fenêtre Manage Identity Certificates (Gérer les certificats d'identité).
  - Add (Ajouter) : choisissez **Add** (Ajouter) pour ajouter un certificat d'identité et ses détails.
  - Show Details (Afficher les détails) : si vous choisissez un certificat particulier et cliquez sur **Show Details** (Afficher les détails), la fenêtre Certificate Details (Détails du certificat) apparaît et indique à qui le certificat a été délivré et par qui il a été délivré, ainsi que des détails sur son numéro de série, son utilisation, les points de confiance associés, sa période de validité, etc.
  - Delete (Supprimer) : mettez en surbrillance le certificat que vous souhaitez supprimer et cliquez sur **Delete** (Supprimer).
  - Export (Exporter) : mettez le certificat en surbrillance et cliquez sur **Export** (Exporter) pour exporter le certificat vers un fichier avec ou sans phrase secrète de chiffrement.
  - Enroll ASA SSL VPN with Entrust (Inscrire ASA SSL VPN avec Entrust) : permet à votre appareil ASA SSL VPN d'être rapidement opérationnel avec un certificat numérique SSL Advantage d'Entrust.

Images du client

ASA peut charger automatiquement le dernier ensemble Secure Client sur le périphérique client lorsqu'il accède au réseau de l'entreprise. Vous pouvez utiliser une expression régulière pour faire correspondre l'agent utilisateur d'un navigateur à une image. Vous pouvez également réduire le temps de configuration de la connexion en déplaçant l'image utilisée par le système d'exploitation le plus courant qui figure en haut de la liste.

Méthodes d'authentification

Précisez les informations d'authentification sur cet écran.

- AAA server group (Groupe de serveurs AAA) : activez cette option pour permettre à l'ASA de communiquer avec un groupe de serveurs AAA distant afin d'authentifier l'utilisateur. Sélectionnez un groupe de serveurs AAA dans la liste des groupes préconfigurés ou cliquez sur **New** (Nouveau) pour créer un nouveau groupe.

- Local User Database Details (Détails de la base de données des utilisateurs locaux) : ajoutez de nouveaux utilisateurs à la base de données locale stockée sur l'ASA.
  - Username (Nom d'utilisateur) : créez un nom d'utilisateur pour l'utilisateur.
  - Password (Mot de passe) : créez un mot de passe pour l'utilisateur.
  - Confirm Password (Confirmer le mot de passe) : saisissez de nouveau le même mot de passe pour le confirmer.
  - Add/Delete (Ajouter/Supprimer) : ajoutez ou supprimez l'utilisateur de la base de données locale.

Attribution d'adresses client

Indiquez une plage d'adresses IP aux utilisateurs Secure Client distants.

- IPv4 Address Pools (Ensembles d'adresses IPv4) : les clients VPN SSL reçoivent de nouvelles adresses IP lorsqu'ils se connectent à l'ASA. Les connexions sans client ne nécessitent pas de nouvelles adresses IP. Les ensembles d'adresses définissent une plage d'adresses que les clients distants peuvent recevoir. Sélectionnez un ensemble d'adresses IP existant ou cliquez sur **New** (Nouveau) pour créer un nouvel ensemble.

  Si vous choisissez **New** (Nouveau), vous devrez fournir une adresse IP de début, une adresse IP de fin et un masque de sous-réseau.

- IPv6 Address Pool (Ensemble d'adresses IPv6) : sélectionnez un ensemble d'adresses IP existant ou cliquez sur **New** (Nouveau) pour créer un nouvel ensemble.

Remarque Les ensembles d'adresses IPv6 ne peuvent pas être créés pour les profils de connexion IKEv2.

Serveurs de résolution de noms réseau)

Précisez quels noms de domaine sont résolus pour l'utilisateur distant lors de l'accès au réseau interne.

- DNS Servers (Serveurs DNS) : saisissez l'adresse IP du serveur DNS.
- WINS Servers (Serveurs WINS) : saisissez l'adresse IP du serveur WINS.
- Domain Name (Nom de domaine) : saisissez le nom de domaine par défaut.

Exemption NAT

Si la traduction de réseau est activée sur l'ASA, le trafic VPN doit être exempt de cette traduction.

Déploiement Secure Client

Vous pouvez installer le programme Secure Client sur un périphérique client en utilisant l'une des deux méthodes suivantes :

- Web launch (Lancement Web) : le progiciel Secure Client s'installe automatiquement lors de l'accès à l'ASA à l'aide d'un navigateur Web.

Remarque Web launch (Lancement Web) n'est pas pris en charge en mode contexte multiple.

- Pre-deployment (Prédéploiement) : installez manuellement le progiciel Secure Client.

Allow Web Launch (Autoriser le lancement Web) est un paramètre global qui affecte toutes les connexions. Si cette option n'est pas cochée (non autorisée), les connexions SSL Secure Client et les connexions SSL sans client ne fonctionnent pas.

Pour le prédéploiement, l'ensemble de profils disk0:/test2_client_profile.xml contient un fichier .msi, et vous devez inclure ce profil client de l'ASA dans votre progiciel Secure Client afin d'assurer le bon fonctionnement des connexions IPsec.

Assistant d'accès à distance IPsec IKEv1

Remarque Le client VPN Cisco est en fin de vie et n'est plus pris en charge. Vous devez passer au client de Secure Client/AnyConnect.

Utilisez l'assistant d'accès à distance IKEv1 pour configurer l'accès à distance sécurisé pour les clients VPN, tels que les utilisateurs mobiles, et pour identifier l'interface qui se connecte à l'homologue IPsec distant.

- VPN Tunnel Interface (Interface de tunnel VPN) : choisissez l'interface à utiliser pour les clients d'accès à distance. Si l'ASA a plusieurs interfaces, arrêtez maintenant et configurez les interfaces sur l'ASA avant d'exécuter cet assistant.
- Enable inbound IPsec sessions to bypass interface access lists (Activer les sessions IPsec entrantes pour contourner les listes d'accès d'interface) : active les sessions entrantes authentifiées IPsec afin qu'elles soient toujours autorisées par l'ASA (c'est-à-dire sans vérifier les instructions des listes d'accès d'interface). Sachez que les sessions entrantes contournent uniquement les listes de contrôle d'accès de l'interface. Les stratégies de groupe configurées, les utilisateurs et les listes de contrôle d'accès téléchargées s'appliquent toujours.

Client d'accès à distance

Les utilisateurs d'accès à distance de différents types peuvent ouvrir des tunnels VPN vers cet ASA. Choisissez le type de client VPN pour ce tunnel.

- Type de client VPN
  - produit Easy VPN Remote.
  - Client Microsoft Windows utilisant L2TP sur IPsec : spécifiez le protocole d'authentification PPP. Les choix sont PAP, CHAP, MS-CHAP-V1, MS-CHAP-V2 et EAP-PROXY :

    Le PAP transmet un nom d'utilisateur et un mot de passe en clair lors de l'authentification et n'est pas sécurisé.

Avec le protocole CHAP, le client renvoie le [défi plus mot de passe] chiffré, avec un nom d'utilisateur en texte clair en réponse au défi du serveur. Le protocole CHAP est plus sécurisé que le protocole PAP, mais il ne chiffre pas les données.

MS-CHAP, version 1 : 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.

MS-CHAP, version 2 : contient des améliorations de sécurité par rapport à MS-CHAP, version 1.

EAP-Proxy : active le protocole EAP qui permet à l'ASA de proxy le processus d'authentification PPP à un serveur d'authentification RADIUS externe.

Si un protocole n'est pas spécifié sur le client distant, ne le spécifiez pas.

- Précisez si le client enverra le nom du groupe de tunnels sous la forme d'un nom d'utilisateur@tunnelgroup.

Méthode d'authentification du client VPN et nom du groupe de tunnels

Utilisez le volet VPN Client Authentication Method and Name (Méthode d'authentification et nom du client VPN) pour configurer une méthode d'authentification et créer une politique de connexion (groupe de tunnels).

- Authentication Method (Méthode d'authentification) : l'homologue du site distant s'authentifie à l'aide d'une clé prépartagée ou d'un certificat.
  - Pre-shared Key (Clé prépartagée) : cliquez pour utiliser une clé prépartagée pour l'authentification entre l'ASA local et l'homologue IPsec distant.

    L'utilisation d'une clé prépartagée est un moyen rapide et facile d'établir la communication avec un nombre limité d'homologues distants et un réseau stable. Cela peut entraîner des problèmes d'évolutivité dans un grand réseau, car chaque homologue IPsec nécessite des informations de configuration pour chaque homologue avec lequel il établit des connexions sécurisées.

    Chaque paire d'homologues IPsec doit échanger des clés prépartagées pour établir des tunnels sécurisés. Utilisez une méthode sécurisée pour échanger la clé prépartagée avec l'administrateur du site distant.

  - re-shared Key (Clé prépartagée) : saisissez une chaîne alphanumérique comprise entre 1 et 128 caractères.

  - Certificate (Certificat) : cliquez pour utiliser des certificats pour l'authentification entre l'ASA local et l'homologue IPsec distant. Pour remplir cette section, vous devez vous être déjà inscrit auprès d'une autorité de certification et avoir téléchargé un ou plusieurs certificats sur l'ASA.

    Vous pouvez gérer efficacement les clés de sécurité utilisées pour établir un tunnel IPsec avec des certificats numériques. Un certificat numérique contient des informations qui identifient un utilisateur ou un périphérique, tel qu'un nom, un numéro de série, une entreprise, un service ou une adresse IP. Un certificat numérique contient également une copie de la clé publique.

    Pour utiliser des certificats numériques, chaque homologue s'inscrit auprès d'une autorité de certification (CA), qui est responsable d'émettre des certificats numériques. Une autorité de certification peut être un tiers de confiance ou une autorité de certification privée que vous établissez au sein de votre organisation.

    Lorsque deux homologues veulent communiquer, ils échangent des certificats et signent numériquement des données pour s'authentifier mutuellement. Lorsque vous ajoutez un nouvel

homologue au réseau, il s'enregistre auprès d'une autorité de certification, et aucun des autres homologues ne nécessite de configuration supplémentaire.

Algorithme de signature de certificat : affiche l'algorithme de signature des certificats numériques, rsa-sig pour RSA.

- Tunnel Group Name (Nom du groupe de tunnels) : saisissez un nom pour créer l'enregistrement qui contient les politiques de connexion de tunnel pour cette connexion IPsec. Une politique de connexion peut préciser les serveurs d'authentification, d'autorisation et de comptabilité, une Stratégie de groupe par défaut et des attributs IKE. Une politique de connexion que vous configurez avec cet assistant VPN spécifie une méthode d'authentification et utilise la stratégie de groupe par défaut de l'ASA.

Authentification du client

Utilisez le volet Client Authentication (authentification du client) pour choisir la méthode par laquelle l'ASA authentifie les utilisateurs distants. Sélectionnez l'une des options suivantes :

- Authenticate using the local user database (Authentifier à l'aide de la base de données d'utilisateurs locaux) : cliquez pour utiliser l'authentification interne à l'ASA. Utilisez cette méthode pour les environnements avec un nombre faible et stable d'utilisateurs. Le volet suivant vous permet de créer des comptes sur l'ASA pour les utilisateurs individuels.
- Authenticate using an AAA server group (Authentifier à l'aide d'un groupe de serveurs AAA) : cliquez pour utiliser un groupe de serveurs externe pour l'authentification des utilisateurs distants.
  - AAA Server Group Name (Nom du groupe de serveurs AAA) : choisissez un groupe de serveurs AAA configuré précédemment.
  - New... (Nouveau...) : cliquez pour configurer un nouveau groupe de serveurs AAA.

Comptes utilisateurs

Utilisez le volet User Accounts (Comptes d'utilisateurs) pour ajouter de nouveaux utilisateurs à la base de données d'utilisateurs interne de l'ASA à des fins d'authentification.

Ensemble d'adresses

Utilisez le volet Address Pool (Ensemble d'adresses) pour configurer un ensemble d'adresses IP locales que l'ASA attribue aux clients VPN distants.

- Nom du groupe de tunnels : affiche le nom du profil de connexion (groupe de tunnels) auquel cet ensemble d'adresses s'applique. Vous définissez ce nom dans le volet VPN Client and Authentication Method (Client VPN et méthode d'authentification) (étape 3).
- Nom de l'ensemble : sélectionnez un identifiant descriptif pour l'ensemble d'adresses.
- New... (Nouveau...) : cliquez pour configurer un nouvel ensemble d'adresses.
- Adresse de début de plage : saisissez l'adresse IP de début dans l'ensemble d'adresses.
- Adresse de fin de plage : saisissez l'adresse IP de fin dans l'ensemble d'adresses.
- Masque de sous-réseau : (facultatif) choisissez le masque de sous-réseau pour ces adresses IP.

Attributs transmis au client (facultatif)

Utilisez le volet Attributes Pushed to Client (Attributs transmis au client) (facultatif) pour que l'ASA transmette des informations sur les serveurs DNS et WINS et le nom de domaine par défaut aux clients d'accès à distance.

- Groupe de tunnels : affiche le nom de la politique de connexion à laquelle l'ensemble d'adresses s'applique. Vous définissez ce nom dans le volet VPN Client Name and Authentication Method (Nom du client VPN et méthode d'authentification).
- Serveur DNS principal : saisissez l'adresse IP du serveur DNS principal.
- Serveur DNS secondaire : saisissez l'adresse IP du serveur DNS secondaire.
- Serveur WINS principal : saisissez l'adresse IP du serveur WINS principal.
- Serveur WINS secondaire : saisissez l'adresse IP du serveur WINS secondaire.
- Nom de domaine par défaut : saisissez le nom de domaine par défaut.

Politique IKE

IKE, également appelé protocole Internet Security Association and Key Management (ISAKMP), est le protocole de négociation qui permet à deux hôtes de se mettre d'accord sur la façon de créer une association de sécurité IPsec. Chaque négociation IKE est divisée en deux sections appelées Phase 1 et Phase 2. La phase 1 crée le premier tunnel, qui protège les messages de négociation IKE ultérieurs. La phase 2 crée le tunnel qui protège les données.

Utilisez le volet IKE Policy (Politique IKE) pour définir les conditions des négociations IKE de phase 1, qui comprennent une méthode de chiffrement pour protéger les données et assurer la confidentialité, une méthode d'authentification pour assurer l'identité des homologues et un groupe Diffie-Hellman pour établir la force de l'algorithme de détermination de la clé de chiffrement. L'ASA utilise cet algorithme pour déduire les clés de chiffrement et de hachage.

- Chiffrement : sélectionnez l'algorithme de chiffrement symétrique que l'ASA utilise pour établir le SA de phase 1 qui protège les négociations de phase 2. L'ASA prend en charge les algorithmes de chiffrement suivants :

Algorithme	Explication
DES	Standard de chiffrement des données. Utilise une clé de 56 bits.
3DES	Triple DES. Effectue le chiffrement à trois reprises à l'aide d'une clé de 56 bits.
AES-128	Standard de chiffrement avancé (AES). Utilise une clé de 128 bits.
AES-192	AES à l'aide d'une clé de 192 bits.
AES-256	AES à l'aide d'une clé de 256 bits.

  La valeur par défaut, 3DES, est plus sécurisée que DES, mais nécessite plus de traitement pour le chiffrement et le déchiffrement. De même, les options AES offrent une sécurité renforcée, mais nécessitent également un traitement renforcé.

- Authentification : choisissez l'algorithme de hachage utilisé pour l'authentification et assurer l'intégrité des données. La valeur par défaut est SHA. MD5 a un condensé plus petit et est considéré comme

légèrement plus rapide que SHA. Il y a eu une démonstration d'attaque réussie (mais très difficile) contre MD5. Cependant, la version du code d'authentification du message Keyed-Hash (HMAC) utilisée par l'ASA empêche cette attaque.

- Groupe Diffie-Hellman : choisissez l'identifiant du groupe Diffie-Hellman, que les deux homologues IPsec utilisent pour obtenir un secret partagé sans le transmettre l'un à l'autre. Le groupe DH par défaut, groupe 14 (2 048 bits), est considéré comme plus sécurisé que les groupes 2 et 5.

Paramètres d'IPsec (facultatif)

Utilisez le volet IPsec Settings (Paramètres d'IPsec) (facultatif) pour identifier les hôtes ou les réseaux locaux qui ne nécessitent pas de traduction d'adresses. Par défaut, l'ASA cache les adresses IP réelles des hôtes internes et des réseaux des hôtes externes en utilisant la traduction d'adresses réseau (NAT) dynamique ou statique. La NAT réduit les risques d'attaque par des hôtes externes non fiables, mais peut être inappropriée pour ceux qui ont été authentifiés et protégés par VPN.

Par exemple, un hôte interne utilisant la NAT dynamique voit son adresse IP traduite en la faisant correspondre à une adresse sélectionnée au hasard dans un ensemble. Seule l'adresse traduite est visible à l'extérieur. Les clients VPN distants qui tentent d'atteindre ces hôtes en envoyant des données à leurs adresses IP réelles ne peuvent pas se connecter à ces hôtes, sauf si vous configurez une règle d'exemption NAT.

Remarque Si vous souhaitez que tous les hôtes et les réseaux soient exemptés de la NAT, ne configurez rien dans ce volet. Si vous avez même une entrée, tous les autres hôtes et réseaux sont soumis à la NAT.

- Interface : choisissez le nom de l'interface qui se connecte aux hôtes ou aux réseaux que vous avez sélectionnés.
- Réseaux exemptés : sélectionnez l'adresse IP de l'hôte ou du réseau que vous souhaitez exempter du réseau de l'interface choisie.
- Enable split tunneling (Activer la tunnellisation fractionnée) : sélectionnez cette option pour que le trafic des clients d'accès à distance destiné à l'Internet public soit envoyé non chiffré. La tunnellisation fractionnée entraîne le chiffrement du trafic vers les réseaux protégés, tandis que le trafic vers des réseaux non protégés n'est pas chiffré. Lorsque vous activez la tunnellisation fractionnée, l'ASA envoie une liste d'adresses IP au client VPN distant après l'authentification. Le client VPN distant chiffre le trafic vers les adresses IP qui se trouvent derrière l'ASA. Tout autre trafic circule non chiffré directement sur Internet, sans faire appel à l'ASA.
- Enable Perfect Forward Secrecy (PFS) (Activer la confidentialité de transmission parfaite [PFS]) : spécifiez s'il faut utiliser la confidentialité de transmission parfaite et la taille des nombres à utiliser dans la génération des clés IPsec de phase 2. PFS est un concept cryptographique dans lequel chaque nouvelle clé n'est liée à aucune clé précédente. Dans les négociations IPsec, les clés de phase 2 sont basées sur les clés de phase 1, sauf si le protocole PFS est activé. PFS utilise des techniques Diffie-Hellman pour générer les clés.

  PFS garantit qu'une clé de session dérivée d'un ensemble de clés publiques et privées à long terme ne sera pas compromise si l'une des clés privées est compromise à l'avenir.

  Le protocole PFS doit être activé des deux côtés de la connexion.

  - Groupe Diffie-Hellman : sélectionnez l'identifiant du groupe Diffie-Hellman que les deux homologues IPsec utilisent pour obtenir un secret partagé sans le transmettre l'un à l'autre. Le groupe DH par défaut, groupe 14 (2 048 bits), est considéré comme plus sécurisé que les groupes 2 et 5.

Résumé

Lorsque vous êtes satisfait de la configuration, cliquez sur **Finish** (Terminer). ASDM enregistre la configuration LAN à LAN. Après avoir cliqué sur **Finish** (Terminer), vous ne pouvez plus utiliser l'assistant VPN pour modifier cette configuration. Utilisez ASDM pour modifier et configurer les fonctionnalités avancées.

Assistant d'accès à distance IPsec IKEv2

Utilisez l'assistant d'accès à distance IKEv2 pour configurer l'accès à distance sécurisé pour les clients VPN, tels que les utilisateurs mobiles, et pour identifier l'interface qui se connecte à l'homologue IPsec distant.

Identification du profil de connexion

Saisissez un **nom de profil de connexion** et choisissez l'**interface d'accès VPN** qui sera utilisée pour l'accès à distance IPsec IKEv2.

- Nom du profil de connexion : saisissez un nom pour créer l'enregistrement qui contient les politiques de connexion de tunnel pour cette connexion IPsec. Une politique de connexion peut préciser les serveurs d'authentification, d'autorisation et de comptabilité, une Stratégie de groupe par défaut et des attributs IKE. Une politique de connexion que vous configurez avec cet assistant VPN spécifie une méthode d'authentification et utilise la stratégie de groupe par défaut de l'ASA.
- Interface d'accès VPN : choisissez l'interface qui établit un tunnel sécurisé avec l'homologue IPsec distant. Si l'ASA dispose de plusieurs interfaces, vous devez planifier la configuration VPN avant d'exécuter cet assistant, en identifiant l'interface à utiliser pour chaque homologue IPsec distant avec lequel vous prévoyez d'établir une connexion sécurisée.

Page d'authentification IPsec basée sur les normes (IKEv2)

Authentification d'homologue IKE : l'homologue du site distant s'authentifie à l'aide d'une clé prépartagée, d'un certificat ou de l'authentification d'homologue à l'aide du protocole EAP.

- Clé prépartagée : saisissez une chaîne alphanumérique comprise entre 1 et 128 caractères.

  L'utilisation d'une clé prépartagée est un moyen rapide et facile d'établir la communication avec un nombre limité d'homologues distants et un réseau stable. Cela peut entraîner des problèmes d'évolutivité dans un grand réseau, car chaque homologue IPsec nécessite des informations de configuration pour chaque homologue avec lequel il établit des connexions sécurisées.

  Chaque paire d'homologues IPsec doit échanger des clés prépartagées pour établir des tunnels sécurisés. Utilisez une méthode sécurisée pour échanger la clé prépartagée avec l'administrateur du site distant.

- Activer l'authentification des certificats : vous permet d'utiliser des certificats pour l'authentification si cette option est cochée.
- Activer l'authentification homologue à l'aide d'EAP : vous permet d'utiliser EAP pour l'authentification si cette option est cochée. Vous devez utiliser des certificats pour l'authentification locale si vous cochez cette case.
- Envoyer une demande d'identité EAP au client : vous permet d'envoyer une demande EAP d'authentification au client VPN d'accès à distance.

Mobike RRC

- Activer la vérification de la routabilité du retour pour mobike : activer la vérification de la routabilité du retour pour les modifications d'adresses IP dynamiques dans les associations de sécurité IKE/IPSEC sur lesquelles mobike est activé.

Authentification IKE

- Activez l'authentification locale et sélectionnez une clé prépartagée ou un certificat
  - Clé prépartagée : saisissez une chaîne alphanumérique comprise entre 1 et 128 :caractères.
  - Certificat : cliquez sur pour utiliser des certificats pour l'authentification entre l'ASA local et l'homologue IPsec distant. Pour remplir cette section, vous devez vous être déjà inscrit auprès d'une autorité de certification et avoir téléchargé un ou plusieurs certificats sur cette dernière.

    Vous pouvez gérer efficacement les clés de sécurité utilisées pour établir un tunnel IPsec avec des certificats numériques. Un certificat numérique contient des informations qui identifient un utilisateur ou un périphérique, tel qu'un nom, un numéro de série, une entreprise, un service ou une adresse IP. Un certificat numérique contient également une copie de la clé publique.

    Pour utiliser des certificats numériques, chaque homologue s'inscrit auprès d'une autorité de certification (CA), qui est responsable d'émettre des certificats numériques. Une autorité de certification peut être un tiers de confiance ou une autorité de certification privée que vous établissez au sein de votre organisation.

    Lorsque deux homologues veulent communiquer, ils échangent des certificats et signent numériquement des données pour s'authentifier mutuellement. Lorsque vous ajoutez un nouvel homologue au réseau, il s'enregistre auprès d'une autorité de certification, et aucun des autres homologues ne nécessite de configuration supplémentaire.

Méthodes d'authentification

Seule l'authentification Radius est prise en charge pour l'accès à distance IPsec IKEv2.

- Groupe de serveurs AAA : choisissez un groupe de serveurs AAA configuré précédemment.
- Nouveau : cliquez sur pour configurer un nouveau groupe de serveurs AAA.
- Détails du groupe de serveur AAA : utilisez cette zone pour modifier le groupe de serveur AAA si vous le souhaitez.

Attribution d'adresses client

Créez ou sélectionnez des ensembles d'adresses IPv4 et IPv6. Les clients d'accès à distance se verront attribuer des adresses issues de pools IPv4 ou IPv6. Les adresses IPv4 prévalent si les deux sont configurées. Consultez *Configuration des ensembles d'adresses IP locales* pour en savoir plus.

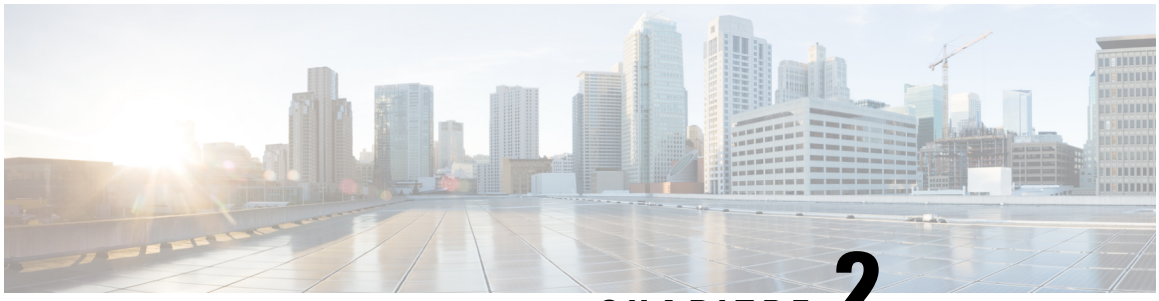
Serveurs de résolution de noms réseau

Précisez comment les noms de domaine sont résolus pour l'utilisateur distant lors de l'accès au réseau interne.

- Serveurs DNS : saisissez l'adresse IP des serveurs DNS.
- Serveurs WINS : saisissez l'adresse IP des serveurs WINS.
- Nom de domaine par défaut : saisissez le nom de domaine par défaut.

Exemption NAT

- Exempter le trafic VPN de la traduction d'adresses réseau : si la NAT est activée sur l'appareil de sécurité adaptable Cisco, cela doit être vérifié.



CHAPITRE 2

IKE

Configurer le protocole d'échange de clés de chiffrement (IKE)

IKE, également appelé ISAKMP, est le protocole de négociation qui permet à deux hôtes de se mettre d'accord sur la façon de créer une association de sécurité IPsec. Pour configurer l'ASA pour les réseaux privés virtuels, vous définissez des paramètres IKE globaux qui s'appliquent à l'échelle du système et vous créez également des politiques IKE que les homologues négocient pour établir une connexion VPN.

Procédure

Étape 1 Activer IKE, à la page 15.

Étape 2 Définir les Paramètres IKE pour le VPN de site à site, à la page 16.

Étape 3 Configurer les Politiques IKE, à la page 22.

Activer IKE

Procédure

Étape 1 Pour activer IKE pour les connexions VPN :

a) Dans ASDM, choisissez Configuration (**Configuration) > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Secure Client Connection Profiles (Profils de connexion Secure Client/AnyConnect**).

b) Dans la zone Access Interfaces (Interfaces d'accès), cochez **Allow Access** (Autoriser l'accès) sous IPsec (IKEv2) Access (Accès IPsec [IKEv2]) pour les interfaces sur lesquelles vous utiliserez IKE.

Étape 2 Pour activer IKE pour le VPN de site à site :

a) Dans ASDM, choisissez Configuration (**Configuration) > Site-to-Site VPN (VPN de site à site) > Connection Profiles (Profils de connexion)**.
b) Sélectionnez les interfaces sur lesquelles vous souhaitez utiliser IKEv1 et IKEv2.

Paramètres IKE pour le VPN de site à site

Dans ASDM, choisissez **Configuration > Site-to-Site VPN > Advanced > IKE Parameters** (Configuration > VPN de site à site > Avancé > Paramètres IKE).

Transparence NAT

- Activer IPsec sur NAT-T

  IPsec sur NAT-T permet aux homologues IPsec d'établir des connexions d'accès à distance et de réseau local (LAN) par l'intermédiaire d'un périphérique NAT. Il le fait en encapsulant le trafic IPsec dans des datagrammes UDP, en utilisant le port 4500, fournissant ainsi 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. Cette fonction est activée par défaut.

  - 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.
  - Lorsque NAT-T et IPsec sur UDP sont activés, NAT-T prévaut.
  - Lorsque cette option est activée, IPsec sur TCP prévaut sur toutes les autres méthodes de connexion.

  La mise en œuvre de l'ASA de NAT-T prend en charge les homologues IPsec derrière un seul périphérique NAT/PAT comme suit :

  - Une connexion de réseau local (LAN) à réseau local (LAN).
  - Il s'agit d'une connexion de réseau local (LAN) ou de plusieurs clients d'accès à distance, mais pas d'un mélange des deux.

  Pour utiliser NAT-T, vous devez :

  - Créez une liste de contrôle d'accès pour l'interface que vous utiliserez afin d'ouvrir le port 4500 (Configuration > Firewall > Access Rules [Configuration > Pare-feu > Règles d'accès]).
  - Activez IPsec sur NAT-T dans ce volet.
  - Dans le paramètre Fragmentation Policy (Politique de fragmentation) du volet Configuration > Site-to-Site VPN > Advanced > IPsec Prefragmentation Policies (Configuration > VPN de site à site > Avancé > Politiques de préfragmentation IPsec), modifiez l'interface que vous utiliserez pour activer la préfragmentation IPsec. Lorsque cela est configuré, il est toujours acceptable de laisser le trafic passer par les périphériques NAT qui ne prennent pas en charge la fragmentation IP; ils n'affectent pas le fonctionnement des périphériques NAT qui le font.

- Activez IPsec sur TCP

  IPsec sur TCP permet à un client VPN d'évoluer dans un environnement dans lequel l'ESP ou IKE standard ne peut pas fonctionner ou ne peut fonctionner qu'avec modification des règles de pare-feu existantes. IPsec sur TCP encapsule les protocoles IKE et IPsec dans un paquet TCP et permet la

tunnellisation sécurisée à travers les périphériques et les pare-feu NAT et PAT. Par défaut, cette fonction est désactivée.

Remarque Cette fonctionnalité ne fonctionne pas avec les pare-feu basés sur des proxys.

IPsec sur TCP fonctionne avec les clients d'accès à distance. Il fonctionne sur toutes les interfaces physiques et VLAN. Il s'agit d'une fonctionnalité de client pour ASA uniquement. 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.
- Lorsque cette option est activée, IPsec sur TCP prévaut sur toutes les autres méthodes de connexion.

Vous activez IPsec sur TCP sur l'ASA et sur le client auquel il se connecte.

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 fonctionnera plus. Par conséquent, vous ne pouvez plus utiliser de navigateur pour gérer l'ASA au moyen de l'interface compatible avec IKE. Pour résoudre ce problème, reconfigurez la gestion HTTP/HTTPS sur différents ports.

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.

Identité envoyée aux homologues

Choisissez l'**identité** que les homologues utiliseront pour s'identifier pendant les négociations IKE :

Address	Utilise les adresses IP des hôtes qui échangent des informations d'identité ISAKMP.
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	L'homologue distant utilise la **chaîne d'identifiant de clé** que vous spécifiez pour rechercher la clé prépartagée.
Automatic	Détermine la négociation IKE par type de connexion : • Adresse IP pour la clé prépartagée • Cert DN pour l'authentification par certificat.

Contrôle de session

- Désactiver les connexions entrantes en mode progressif

  Les négociations IKE de phase 1 peuvent utiliser le mode principal ou le mode progressif. Les deux fournissent les mêmes services, mais le mode progressif ne nécessite que deux échanges entre les homologues, au lieu de trois. Le mode agressif est plus rapide, mais ne fournit pas de protection d'identité pour les parties qui communiquent. Il est donc nécessaire qu'ils échangent des informations d'identification avant d'établir une SA sécurisée dans laquelle chiffrer les informations. Par défaut, cette fonction est désactivée.

- Alerter les homologues avant la déconnexion
  - Les sessions client ou de réseau local (LAN) peuvent être abandonnées pour plusieurs raisons, telles que : l'arrêt ou le redémarrage de l'ASA, le délai d'inactivité de la session, le temps de connexion maximal dépassé ou l'arrêt de l'administrateur.
  - L'ASA peut notifier les homologues admissibles (dans les configurations de réseau local [LAN] à réseau local [LAN]) des sessions qui sont sur le point d'être déconnectées et leur transmettre la raison. L'homologue ou le client qui reçoit l'alerte décode la raison et l'affiche dans le journal des événements ou dans une fenêtre contextuelle. Par défaut, cette fonction est désactivée.
  - Ce volet vous permet d'activer la fonctionnalité pour que l'ASA envoie ces alertes et transmette la raison de la déconnexion.

  Les clients et homologues admissibles sont les suivants :
  - Appareils de sécurité avec Alerts (Alertes) activé.
  - Clients VPN exécutant la version 4.0 ou ultérieure (aucune configuration requise).

- Attendre que toutes les sessions actives se terminent volontairement avant le redémarrage

  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.

- Nombre de SA autorisées dans la négociation pour IKEv1

  Limite le nombre maximal de SA qui peuvent être en négociation à tout moment.

Paramètres spécifiques IKE v2

Davantage de contrôles de session sont disponibles pour IKE v2, ce qui limite le nombre de SA ouvertes. Par défaut, l'ASA ne limite pas le nombre de SA ouvertes :

- Cookie Challenge (Défi des témoins) : permet à l'ASA d'envoyer des défis liés aux témoins aux périphériques homologues en réponse aux paquets initiés par la SA.
  - % du seuil avant que les SA entrantes ne soient contestées par les témoins : le pourcentage du nombre total de SA autorisées pour l'ASA qui sont en négociation, ce qui déclenche la contestation des témoins pour les futures négociations d'une SA. La plage va de zéro à 100 %. La valeur par défaut est de 50 %.

- Nombre de SA autorisées dans la négociation : limite le nombre maximal de SA qui peuvent être en négociation à tout moment. S'il est utilisé avec le Cookie Challenge (Défi des témoins), configurez le seuil de défi pour les témoins sur une valeur inférieure à cette limite pour une vérification par recoupement efficace.
- Nombre maximal de SA autorisées : limite le nombre de connexions IKEv2 autorisées. Par défaut, la limite est le nombre maximal de connexions spécifiées par la licence.
- Notify Invalid Selector (Notification d'un sélecteur non valide) : permet à un administrateur d'activer ou de désactiver l'envoi d'une notification IKE à l'homologue lorsqu'un paquet entrant reçu sur une SA ne correspond pas aux sélecteurs de trafic de cette SA. L'envoi de cette notification est désactivé par défaut.

Prévention des attaques DoS avec les paramètres spécifiques IKE v2

Vous pouvez empêcher les attaques par déni de service (DoS) pour les connexions IPsec IKEv2 en configurant Cookie Challenge (Défi des témoins), qui remet en question l'identité des associations de sécurité (SA) entrantes, ou en limitant le nombre de SA ouvertes. Par défaut, l'ASA ne limite pas le nombre de SA ouvertes et ne met jamais en cause les témoins. Vous pouvez également limiter le nombre de SA autorisées, ce qui empêche d'autres connexions de négocier afin de protéger contre les attaques de mémoire et/ou de CPU que la fonctionnalité Cookie Challenge (Défi des témoins) pourrait ne pas être en mesure de déjouer, et protège les connexions actuelles.

Avec une attaque DoS, un agresseur lance l'attaque lorsque l'appareil homologue envoie un paquet d'initialisation SA et que l'ASA envoie sa réponse, mais l'appareil homologue ne répond pas. Si le périphérique homologue le fait continuellement, toutes les requêtes SA autorisées sur l'ASA peuvent être utilisées jusqu'à ce qu'il arrête de répondre.

L'activation d'un pourcentage de seuil pour la contestation des témoins limite le nombre de négociations d'un SA ouvertes. Par exemple, avec le paramètre par défaut de 50 %, lorsque 50 % des SA autorisées sont en négociation (ouvertes), le témoin ASA conteste tous les paquets d'initialisation SA supplémentaires qui arrivent.

S'il est utilisé simultanément avec le **Number of SAs Allowed in Negotiation** ou le Nombre maximal de SA autorisées, configurez le seuil de contestation des témoins sur une valeur inférieure à ces paramètres pour une vérification par recoupement efficace.

Vous pouvez également limiter la durée de vie de tous les SA au niveau IPsec en choisissant Configuration > Site-to-Site VPN > Advanced > System Options (Configuration > VPN de site à site > Avancé > Options système).

À propos de la carte de chiffrement IKEv2 multi-homologues

À partir de la version 9.14(1), ASA IKEv2 prend en charge les cartes 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 de plusieurs homologues sur IKEv2 est utile, en particulier 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 sont utilisées pour accepter la demande des homologues qui initient le tunnel.

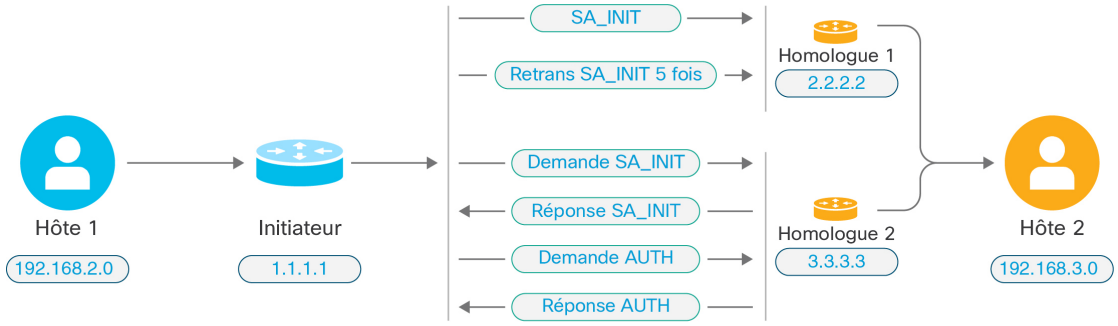
Comportement de l'initiateur IKEv2

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 épuisés, IKEv2 relance la session à partir de Peer1 jusqu'à ce qu'une SA soit établie avec l'un des homologues. La figure suivante décrit 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 de chiffrement,.

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

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

Lignes directrices relatives à l'homologue multiple IKEv2

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 Peer1, indépendamment du déplacement de la carte de chiffrement vers l'adresse IP 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 à homologues multiples IKEv2 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.
```

Politiques IKE

Configuration > Site-to-Site VPN (VPN de site à site) > Advanced (Avancé) > IKE Policies (Politiques IKE)

Utilisez ce volet pour ajouter, modifier ou supprimer des politiques IKEv1 et IKEv2.

Pour définir les conditions des négociations IKE, vous créez une ou plusieurs politiques IKE, qui comprennent les éléments suivants :

- Une priorité unique (de 1 à 65 543, 1 étant la priorité la plus élevée).
- 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 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 établir la force de l'algorithme de détermination de la clé de chiffrement. L'ASA utilise cet algorithme pour déduire les clés de chiffrement et de hachage.
- Une limite de temps pendant laquelle l'ASA utilise une clé de chiffrement avant de la remplacer.

Chaque négociation IKE est divisée en deux sections appelées Phase 1 et Phase 2. La phase 1 crée le premier tunnel, qui protège les messages de négociation IKE ultérieurs. La phase 2 crée le tunnel qui protège les données.

Pour IKEv1, vous ne pouvez activer qu'un seul paramètre pour chaque paramètre. Pour IKEv2, chaque proposition peut comporter plusieurs paramètres pour Encryption (Chiffrement), D-H Group (Groupe D-H), Integrity Hash (Hachage d'intégrité) et PRF Hash (Hachage PRF).

Si vous ne configurez aucune politique IKE, l'ASA utilise la politique par défaut, qui est toujours définie à la priorité la plus basse et qui contient la valeur par défaut pour chaque paramètre. Si vous ne spécifiez pas de valeur pour un paramètre spécifique, la valeur par défaut prend effet.

Lorsque la négociation IKE commence, l'homologue qui initie la négociation envoie toutes ses politiques à l'homologue distant, et ce dernier recherche une correspondance avec ses propres politiques, par ordre de priorité.

Il existe une correspondance entre les politiques IKE si elles ont les mêmes valeurs de chiffrement, de hachage, d'authentification et de Diffie-Hellman, ainsi qu'une durée de vie SA inférieure o Si les durées de vie ne sont pas identiques, la durée de vie la plus courte (de l'homologue distant) s'applique. Si aucune correspondance n'existe, IKE refuse la négociation et l'IKE SA n'est pas établie.

Champs

- IKEv1 Policies (Politiques IKEv1) : affiche les paramètres de chaque politique IKE configurée.
  - Priority # (Priorité #) : affiche la priorité de la politique.
  - Encryption (Chiffrement) : affiche la méthode de chiffrement.
  - Hash (Hachage) : affiche l'algorithme de hachage.
  - D-H Group (Groupe D-H) : affiche le groupe Diffie-Hellman.
  - Authentication (Authentification) : affiche la méthode d'authentification.
  - Lifetime (secs) (Durée de vie [s]) : affiche la durée de vie de la SA en secondes.
- IKEv2 Policies (Politiques IKEv2) : affiche les paramètres de chaque politique IKEv2 configurée.
  - Priority # (Priorité #) : affiche la priorité de la politique.
  - Encryption (Chiffrement) : affiche la méthode de chiffrement.
  - Integrity Hash (Hachage d'intégrité) : affiche l'algorithme de hachage.
  - PRF Hash (Hachage PRF) : affiche l'algorithme de hachage de la fonction pseudo-aléatoire (PRF).
  - D-H Group (Groupe D-H) : affiche le groupe Diffie-Hellman.
  - Lifetime (secs) (Durée de vie [s]) : affiche la durée de vie de la SA en secondes.

Créer ou modifier une politique IKEv1

Configuration > Site-to-Site VPN (VPN de site à site) > Advanced (Avancé) > IKE Policies (Politiques IKE) > Add/Edit IKE Policy (Ajouter/modifier une politique IKE)

Priority # (Priorité #) : saisissez un nombre pour définir une priorité pour la politique IKE. La plage est comprise entre 1 et 65 535, 1 étant la priorité la plus élevée.

Encryption (Chiffrement) : choisissez une méthode de chiffrement. Il s'agit d'une méthode de chiffrement symétrique qui protège les données transmises entre deux homologues IPsec. Les choix sont les suivants :

DES	DES-CBC 56 bits Moins sécurisée, mais plus rapide que les autres solutions. Il s'agit du paramètre par défaut.
3DES	Triple DES 168 bits
aes	AES-128 bits.
aes-192	AES-192 bits.
aes-256	AES 256 bits.

Hachage : choisissez l'algorithme de hachage qui garantit l'intégrité des données. Il garantit qu'un paquet provient de celui dont vous pensez qu'il provient et qu'il n'a pas été modifié en cours de transit.

sha	SHA-1	La valeur par défaut est SHA-1. MD5 a un condensé plus petit et est considéré comme légèrement plus rapide que SHA-1. Une attaque réussie (mais très difficile) contre MD5 s'est produite ; cependant, la variante de HMAC utilisée par IKE empêche cette attaque.
md5	MD5	

Authentification : choisissez la méthode d'authentification utilisée par l'ASA pour établir l'identité de chaque homologue IPsec. Les clés prépartagées n'évoluent pas facilement avec un réseau en croissance, mais sont plus faciles à configurer dans un petit réseau. Les choix sont les suivants :

pre-share	Clés prépartagées.
rsa-sig	Un certificat numérique avec des clés générées par l'algorithme de signatures RSA

Groupe Diffie-Hellman : choisissez le groupe Diffie-Hellman que les deux homologues IPsec utilisent pour obtenir un secret partagé sans le transmettre l'un à l'autre.

1	Groupe 1 (768 bits)	, le groupe 2 (Diffie-Hellman 1 024 bits), nécessite moins de temps CPU pour s'exécuter, mais est moins sécurisé que le groupe 1 ou 5.
2	Groupe 2 (1 024 bits)	
5	Groupe 5 (1 536 bits)	
14	Groupe 14 (2 048 bits)	Le groupe Diffie-Hellman par défaut est le groupe 14 (Diffie-Hellman 2 048 bits)

Durée de vie (s) : cochez la case Illimité ou saisissez un entier pour la durée de vie de la SA. La valeur par défaut est 86 400 secondes (24 heures). Avec des durées de vie plus longues, l'ASA configure les futures associations de sécurité IPsec moins rapidement. La force de chiffrement est suffisamment élevée pour assurer

la sécurité sans utiliser des temps de renouvellement très rapides, de l'ordre de quelques minutes. Nous vous recommandons de conserver la valeur par défaut.

Mesure de temps : choisissez une mesure de temps. L'ASA accepte les valeurs suivantes :

120 secondes
2 à 1 440 minutes
1 à 24 heures
1 jour

Créer ou modifier une politique IKEv2

Configuration > Site-to-Site VPN > Advanced > IKE Policies > Add/Edit IKEv2 Policy (Configuration > VPN de site à site > Avancé > Politiques IKE > Ajouter/Modifier une politique IKEv2)

Priority # (Priorité #) : saisissez un nombre pour définir une priorité pour la politique IKEv2. La plage est comprise entre 1 et 65 535, 1 étant la priorité la plus élevée.

Encryption (Chiffrement) : choisissez une méthode de chiffrement. Il s'agit d'une méthode de chiffrement symétrique qui protège les données transmises entre deux homologues IPsec. Les choix sont les suivants :

DES	Spécifie le chiffrement DES-CBC 56 bits pour ESP.
3DES	(Par défaut) Spécifie l'algorithme de chiffrement triple DES pour ESP.
aes	Spécifie AES avec un chiffrement de clé de 128 bits pour ESP.
aes-192	Spécifie AES avec un chiffrement de clé de 192 bits pour ESP.
aes-256	Spécifie AES avec un chiffrement de clé de 256 bits pour ESP.
aes-gcm	Spécifie la prise en charge d'AES-GCM/GMAC 128 bits pour le chiffrement symétrique et l'intégrité.
aes-gcm-192	Spécifie la prise en charge d'AES-GCM/GMAC 192 bits pour le chiffrement symétrique et l'intégrité.
aes-gcm-256	Spécifie la prise en charge d'AES-GCM/GMAC 256 bits pour le chiffrement symétrique et l'intégrité.
NUL	Indique aucun chiffrement.

Groupe Diffie-Hellman : choisissez le groupe Diffie-Hellman que les deux homologues IPsec utilisent pour obtenir un secret partagé sans le transmettre l'un à l'autre.

1	Groupe 1 (768 bits)	La valeur par défaut, le groupe 2 (Diffie-Hellman 1 024 bits), nécessite moins de temps CPU pour s'exécuter, mais est moins sécurisé que le groupe 2 ou 5.
2	Groupe 2 (1 024 bits)	
5	Groupe 5 (1 536 bits)	

14	Groupe 14	
19	Groupe 19	
20	Groupe 20	
21	Groupe 21	
24	Groupe 24	

Integrity Hash (Hachage d'intégrité) : choisissez l'algorithme de hachage qui garantit l'intégrité des données pour le protocole ESP. Il garantit qu'un paquet provient de celui dont vous pensez qu'il provient et qu'il n'a pas été modifié en cours de transit.

sha	SHA-1	La valeur par défaut est SHA 1. MD5 a un condensé plus petit et est considéré comme légèrement plus rapide que SHA-1. Une attaque réussie (mais très difficile) contre MD5 s'est produite ; cependant, la variante de HMAC utilisée par IKE empêche cette attaque.
md5	MD5	
sha256	SHA 2, condensé de 256 bits	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 256 bits.
sha384	**SHA 2, 384-bit digest**	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 384 bits.
sha512	**SHA 2, 512-bit digest**	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 512 bits.
null (nul)		Indique qu'AES-GCM ou AES-GMAC est configuré comme algorithme de chiffrement. Vous devez choisir l'algorithme d'intégrité nulle si AES-GCM a été configuré comme algorithme de chiffrement.

Fonction pseudo-aléatoire (PRF) : précisez la PRF utilisée pour la construction du matériel de saisie pour tous les algorithmes cryptographiques utilisés dans le SA.

sha	SHA-1	La valeur par défaut est SHA-1. MD5 a un condensé plus petit et est considéré comme légèrement plus rapide que SHA-1. Une attaque réussie (mais très difficile) contre MD5 s'est produite ; cependant, la variante de HMAC utilisée par IKE empêche cette attaque.
md5	MD5	
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.

Durée de vie (s) : cochez la case Illimité ou saisissez un entier pour la durée de vie de la SA. La valeur par défaut est 86 400 secondes (24 heures). Avec des durées de vie plus longues, l'ASA configure plus rapidement les futures associations de sécurité IPsec. La force de chiffrement est suffisamment élevée pour assurer la sécurité sans utiliser des temps de renouvellement très rapides, de l'ordre de quelques minutes. Nous vous recommandons de conserver la valeur par défaut.

L'ASA accepte les valeurs suivantes :

120 secondes
2 - 1 440 minutes
1 à 24 heures
1 jour

Configurer 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. L'ASA prend en charge les connexions IPsec de réseau local (LAN) à réseau local (LAN) avec les homologues Cisco (IPv4 ou IPv6) et avec les homologues tiers qui sont conformes à toutes les normes pertinentes.

Lors de l'établissement du tunnel, les deux homologues négocient des associations de sécurité 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.

L'ASA prend en charge ces attributs IPsec :

- Mode principal pour la négociation des associations de sécurité ISAKMP de phase 1 lors de l'utilisation de certificats numériques pour l'authentification
- Mode agressif pour négocier les associations de sécurité ISAKMP (SA) de phase 1 lors de l'utilisation de clés prépartagées pour l'authentification
- Algorithmes d'authentification :
  - ESP-MD5-HMAC-128
  - ESP-SHA1-HMAC-160
- Modes d'authentification
  - Clés prépartagées
  - Certificats numériques X.509
- Algorithmes de chiffrement :
  - AES-128, -192, et -256
  - 3DES-168
  - DES-56

- ESP-NULL

- Authentification étendue (XAuth)
- Configuration en mode (également connue sous le nom de méthode de configuration ISAKMP)
- Mode d'encapsulation de tunnel
- Compression d'IP (IPCOMP) à l'aide de LZS

Procédure

Étape 1 Configurer les Carte de chiffrement, à la page 28.

Étape 2 Configurer les Politiques de pré-fragmentation IPsec, à la page 37.

Étape 3 Configurer les Propositions IPsec (ensembles de transformations), à la page 39.

Carte de chiffrement

Configuration > Site-to-Site VPN (VPN de site à site) > Advanced (Avancé) > Crypto Maps (Cartes de chiffrement)

Ce volet affiche les cartes de chiffrement actuellement configurées, qui sont définies dans les règles IPsec. Ici, vous pouvez ajouter, modifier, supprimer et déplacer vers le haut, déplacer vers le bas, couper, copier et coller une règle IPsec.

Remarque Vous ne pouvez pas modifier, supprimer ou copier une règle implicite. L'ASA accepte implicitement la proposition de sélection du trafic des clients distants lorsqu'elle est configurée avec une politique de tunnel dynamique. Vous pouvez le remplacer en accordant une sélection de trafic spécifique.

Vous pouvez également **rechercher** (filtrer l'affichage des règles) en sélectionnant Interface, Source, Destination, Destination Service (Service de destination) ou Rule Query (Requête de règles), en sélectionnant is (est) ou contains (contient), puis en saisissant le paramètre de filtre. Cliquez sur... pour lancer une boîte de dialogue de navigation qui affiche toutes les entrées existantes que vous pouvez choisir. Utilisez **Diagram** (Diagramme) pour afficher les règles sous forme graphique.

Les règles IPsec spécifient les éléments suivants :

- Type : priorité : affiche le type de règle (statique ou dynamique) et sa priorité.
- Sélection de trafic
  - # : indique le numéro de la règle.
  - Source : indique les adresses IP qui sont soumises à cette règle lorsque le trafic est envoyé vers les adresses IP répertoriées dans la colonne Remote Côté Host/Network (Hôte/Réseau du côté distant). En mode détail (voir le bouton Show Detail (Afficher les détails)), une colonne d'adresses peut contenir un nom d'interface avec le mot any, tel que inside:any. any signifie que tout hôte sur l'interface interne est affecté par la règle.

- Destination : répertorie les adresses IP qui sont soumises à cette règle lorsque le trafic est envoyé à partir des adresses IP répertoriées dans la colonne Hôte/Réseau du côté de l'appareil de sécurité. En mode détail (voir le bouton Show Detail (Afficher les détails)), une colonne d'adresses peut contenir un nom d'interface avec le mot any, tel que outside:any. any signifie que tout hôte sur l'interface externe est affecté par la règle. Également en mode détail, une colonne d'adresses peut contenir des adresses IP entre crochets. Par exemple, [209.165.201.1-209.165.201.30]. Ces adresses sont des adresses traduites. Lorsqu'un hôte interne établit une connexion avec un hôte externe, l'ASA associe l'adresse de l'hôte interne à une adresse de l'ensemble. Après qu'un hôte ait créé une connexion sortante, l'ASA conserve ce mappage d'adresse. Cette structure de mappage d'adresses s'appelle un xlate et reste en mémoire pendant un certain temps.
- Service : spécifie le service et le protocole spécifiés par la règle (TCP, UDP, ICMP ou IP).
- Action : spécifie le type de règle IPsec (protéger ou ne pas protéger).

- Transform Set (Ensemble de transformation) : affiche l'ensemble de transformation pour la règle.
- Peer (Homologue) : identifie l'homologue IPsec.
- PFS : affiche les paramètres de confidentialité de transmission parfaite pour la règle.
- NAT-T Enabled (NAT-T activé) : indique si la traversée NAT est activée pour la politique.
- Reverse Route Enabled (Route inversée activée) : indique si l'injection de route inverse (RRI) est activée pour la politique. 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 soit 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.
  - Dynamic (Dynamique) : si la dynamique est spécifiée, les RRI sont créés lors de l'établissement réussi des associations de sécurité IPsec et supprimés après la suppression des SA IPsec.

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

- Connection Type (Type de connexion) : (significatif uniquement pour les politiques de tunnel statique.) Identifie le type de connexion pour cette politique comme bidirectionnel, d'origine uniquement ou de réponse uniquement).
- SA Lifetime (Durée de vie SA) : affiche la durée de vie SA pour la règle.
- CA Certificate (Certificat de l'autorité de certification) : affiche le certificat de l'autorité de certification de la politique. Cela s'applique uniquement aux connexions statiques.
- IKE Negotiation Mode (Mode de négociation IKE) : affiche si les négociations IKE utilisent le mode principal ou le mode agressif.
- Description : (facultatif) spécifie une brève description de cette règle. Pour une règle existante, il s'agit de la description que vous avez saisie lors de l'ajout de la règle. Une règle implicite comprend la description suivante : « Règle implicite ». Pour modifier la description de n'importe quelle règle, sauf d'une règle implicite, cliquez avec le bouton droit sur cette colonne et choisissez Edit Description (Modifier la description) ou double-cliquez sur la colonne.

- Enable Anti-replay window size (Activer la taille de la fenêtre anti-relecture) : définit la taille de la fenêtre anti-relecture entre 64 et 1 028 par incréments de 64. Un effet secondaire de la mise en file prioritaire dans une politique QoS hiérarchique avec régulation du trafic (voir « Actions de règles> Onglet QoS ») est le réordonnancement des paquets. Pour les paquets IPsec, les paquets en panne qui ne sont pas dans la fenêtre d'anti-relecture génèrent des messages d'avertissement syslog. Ces avertissements deviennent de fausses alarmes dans le cas de la mise en file d'attente prioritaire. La configuration de la taille du volet anti-relecture vous aide à éviter d'éventuelles fausses alarmes.
- Enable IPsec Inner Routing Lookup (Activer la recherche de routage interne IPsec) : par défaut, les recherches ne sont pas effectuées pour les paquets envoyés via le tunnel IPsec; les recherches d'adjacence par paquet sont effectuées uniquement pour les paquets ESP externes. 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 opérationnel, les paquets traversant 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.

Créer ou modifier une politique de tunnel de règle IPsec (carte de chiffrement) - Onglet Basic (Base)

Utilisez ce pour définir une nouvelle politique de tunnel pour une règle IPsec. Les valeurs que vous définissez ici s'affichent dans le tableau des règles IPsec après que vous avez cliqué sur **OK**. Toutes les règles sont activées par défaut dès qu'elles apparaissent dans le tableau des règles IPsec.

Le volet Tunnel Policy (Politique de tunnel) vous permet de définir une politique de tunnel utilisée pour négocier une association de sécurité (SA) IPsec (phase 2). ASDM enregistre vos modifications de configuration, mais ne les enregistre pas dans la configuration en cours tant que vous n'avez pas cliqué sur **Apply** (Appliquer).

Chaque politique de tunnel doit spécifier un ensemble de transformations et identifier l'interface de l'appareil de sécurité à laquelle elle s'applique. L'ensemble de transformation identifie les algorithmes de chiffrement et de hachage qui effectuent les opérations de chiffrement et de déchiffrement IPsec. Comme tous les homologues IPsec ne prennent pas en charge les mêmes algorithmes, vous pouvez spécifier un certain nombre de politiques et affecter une priorité à chacune. L'appareil de sécurité négocie ensuite avec l'homologue IPsec distant pour convenir d'un ensemble de transformations pris en charge par les deux homologues.

Les politiques de tunnel peuvent être *statiques* ou *dynamiques*. Une politique de tunnel statique identifie un ou plusieurs homologues IPsec distants ou sous-réseaux auxquels votre appareil de sécurité autorise les connexions IPsec. Une politique statique peut être utilisée si votre appareil de sécurité amorce la connexion ou reçoit une demande de connexion d'un hôte distant. Une politique statique vous oblige à saisir les informations nécessaires pour identifier les hôtes ou les réseaux autorisés.

Une politique de tunnel dynamique est utilisée lorsque vous ne pouvez pas ou ne souhaitez pas fournir d'informations sur les hôtes distants qui sont autorisés à établir une connexion avec l'appareil de sécurité. Si vous utilisez uniquement votre appareil de sécurité comme client VPN par rapport à un périphérique de site central VPN distant, vous n'avez pas besoin de configurer de politiques de tunnel dynamique. Les politiques de tunnel dynamique sont plus utiles pour permettre aux clients d'accès à distance d'établir une connexion à votre réseau par l'intermédiaire d'un appareil de sécurité agissant en tant qu'appareil de site central VPN. Une politique de tunnel dynamique est utile lorsque les clients d'accès à distance ont des adresses IP affectées dynamiquement ou lorsque vous ne souhaitez pas configurer des politiques distinctes pour un grand nombre de clients d'accès à distance.

Configuration > Site-to-Site VPN (VPN de site à site) > Advanced (Avancé) > Crypto Maps (Cartes de chiffrement) > Create / Edit IPsec Rule (Créer / Modifier une règle IPsec) > Tunnel Policy (Crypto Map) - Basic (Politique de tunnel (carte de chiffrement) - Base)

- Interface : choisissez le nom de l'interface à laquelle cette politique s'applique.
- Policy Type (Type de politique) : choisissez le type, statique ou dynamique, de cette politique de tunnel.
- Priority (Priorité) : saisissez la priorité de la politique.
- IKE Proposals (Transform Sets) (Propositions IKE (Ensembles de transformation)) : spécifie les propositions IPsec IKEv1 et IKEv2.
  - IKEv1 IPsec Proposal (Proposition IPsec IKEv1) : choisissez la proposition (ensemble de transformation) pour la politique et cliquez sur **Add** (Ajouter) pour la déplacer dans la liste des ensembles de transformation actifs. Cliquez sur **Move Up** (Déplacer vers le haut) ou **Move Down** (Déplacer vers le bas) pour réorganiser l'ordre des propositions dans la zone de liste. Vous pouvez ajouter un maximum de 11 propositions à une entrée de carte de chiffrement ou à une entrée de carte de chiffrement dynamique.
  - IKEv2 IPsec Proposal (Proposition IPsec IKEv2) : choisissez la proposition (ensemble de transformation) pour la politique et cliquez sur **Add** (Ajouter) pour la déplacer dans la liste des ensembles de transformation actifs. Cliquez sur **Move Up** (Déplacer vers le haut) ou **Move Down** (Déplacer vers le bas) pour réorganiser l'ordre des propositions dans la zone de liste. Vous pouvez ajouter un maximum de 11 propositions à une entrée de carte de chiffrement ou à une entrée de carte de chiffrement dynamique.
- Peer Settings - Optional for Dynamic Crypto Map Entries (Paramètres homologues - Facultatif pour les entrées de carte de chiffrement dynamique) : configurez les paramètres homologues pour la politique.
  - Connection Type (Type de connexion) : (significatif uniquement pour les politiques de tunnel statique.) Choisissez bidirectionnel, origine uniquement ou réponse uniquement pour préciser le type de connexion de cette politique. Pour les connexions de réseau local (LAN à réseau local), choisissez bidirectionnel ou réponse uniquement (pas de source uniquement). Choisissez la réponse uniquement pour la redondance LAN-LAN. Originate Only (Générer uniquement), vous pouvez spécifier jusqu'à 10 homologues redondants. Pour unidirectionnel, vous pouvez spécifier l'origine uniquement ou la réponse uniquement, et aucun n'est activé par défaut.
  - IP Address of Peer to Be Added (Adresse IP de l'homologue à ajouter) : saisissez l'adresse IP de l'homologue IPsec que vous ajoutez. À partir de la version 9.14(1), l'ASA prend en charge plusieurs homologues dans IKEv2. Vous pouvez ajouter un maximum de 10 homologues à la carte de chiffrement.
- Enable Perfect Forwarding Secrecy (activer la confidentialité de transmission parfaite) : cochez cette option pour activer la confidentialité de transmission parfaite pour la politique. PFS est un concept cryptographique dans lequel chaque nouvelle clé n'est liée à aucune clé précédente. Dans les négociations IPsec, les clés de phase 2 sont basées sur les clés de phase 1, sauf si vous spécifiez la confidentialité de transmission parfaite.
- Diffie-Hellman Group (Groupe Diffie-Hellman) : lorsque vous activez PFS, vous devez également choisir un groupe Diffie-Hellman que l'ASA utilise pour générer des clés de session. Voici les différents choix proposés :
  - Groupe 1 (768 bits) = utilise la confidentialité de transmission parfaite et utilise le groupe Diffie-Hellman 1 pour générer des clés de session IPsec, où les numéros premiers et de génération sont de 768 bits. Cette option est plus sécurisée, mais nécessite plus de surdébit de traitement.
  - Groupe 2 (1 024 bits) = utilise la confidentialité de transmission parfaite et utilise le groupe Diffie-Hellman 2 pour générer des clés de session IPsec, où les numéros premiers et de génération

sont de 1 024 bits. Cette option est plus sécurisée que le groupe 1, mais nécessite un surdébit de traitement plus important.

- Groupe 5 (1 536 bits) : utilisez la confidentialité de transmission parfaite et utilisez le groupe Diffie-Hellman 5 pour générer des clés de session IPsec, où les numéros du premiers et du générateur sont de 1 536 bits. Cette option est plus sécurisée que le groupe 2, mais nécessite un surdébit de traitement plus important.
- Groupe 14 (2 048 bits) : utilisez la confidentialité de transmission parfaite et utilisez le groupe Diffie-Hellman 14 pour IKEv2.
- Groupe 19 : utilisez la confidentialité de transmission parfaite et utilisez le groupe Diffie-Hellman 19 pour IKEv2 afin de prendre en charge ECDH.
- Groupe 20 : utilisez la confidentialité de transmission parfaite et utilisez le groupe Diffie-Hellman 20 pour IKEv2 afin de prendre en charge ECDH.
- Groupe 21 : utilisez la confidentialité de transmission parfaite et utilisez le groupe Diffie-Hellman 21 pour IKEv2 afin de prendre en charge ECDH.
- Groupe 24 : utilisez la confidentialité de transmission parfaite et utilisez le groupe Diffie-Hellman 24 pour IKEv2.

Créer ou modifier une politique de tunnel de règle IPsec (carte de chiffrement) - Onglet Avancé

Configuration > Site-to-Site VPN > Advanced > Crypto Maps > Create / Edit IPsec Rule > Tunnel Policy (Crypto Map) - Advanced (Configuration > VPN de site à site > Avancé > Cartes de chiffrement > Créer / Modifier une règle IPsec > Stratégie de tunnel [carte de chiffrement] - Avancé)

- Enable NAT-T (Activer NAT-T) : active la traversée NAT (NAT-T) pour cette stratégie.
- Enable Reverse Route Injection (Activer l'injection de route inverse) : active l'injection de route inverse pour cette stratégie. L'injection de route inverse (RRI) est utilisée pour remplir la table de routage d'un routeur interne qui exécute des protocoles de routage dynamique tels que l'Open Shortest Path First (OSPF), le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) si vous utilisez ASA, ou le protocole d'information de routage (RIP) pour les clients VPN distants ou les sessions de réseau local (LAN) à LAN. 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 soit 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.
  - Dynamique : si dynamic est spécifié, les RRI sont créées lors de l'établissement réussi des associations de sécurité IPsec et supprimées après la suppression des SA IPsec. En règle générale, les routes RRI sont utilisées pour amorcer un tunnel s'il n'y en a pas et que le trafic doit être chiffré. Avec la prise en charge dynamique des RRI, aucune route n'est présente avant l'activation du tunnel. Par conséquent, un ASA avec une RRI dynamique configuré fonctionnerait généralement uniquement comme répondeur.

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

- Security Association Lifetime Settings (Paramètres de durée de vie de l'association de sécurité) : configure la durée d'une association de sécurité (SA). Ce paramètre spécifie comment mesurer la durée de vie des clés de SA IPsec, qui correspond à la durée de vie de la SA IPsec jusqu'à son expiration et doit être renégociée avec de nouvelles clés.
  - Time (Temps) : spécifie la durée de vie de la SA en heures (hh), minutes (mm) et en secondes (ss).
  - Traffic Volume (Volume du trafic) : définit la durée de vie de la SA en termes de kilo-octets de trafic. Saisissez le nombre de kilo-octets de données de charge utile après lequel la SA IPsec expire. Le minimum est de 100 Ko, la valeur par défaut est de 10 000 Ko, et le maximum est de 2 147 483 647 Ko.
- Static Type Only Settings (Paramètres de type statique uniquement) : spécifie les paramètres pour les politiques de tunnel statique.
  - Device Certificate (Certificat d'appareil) : choisissez le certificat à utiliser. Si vous choisissez autre chose que None (Use Preshared Keys) [None (Utiliser des clés prépartagées)], qui est la valeur par défaut. La case Send CA certificate chain (Envoyer la chaîne de certificats de l'autorité de certification) devient active lorsque vous choisissez autre chose que None.
  - Send CA certificate chain (Envoyer la chaîne de certificats de l'autorité de certification) : active la transmission de l'ensemble de la chaîne de points de confiance.
  - IKE Negotiation Mode (Mode de négociation IKE) : choisit le mode de négociation IKE, Main (Principal) ou Aggressive (Progressif). Ce paramètre définit le mode d'échange des informations de clé et de configuration des SA. Il définit le mode utilisé par l'initiateur de la négociation; le répondeur négocie automatiquement. Le mode agressif est plus rapide, utilise moins de paquets et moins d'échanges, mais il ne protège pas l'identité des parties qui communiquent. Le mode principal est plus lent, utilisant plus de paquets et plus d'échanges, mais il protège les identités des parties qui communiquent. Ce mode est plus sécurisé et il s'agit de la sélection par défaut. Si vous choisissez Aggressive (Mode agressif), la liste Diffie-Hellman Group (Groupe Diffie-Hellman) devient active.
  - Diffie-Hellman Group (Groupe Diffie-Hellman) : choisissez le groupe Diffie-Hellman à appliquer. Les choix sont les suivants : Groupe 1 (768 bits), Groupe 2 (1 024 bits) ou Groupe 5 (1 536 bits).
- ESP v3 : spécifiez si les messages d'erreur ICMP entrants sont validés pour les cartes de chiffrement statiques et dynamiques, définissez la stratégie par association de sécurité ou activez les paquets de flux de trafic :
  - Validate incoming ICMP error messages (Valider les messages d'erreur ICMP entrants) : choisissez s'il faut valider les messages d'erreur ICMP reçus dans un tunnel IPsec et destinés à un hôte intérieur sur le réseau privé.
  - Enable Do Not Fragment (DF) policy (Activer la stratégie Ne pas fragmenter [DF]) : définit comment le sous-système IPsec gère les paquets volumineux dont le bit « Ne pas fragmenter » (DF) est défini dans l'en-tête IP. Effectuez l'une des opérations suivantes :

    Clear DF bit (Effacer le bit DF) : ignore le bit DF.

    Copy DF bit (Copier le bit DF) : maintient le bit DF.

    Set DF bit (Définir le bit DF) : définit et utilise le bit DF.
  - Sélectionnez Enable Traffic Flow Confidentiality (TFC) packets (Activer les paquets TFC de confidentialité du flux de trafic) pour activer des paquets TFC factices qui masquent le profil de trafic qui traverse le tunnel.

Remarque Vous devez avoir une proposition IKEv2 IPsec définie dans l'onglet Tunnel Policy (Crypto Map) Basic (Base de la stratégie de tunnel [carte de chiffrement]) avant d'activer TFC.

Utilisez les paramètres Burst (Rafale), Payload Size (Taille de la charge utile) et Timeout (Expiration) pour générer des paquets de longueur aléatoire à des intervalles aléatoires sur la SA specifiée.

Créer ou modifier l'onglet Sélection du trafic de règle IPsec

Configuration > Site-to-Site VPN (VPN de site à site) > Advanced (Avancé) > Crypto Maps (Cartes de chiffrement) > Create / Edit IPsec Rule (Créer/modifier une règle IPsec) > Traffic Selection (Sélection du trafic)

Ce volet vous permet de définir le trafic à protéger (autoriser) ou à ne pas protéger (refuser).

- Action : précisez l'action que cette règle doit exécuter. Les sélections sont protect (protéger) et do not protect (ne pas protéger).
- Source : spécifiez l'adresse IP, le groupe d'objets réseau ou l'adresse IP de l'interface de l'hôte ou du réseau source. Une règle ne peut pas utiliser la même adresse comme source et destination. Cliquez sur ... pour lancer la boîte de dialogue Browse Source (Parcourir la source), qui contient les champs suivants :
  - Add/Edit (Ajouter/Modifier) : choisissez IP Address (Adresse IP) ou Network Object Group (Groupe d'objets réseau) pour ajouter d'autres adresses ou groupes source.
  - Delete (Supprimer) : cliquez pour supprimer une entrée.
  - Filter (Filtre) : saisissez une adresse IP pour filtrer les résultats affichés.
  - Name (Nom) : indique que les paramètres suivants précisent le nom de l'hôte ou du réseau source.
  - IP Address (Adresse IP) : indique que les paramètres suivants précisent l'interface, l'adresse IP et le masque de sous-réseau de l'hôte ou du réseau source.
  - Netmask (Masque réseau) : choisit un masque de sous-réseau standard à appliquer à l'adresse IP. Ce paramètre s'affiche lorsque vous choisissez le bouton d'option IP Address (Adresse IP).
  - Description : saisissez une description.
  - Selected Source (Source sélectionnée) : cliquez sur **Source** pour inclure l'entrée sélectionnée comme source.
- Destination : spécifiez l'adresse IP, le groupe d'objets réseau ou l'adresse IP de l'interface de l'hôte ou du réseau de destination. Une règle ne peut pas utiliser la même adresse comme source et comme destination. Cliquez ... pour lancer la boîte de dialogue Browse Destination (Parcourir la destination), qui contient les champs suivants :
  - Add/Edit (Ajouter/Modifier) : choisissez IP Address (Adresse IP) ou Network Object Group (Groupe d'objets réseau) pour ajouter d'autres adresses ou groupes de destination.
  - Delete (Supprimer) : cliquez pour supprimer une entrée.
  - Filter (Filtre) : saisissez une adresse IP pour filtrer les résultats affichés.

- Name (Nom) : indique que les paramètres suivants précisent le nom de l'hôte ou du réseau de destination.
- IP Address (Adresse IP) : indique que les paramètres suivants précisent l'interface, l'adresse IP et le masque de sous-réseau de l'hôte ou du réseau de destination.
- Netmask (Masque réseau) : choisit un masque de sous-réseau standard à appliquer à l'adresse IP. Ce paramètre s'affiche lorsque vous choisissez le bouton d'option IP Address (Adresse IP).
- Description : saisissez une description.
- Selected Destination (Destination sélectionnée) : cliquez sur **Destination** pour inclure l'entrée sélectionnée comme destination.

- Service : saisissez un service ou cliquez sur ... pour lancer la boîte de dialogue de navigation des services, où vous pouvez choisir dans une liste de services.
- Description : saisissez une description pour l'entrée de sélection du trafic.
- Plus d'options
  - nable Rule (Activer la règle) — Cliquez pour activer cette règle.
  - Source Service (Service source) : saisissez un service ou cliquez sur **...** pour lancer la boîte de dialogue de navigation des services, où vous pouvez choisir dans une liste de services.
  - Time Range (Plage temporelle) : définissez une plage temporelle pour laquelle cette règle s'applique.
  - Group (Groupe) : indique que les paramètres suivants précisent l'interface et le nom de groupe de l'hôte ou du réseau source.
  - Interface : choisissez le nom d'interface pour l'adresse IP. Ce paramètre s'affiche lorsque vous choisissez le bouton d'option IP Address (Adresse IP).
  - IP address (Adresse IP) : spécifie l'adresse IP de l'interface à laquelle cette politique s'applique. Ce paramètre s'affiche lorsque vous choisissez le bouton d'option IP Address (adresse IP).
  - Destination : spécifiez l'adresse IP, le groupe d'objets réseau ou l'adresse IP de l'interface de l'hôte ou du réseau source ou de destination. Une règle ne peut pas utiliser la même adresse comme source et comme destination. Cliquez sur **...** pour l'un de ces champs afin de lancer la boîte de dialogue Browse (Parcourir), qui contient les champs suivants :
  - Name (nom) : choisissez le nom de l'interface à utiliser comme hôte ou réseau source ou de destination. Ce paramètre s'affiche lorsque vous choisissez le bouton d'option Name (Nom). Il s'agit du seul paramètre associé à cette option.
  - Interface : choisissez le nom d'interface pour l'adresse IP. Ce paramètre s'affiche lorsque vous cliquez sur le bouton d'option Group (Groupe).
  - Group (groupe) : choisissez le nom du groupe sur l'interface spécifiée pour l'hôte ou le réseau source ou de destination. Si la liste ne contient aucune entrée, vous pouvez saisir le nom d'un groupe existant. Ce paramètre s'affiche lorsque vous cliquez sur le bouton d'option Group (Groupe).

- **Protocol and Service** (Protocole et service) : spécifie les paramètres de protocole et de service pertinents pour cette règle.

Remarque Les règles IPsec « any-any » ne sont pas autorisées. Ce type de règle empêcherait le périphérique et son homologue de prendre en charge plusieurs tunnels de réseau local à réseau local.

- TCP : spécifie que cette règle s'applique aux connexions TCP. Cette sélection affiche également les zones de groupe Port source et Port de destination.
- UDP : spécifie que cette règle s'applique aux connexions UDP. Cette sélection affiche également les zones de groupe Port source et Port de destination.
- ICMP : spécifie que cette règle s'applique aux connexions ICMP. Cette sélection affiche également la zone de groupe Type ICMP.
- IP : spécifie que cette règle s'applique aux connexions IP. Cette sélection affiche également la zone de groupe IP Protocol (Protocole IP).
- Manage Service Groups (Gérer les groupes de services) : affiche le volet Manage Service Groups (Gérer les groupes de services), dans lequel vous pouvez ajouter, modifier ou supprimer un groupe de services/ports TCP/UDP.
- Source Port and Destination Port (Port source et Port de destination) : contiennent les paramètres de port TCP ou UDP, selon le bouton d'option que vous avez choisi dans la zone de groupe Protocol and Service (Protocole et service).
- Service : indique que vous spécifiez les paramètres d'un service individuel. Spécifie le nom du service et un opérateur booléen à utiliser lors de l'application du filtre.
- Boolean operator (unlabeled) (Opérateur booléen [sans étiquette]) : répertorie les conditions booléennes (equal [égal], not equal [différent], greater than [supérieur à], less than [inférieur à] ou range [plage]) à utiliser pour faire correspondre le service précisé dans la zone de service.
- Service (unlabeled) (Service [sans étiquette]) : identifie le service (comme https, ldaps ou any) à mettre en correspondance. Si vous avez spécifié l'opérateur de service de plage, ce paramètre devient deux zones, dans lesquelles vous saisissez le début et la fin de la plage.
- … : affiche une liste de services dans laquelle vous pouvez choisir le service à afficher dans la zone Service.
- Service Group (Groupe de services) : indique que vous précisez le nom d'un groupe de services pour le port source.
- Service (unlabeled) (Service [sans étiquette]) : choisissez le groupe de services à utiliser.
- ICMP Type (Type ICMP) : spécifie le type ICMP à utiliser. La valeur par défaut est any. Cliquez sur le bouton **...** pour afficher une liste des types disponibles.

• Options

- Time Range (Plage temporelle) : spécifiez le nom d'une plage temporelle existante ou créez une nouvelle plage.
- … : affiche le volet Add Time Range (Ajouter une plage temporelle), dans lequel vous pouvez définir une nouvelle plage temporelle.

- Please enter the description below (optional) (Veuillez saisir la description ci-dessous [facultatif]) : fournit un espace pour saisir une brève description de la règle.

Politiques de pré-fragmentation IPsec

Configuration > Site-to-Site VPN (VPN de site à site) > Advanced (Avancé) > IPsec Prefragmentation Policies (Politiques de préfragmentation IPsec)

La politique de préfragmentation IPsec spécifie comment traiter les paquets qui dépassent le paramètre d'unité de transmission maximale (MTU) lors de la tunnellisation du trafic via l'interface publique. Cette fonctionnalité permet de gérer les cas où un routeur ou un périphérique NAT entre l'ASA et le client rejette ou abandonne des fragments d'adresses IP. Par exemple, supposons qu'un client souhaite effectuer un FTP get à partir d'un serveur FTP derrière un ASA. Le serveur FTP transmet des paquets qui, encapsulés, dépasseraient la taille MTU de l'ASA sur l'interface publique. Les options sélectionnées déterminent la façon dont l'ASA traite ces paquets. La politique de préfragmentation s'applique à tout le trafic sortant de l'interface publique de l'ASA.

L'ASA encapsule tous les paquets tunnelisés. Après l'encapsulation, l'ASA fragmente les paquets qui dépassent le paramètre MTU avant de les transmettre par l'intermédiaire de l'interface publique. Il s'agit de la politique par défaut. Cette option fonctionne dans les situations où les paquets fragmentés sont autorisés à passer par le tunnel sans restriction. Pour l'exemple FTP, les paquets volumineux sont encapsulés puis fragmentés au niveau de la couche IP. Les périphériques intermédiaires peuvent abandonner des fragments ou simplement des fragments hors séquence. Les périphériques d'équilibrage de charge peuvent introduire des fragments hors séquence.

Lorsque vous activez la préfragmentation, l'ASA fragmente les paquets tunnelisés qui dépassent le paramètre MTU avant de les encapsuler. Si le bit DF sur ces paquets est défini, l'ASA efface le bit DF, fragmente les paquets, puis les encapsule. Cette action crée deux paquets IP indépendants non fragmentés quittant l'interface publique et transmet avec succès ces paquets au site homologue en transformant les fragments en paquets complets devant être réassemblés sur le site homologue. Dans notre exemple, l'ASA remplace la MTU et permet la fragmentation en effaçant le bit DF.

Remarque La modification de l'unité de transfert maximale (MTU) ou de l'option de préfragmentation sur une interface supprime toutes les connexions existantes. Par exemple, si 100 tunnels actifs se terminent sur l'interface publique et que vous modifiez la MTU ou l'option de préfragmentation sur l'interface externe, tous les tunnels actifs sur l'interface publique sont abandonnés.

Utilisez ce volet pour afficher ou **Edit** (Modifier) une politique de préfragmentation IPsec existante et une politique du bit Do Not Fragment (DF) pour une interface sélectionnée dans le volet parent.

Champs

- Interface : identifiant de l'interface. Vous ne pouvez pas modifier ce paramètre à l'aide de cette boîte de dialogue.
- Activer la préfragmentation IPsec : active ou désactive la préfragmentation IPsec. L'ASA fragmente les paquets tunnelisés qui dépassent le paramètre MTU avant de les encapsuler. Si le bit DF sur ces paquets est défini, l'ASA efface le bit DF, fragmente les paquets, puis les encapsule. Cette action crée deux paquets IP indépendants non fragmentés quittant l'interface publique et transmet avec succès ces paquets au site homologue en transformant les fragments en paquets complets devant être réassemblés sur le site homologue.

- Politique de paramètre du bit DF : politique du bit Do Not Fragment (DF) : Copy (Copier), Clear (Effacer) ou Set (Définir)

Configurer les options de fragmentation IKEv2

Sur l'ASA, la fragmentation IKEv2 peut être activée ou désactivée, la MTU (unité de transmission maximale) utilisée lors de la fragmentation des paquets IKEv2 peut être spécifiée, et une méthode de fragmentation préférée peut être configurée par l'administrateur sur l'écran suivant :

Configuration > **Site-to-Site VPN (VPN de site à site)** > **Advanced (Avancé)** > **IKE parameters (Paramètres IKE)**

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 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 spécifiée par l'administrateur, l'unité de transfert maximale 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 », veillez 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 :

- 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 Secure Client, 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.

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.

Procédure

Étape 1 Dans ASDM, accédez à **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Advanced (Avancé)** > **IKE parameters (Paramètres IKE)**

Étape 2 Sélectionnez ou désélectionnez le champ **Enable fragmentation** (Activer la fragmentation).

Étape 3 Précisez la taille du champ **Fragmentation MTU** (MTU de fragmentation).

Étape 4 Précisez la **méthode de fragmentation préférée**.

Propositions IPsec (ensembles de transformations)

Configuration Site-to-Site VPN (VPN de site à site) Advanced (Avancé) IPsec Proposals (Transform Sets) (Propositions IPsec [ensembles de transformation]).

Une transformation est un ensemble d'opérations effectuées sur un flux de données pour assurer l'authentification des données, la confidentialité des données et la compression des données. Par exemple, une transformation est le protocole ESP avec chiffrement 3DES et l'algorithme d'authentification HMAC-MD5 (ESP-3DES-MD5).

Utilisez ce volet pour afficher, **Add** (Ajouter), **Edit** (Modifier) ou **Delete** (Supprimer) les ensembles de transformations IKEv1 et IKEv2 décrits ci-dessous. Chaque tableau affiche le nom et les détails des ensembles de transformation configurés.

Ensembles de transformations (propositions IPsec)

- **Mode** : mode d'application du chiffrement et de l'authentification ESP. Cela permet de déterminer quelle partie du paquet IP d'origine a été appliquée à l'ESP.
  - **Mode tunnel** : (par défaut) 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. L'intégralité du datagramme IP d'origine est chiffrée et devient la charge utile dans 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 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 de 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.

- **Chiffrement ESP** : algorithmes de chiffrement Encapsulating Security Protocol (ESP) pour les ensembles de transformations. ESP fournit des services de confidentialité des données, une authentification facultative des données et des services d'anti-relecture. ESP encapsule les données protégées.
- **Authentification ESP** : algorithmes d'authentification ESP pour l'ensemble de transformations.

Propositions IPsec IKEv2

- **Mode** : mode d'application du chiffrement et de l'authentification ESP. Cela permet de déterminer quelle partie du paquet IP d'origine a été appliquée à l'ESP.
  - **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 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.

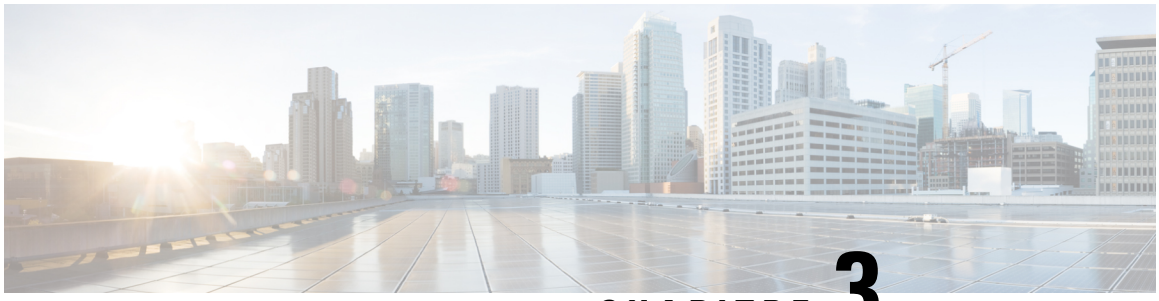
    Ce mode présente l'avantage d'ajouter seulement quelques octets à chaque paquet et de permettre aux périphériques du réseau public de voir la source et la destination finales du paquet. Le mode de transport vous permet d'activer le traitement spécial (par exemple, QoS) sur le réseau intermédiaire en 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.

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.

- **Chiffrement** : affiche l'algorithme de chiffrement Encapsulating Security Protocol (ESP) pour la proposition IPsec IKEv2. ESP fournit des services de confidentialité des données, une authentification facultative des données et des services d'anti-relecture. ESP encapsule les données protégées.
- **Integrity Hash** (Hachage d'intégrité) : affiche l'algorithme de hachage qui garantit l'intégrité des données pour le protocole ESP. Il garantit qu'un paquet provient de l'expéditeur attendu et qu'aucune modification n'a été apportée en transit. Il garantit qu'un paquet provient de l'expéditeur attendu et qu'aucune modification n'a été apportée en transit. Vous devez choisir l'algorithme d'intégrité nulle si AES-GCM/GMAC a été configuré comme algorithme de chiffrement.



CHAPITRE 3

Haute disponibilité

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 ASDM 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 (lbpublic) et privées/internes (lbprivate).

- 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 keepalive, 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 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 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 ayant la même priorité sont trouvées, celle ayant 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 déclaré le directeur comme parti et commence un nouveau cycle d'élection de directeur.

Foire aux questions sur l'équilibrage de 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 Clientou 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'appareil de sécurité adaptable Cisco 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 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 charges VPN nécessite une licence de cryptage renforcé (3DES/AES). 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, à moins que la licence ne le permette.

Conditions préalables à l'équilibrage de la charge VPN

Veuillez consulter également les Directives et limites pour l'équilibrage de charge VPN, à la page 49.

- 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.

  Pour ce faire, accédez à **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > 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, 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.

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, 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, 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 l'équilibrage de charge VPN avec l'Assistant Haute disponibilité et évolutivité :

Procédure

Étape 1 Sélectionnez **Wizards (Assistants)** > **High Availability and Scalability Wizard (Assistant de haute disponibilité et d'évolutivité)**.

Étape 2 Dans l'écran Configuration Type (Type de configuration), cliquez sur **Configure VPN Cluster Load Balancing** (Configurer l'équilibrage de charge de la grappe VPN), puis sur **Next** (Suivant).

Étape 3 Choisissez l'adresse IP unique qui représente l'ensemble du groupe d'équilibrage de charge VPN. Précisez une adresse IP qui se trouve dans la plage d'adresses de sous-réseau public partagée par tous les ASA du groupe.

Étape 4 Précisez 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 VPN.

Étape 5 Pour activer le chiffrement IPsec et vous assurer que toutes les informations d'équilibrage de charge VPN transmises entre les périphériques sont chiffrées, cochez la case **Enable IPsec Encryption** (Activer le chiffrement IPsec).

Étape 6 Précisez et vérifiez le **secret partagé IPsec**. La valeur que vous saisissez s'affiche sous forme d'astérisques consécutifs.

Étape 7 Précisez la priorité attribuée 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, soit en cas de défaillance d'un directeur existant. Plus la priorité est élevée (par exemple, 10), plus grande est la probabilité que ce périphérique devienne le directeur.

Remarque
Si les périphériques du groupe d'équilibrage de charge VPN sont mis sous tension à des moments différents, le premier périphérique mis sous tension adopte le rôle de directeur. Chaque périphérique du groupe vérifie quand il est mis sous tension pour s'assurer que le groupe dispose d'un directeur. S'il n'y en a pas, ce périphérique adopte le rôle. Les périphériques mis sous tension et ajoutés au groupe deviennent ultérieurement des membres du groupe. Si tous les périphériques du groupe sont mis sous tension simultanément, le périphérique dont la priorité est la plus élevée devient le directeur. Si deux périphériques ou plus du groupe sont mis sous tension simultanément et que les deux ont le paramètre de priorité le plus élevé, celui qui a l'adresse IP la plus basse devient le directeur.

Étape 8 Choisissez **Public Interface of This Device** (Interface publique de ce périphérique).

Étape 9 Choisissez **Private Interface of This Device** (Interface privée de ce périphérique).

Étape 10 Cochez la case **Send FQDN to client instead of an IP address when redirecting** (Envoyer le nom de domaine complet au client au lieu d'une adresse IP lors de la redirection) pour que le directeur envoie un nom de domaine complet utilisant l'hôte et le nom de domaine du périphérique au lieu de l'adresse IP externe lors de la redirection des connexions du client VPN vers ce périphérique.

Étape 11 Cliquez sur **Next** (suivant). Passez en revue votre configuration dans l'écran Summary (Résumé).

Étape 12 Cliquez sur **Finish** (Terminer).

La configuration du groupe d'équilibrage de charge VPN est envoyée à l'ASA.

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 , 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.

Les URL de groupe sont configurées dans le volet **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) >** Secure Client **Connection Profiles (Profils**

de connexion) > *connection profile name (nom du profil de connexion)* > **Add or Edit (Ajouter ou modifier) > Advanced (Avancé) > Group Alias / Group URL (Alias de groupe / URL de groupe)**.

Configurer l'équilibrage de charge du VPN (sans l'assistant)

Procédure

Étape 1 Sélectionnez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Load Balancing (Équilibrage de charge).**

Étape 2 Cochez **Participate in Load Balancing** (Participer à l'équilibrage de charge) pour indiquer que cet ASA participe à la grappe d'équilibrage de charge.

Vous devez activer l'équilibrage de charge de cette manière sur chaque ASA qui y participe.

Étape 3 Configurez les champs suivants dans la zone **VPN Cluster Configuration (Configuration de la grappe VPN)**. Ces valeurs doivent être identiques pour l'ensemble de la grappe virtuelle. Tous les serveurs de la grappe doivent avoir une configuration de grappe identique.

- **Adresse IPv4 de la grappe** : spécifie l'adresse IPv4 unique qui représente l'ensemble de la grappe virtuelle IPv4. Choisissez une adresse IP qui se trouve dans la plage d'adresses du sous-réseau public partagée par tous les ASA de la grappe virtuelle.
  - **Port UDP** : spécifie le port UDP de la grappe virtuelle à laquelle cet appareil 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.
- **Cluster IPv6 Address (adresse IP de la grappe)** : spécifie l'adresse IPv6 unique qui représente l'ensemble de la grappe virtuelle IPv6. Choisissez une adresse IP qui se trouve dans la plage d'adresses du sous-réseau public partagée par tous les ASA de la grappe virtuelle. Les clients disposant d'adresses IPv6 peuvent établir des connexions Secure Client au moyen de l'adresse IPv6 publique de la grappe ASA ou d'un serveur GSS. De même, les clients disposant d'adresses IPv6 peuvent établir des connexions VPN Secure Client au moyen de l'adresse IPv4 publique de la grappe ASA ou d'un serveur GSS. L'un ou l'autre type de connexion peut être réparti dans la grappe ASA.

  Remarque
  Dans les champs Cluster IPv4 Address (Adresse IPv4 de la grappe) et Cluster IPv6 Address (Adresse IPv6 de la grappe), vous pouvez également préciser le nom de domaine pleinement qualifié de la grappe virtuelle, à condition qu'un groupe de serveurs DNS soit configuré avec au moins un serveur DNS et que la recherche DNS soit activée sur l'une des interfaces de l'ASA.
- **Enable IPsec Encryption** (Activer le chiffrement IPsec) : active ou désactive le chiffrement IPsec. Si vous cochez cette case, vous devez également préciser et confirmer un secret partagé. Les ASA de la grappe virtuelle communiquent au moyen de tunnels LAN-à-LAN utilisant IPsec. Pour vous assurer que tous les renseignements d'équilibrage de charge échangés entre les périphériques sont chiffrés, cochez cette case.
- **IPsec Shared Secret** (Secret partagéIPsec) : spécifie le secret partagé entre les homologues IPsec lorsque vous avez activé le chiffrement IPsec. La valeur que vous saisissez dans la zone s'affiche sous forme d'astérisque consécutif.
- **Verify Secret**(vérifier le secret) : saisir de nouveau le secret partagé. Confirme la valeur du secret partagé saisie dans la zone IPsec Shared Secret (Secret partagé IPsec).

Étape 4 Configurez les champs de la zone **VPN Server Configuration** (Configuration du serveur VPN) pour un ASA spécifique :

- **Interface publique** : spécifie le nom ou l'adresse IP de l'interface publique pour cet appareil.
- **Interface privée** : spécifie le nom ou l'adresse IP de l'interface privée pour cet appareil.
- **Priorité** : spécifie la priorité affectée à cet appareil dans la grappe. La plage est de 1 à 10. La priorité indique la probabilité que ce périphérique devienne le maître virtuel de la grappe, soit au démarrage, soit en cas d'échec d'un maître existant. Plus vous définissez la priorité (par exemple, 10), plus il est probable que ce périphérique devienne le maître de la grappe virtuelle.

  Remarque
  Si les périphériques de la grappe virtuelle sont mis sous tension à des moments différents, le premier périphérique mis sous tension assume le rôle de maître de la grappe virtuelle. Étant donné que chaque grappe virtuelle nécessite un maître, chaque périphérique de la grappe virtuelle vérifie, lorsqu'il est mis sous tension, que la grappe dispose d'un maître virtuel. S'il n'y en a pas, ce périphérique prend en charge le rôle. Les périphériques mis sous tension et ajoutés plus tard à la grappe deviennent des périphériques de secours. Si tous les périphériques de la grappe virtuelle sont mis sous tension simultanément, le périphérique dont le paramètre de priorité est le plus élevé devient le maître de la grappe virtuelle. Si au moins deux périphériques de la grappe virtuelle sont mis sous tension simultanément et ont le paramètre de priorité le plus élevé, celui qui a l'adresse IP la plus basse devient le maître de la grappe virtuelle.

- **NAT Assigned IPv4 Address** (Adresse IPv4 attribuée par la NAT) : spécifie l'adresse IP à laquelle l'adresse IP de ce périphérique est traduite par la NAT. Si la NAT n'est pas utilisée (ou si le périphérique ne se trouve pas derrière un pare-feu utilisant la NAT), laissez le champ vide.
- NAT Assigned IPv6 Address (adresse IPv6 attribuée par NAT) : spécifie l'adresse IP à laquelle l'adresse IP de ce périphérique est traduite par la NAT. Si la NAT n'est pas utilisée (ou si le périphérique ne se trouve pas derrière un pare-feu utilisant la NAT), laissez le champ vide.
- **Send FQDN to client** (Envoyer le nom de domaine complet au client) : cochez cette case pour que le maître de grappe VPN envoie un nom de domaine complet en utilisant l'hôte et le nom de domaine du périphérique de grappe au lieu de l'adresse IP externe lors de la redirection des connexions du client VPN vers ce périphérique de grappe.

  Par défaut, l'ASA envoie uniquement les adresses IP dans la redirection de l'équilibrage de charge à un client. Si les certificats utilisés reposent sur des noms DNS, ils ne seront pas valides lorsque les connexions sont redirigées vers un périphérique de secours.

  En tant que maître de la grappe VPN, cet ASA peut envoyer le nom de domaine pleinement qualifié (FQDN) d'un périphérique de la grappe (un autre ASA de la grappe), au moyen d'une recherche DNS inverse, au lieu de son adresse IP externe, lors de la redirection des connexions du client VPN vers ce périphérique de la grappe.

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

  Remarque
  Lors de l'utilisation d'IPv6 et de l'envoi de FQDN au client, ces noms doivent pouvoir être résolus par l'ASA au moyen du DNS.

Prochaine étape

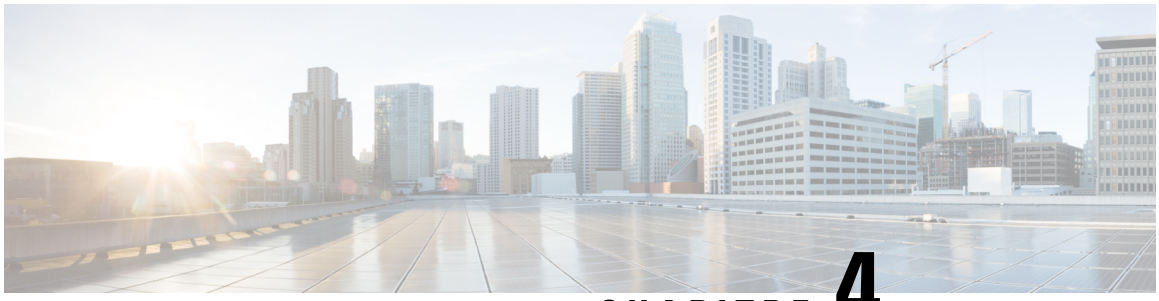
Lorsque plusieurs nœuds ASA sont regroupés pour l'équilibrage de la charge et que l'utilisation des URL de groupe est souhaitée pour les connexions Secure Client, les nœuds ASA individuels doivent :

- Configurez chaque profil de connexion d'accès à distance avec une URL de groupe pour chaque adresse de cluster 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.

Les URL de groupe sont configurées dans le volet **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) >**Secure Client **Connection Profiles (Profils de connexion)>** *connection profile name (nom du profil de connexion)* > **Add or Edit (Ajouter ou modifier) > Advanced (Avancé) > Group Alias / Group URL (Alias de groupe / URL de groupe)**.

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

Configuration générale du VPN

Options système

Le volet **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Advanced (Avancé) > IPsec > System Options (Options système)** (également

accessible à l'aide de **Configuration > Site-to-Site VPN (VPN de site à site) > Advanced (Avancé) > System Options (Options système)**) vous permet de configurer les fonctionnalités spécifiques aux sessions IPsec et VPN sur l'ASA.

- Limit the maximum number of active IPsec VPN sessions (Limiter le nombre maximal de sessions VPN IPsec actives) : active ou désactive la limitation du nombre maximal de sessions VPN IPsec actives. La plage dépend de la plateforme matérielle et de la licence logicielle.
  - Maximum IPsec Sessions (Nombre maximal de sessions IPsec) : spécifie le nombre maximal de sessions VPN IPsec actives autorisées. Ce champ est actif uniquement lorsque vous cochez la case précédente pour limiter le nombre maximal de sessions VPN IPsec actives.
- L2TP Tunnel Keepalive Timeout (Délai d'attente Keepalive du tunnel L2TP) : spécifie la fréquence, en secondes, des messages Keepalive. Plage : 10 à 300 secondes. La valeur par défaut est de 60 secondes. Il s'agit d'une option système avancée pour l'accès réseau (client) uniquement.
- Reclasser les flux existants lorsque les tunnels VPN sont établis
- Préserver les flux VPN avec état lorsque le tunnel tombe : active ou désactive la sauvegarde des flux tunnelisés IPsec en mode d'extension du réseau (NEM). Avec la fonctionnalité de flux de tunnel IPsec persistant activée, tant que le tunnel est recréé dans la boîte de dialogue d'expiration, les données continuent de circuler avec succès, car l'appareil de sécurité a toujours accès aux informations d'état. Cette option est désactivée par défaut.

Remarque 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).

- Durée de vie de l'association de sécurité IPsec : configure la durée d'une association de sécurité (SA). Ce paramètre spécifie comment mesurer la durée de vie des clés de SA IPsec, qui correspond à la durée de vie de la SA IPsec jusqu'à son expiration et doit être renégociée avec de nouvelles clés.
  - **Temps** : spécifie la durée de vie de la SA en heures (hh), minutes (mm) et en secondes (ss).
  - **Volume du trafic** : définit la durée de vie de la SA en termes de kilo-octets de trafic. Saisissez le nombre de kilo-octets de données de charge utile après lequel la SA IPsec expire, ou cochez la case unlimited (sans limite). Le minimum est de 100 Ko, la valeur par défaut est de 10 000 Ko, et le maximum est de 2 147 483 647 Ko.
- nable PMTU (Path Maximum Transmission Unit) Aging (Activer le vieillissement PMTU [Path Maximum Transmission Unit]) : permet à un administrateur d'activer le vieillissement PMTU.
  - Interval to Reset PMTU of an SA (Security Association) (Intervalle de réinitialisation du PMTU d'une SA [Security Association]) : saisissez le nombre de secondes après lesquelles la valeur PMTU d'une SA est réinitialisée à sa valeur d'origine.
- Activez les sessions IPsec entrantes pour contourner les listes d'accès de l'interface. La Stratégie de groupe et les listes de contrôle d'autorisation par utilisateur s'appliquent toujours au trafic. Par défaut, l'ASA permet au trafic VPN de se terminer sur une interface ASA; vous n'avez pas besoin d'autoriser IKE ou ESP (ou d'autres types de paquets VPN) dans une règle d'accès. Lorsque cette option est cochée,

vous n'avez pas non plus besoin d'une règle d'accès pour les adresses IP locales des paquets VPN déchiffrés. Comme le tunnel VPN a été terminé avec succès à l'aide des mécanismes de sécurité VPN, cette fonctionnalité simplifie la configuration et optimise les performances de l'ASA sans aucun risque de sécurité. (La Stratégie de groupe et les listes de contrôle d'autorisation par utilisateur s'appliquent toujours au trafic.)

Vous pouvez exiger qu'une règle d'accès s'applique aux adresses IP locales en décochant cette option. La règle d'accès s'applique à l'adresse IP locale, et non à l'adresse IP du client d'origine utilisée avant le déchiffrement du paquet VPN.

- Permit communication between VPN peers connected to the same interface (Autoriser la communication entre homologues VPN connectés à la même interface) : active ou désactive cette fonctionnalité.

  Vous pouvez également rediriger le trafic VPN client entrant vers la sortie de la même interface, non chiffrée ou chiffrée. Si vous renvoyez le trafic VPN par la même interface sans chiffrement, vous devez activer la NAT pour l'interface afin que les adresses publiquement routables remplacent vos adresses IP privées (sauf si vous utilisez déjà des adresses IP publiques dans votre ensemble d'adresses IP locales).

- Compression Settings (Paramètres de compression) : précise les fonctionnalités pour lesquelles vous souhaitez activer la compression : WebVPN et SSL VPN Client. La compression est activée par défaut.

Configurer le nombre maximal de sessions VPN

Pour spécifier le nombre maximal autorisé de sessions VPN Secure Client, procédez comme suit :

Procédure

Étape 1 Choisissez **Configuration** > **Remote Access** > **VPN (VPN d'accès à distance)** > **Advanced** > **(Avancé)** > **Maximum VPN Sessions** > **(Nombre maximal de sessions VPN).**

Étape 2 Dans le champ **Maximum Sessions** (Nombre maximal de sessions) Secure Client, saisissez le nombre maximal de sessions autorisées.

Les valeurs valides vont de 1 au nombre maximal de sessions autorisées par votre licence.

Étape 3 Dans le champ **Maximum Other VPN Sessions** (Nombre maximal d'autres sessions VPN), saisissez le nombre maximal de sessions VPN autorisées, ce qui inclut les sessions client VPN Cisco (IPsec IKEv1) et les sessions VPN de réseau à réseau.

Les valeurs valides vont de 1 au nombre maximal de sessions autorisées par votre licence.

Étape 4 Cliquez sur **Apply** (Appliquer).

Configurer DTLS

La sécurité de la couche de transport des datagrammes (DTLS) permet au Secure Client d'établir une connexion VPN SSL en utilisant 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 les performances des applications en temps réel sensibles aux retards de paquets.

Avant de commencer

Consultez Paramètres SSL, à la page 235pour configurer DTLS sur cette tête de réseau et connaître la version de DTLS 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 Stratégie de groupe interne, Secure Client, Détection d'homologue mort, à la page 92.

Procédure

Étape 1 Précisez les options DTLS pour les connexions VPN Secure Client :

a) Accédez à **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Secure Client Connection Profiles (Profils de connexion Secure Client/AnyConnect) , section Access Interfaces (Interfaces d'accès)**.

b) Dans le tableau **Interface**, sur la ligne de l'interface que vous configurez pour les connexions Secure Client, cochez les protocoles que vous souhaitez activer sur l'interface.

- Lorsque vous cochez ou activez **SSL Access / Allow Access** (Accès SSL / Autoriser l'accès), **Enable DTLS** (Activer DTLS) est coché ou activé par défaut.
- Pour désactiver DTLS, décochez la case **Enable DTLS** (Activer DTLS). Les connexions VPN SSL utiliseront uniquement un tunnel VPN SSL.

c) Choisissez **Port Settings (Paramètres de port)** pour configurer les **SSL Ports** (Ports SSL).

- **HTTPS Port** (Port HTTPS : le port à activer pour les connexions SSL HTTPS (basées sur le navigateur). La plage est comprise entre 1 et 65 535. La valeur du port par défaut est 443.
- **DTLS Port** (Port DTLS) : le port UDP à activer pour les connexions DTLS. La plage est comprise entre 1 et 65 535. La valeur du port par défaut est 443.

Étape 2 Précisez les options DTLS pour des stratégies de groupe spécifiques.

a) Accédez à **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Group Policies (Stratégies de groupe)**, puis à **Add/Edit (Ajouter/Modifier) > Advanced (Avancé) >** Secure Client.

b) Choisissez Inherit (default) (Hériter [par défaut]), Enable (Activer) ou Disable (Désactiver) **la sécurité de couche de transport datagramme (DTLS)**.

c) Choisissez Inherit (default) (Hériter [par défaut]), Enable (Activer) ou Disable (Désactiver) pour **DTLS Compression** (Compression DTLS), qui configure la compression pour DTLS.

Configurer les groupes de serveurs DNS

La boîte de dialogue **Configuration > Remote Access VPN (VPN d'accès à distance) > DNS** affiche les serveurs DNS configurés dans un tableau, y compris le nom du groupe de serveurs, les serveurs, le délai d'expiration en secondes, le nombre de tentatives autorisées et le nom de domaine. Vous pouvez ajouter, modifier ou supprimer des groupes de serveurs DNS dans cette boîte de dialogue.

- Add or Edit (Ajouter ou Modifier) : ouvre la boîte de dialogue Add or Edit DNS Server Group (Ajouter ou Modifier un groupe de serveurs DNS). De l'aide pour laquelle existe ailleurs
- Delete (Supprimer) : supprime la ligne sélectionnée du tableau. Il n'y a ni confirmation ni annulation.
- DNS Server Group (Groupe de serveurs DNS) : sélectionne le serveur à utiliser comme groupe de serveurs DNS pour cette connexion. La valeur par défaut est DefaultDNS.
- Manage (Gérer) : ouvre la boîte de dialogue Configure DNS Server Groups (Configurer les groupes de serveurs DNS).

Configurer l'ensemble des 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. Ces modifications peuvent accélérer le chemin de données du VPN SSL et offrir des gains de performance visibles par la clientèle dans Secure Client, 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

Étape 1 Choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Advanced (Avancé)** > **Crypto Engine (Moteur de chiffrement)**.

Étape 2 Dans la liste déroulante Accelerator Bias (Priorité de l'accélérateur), précisez comment allouer les processeurs accélérateurs de chiffrement :

Remarque
Ce champ ne s'affiche que si la fonctionnalité est disponible sur le périphérique.

- **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 favorisant l'administration/SSL. Utilisez ce biais lorsque vous prenez en charge les sessions VPN d'accès à distance Secure Client basées sur SSL.

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

Adressage du client pour les connexions VPN SSL

Utilisez cette boîte de dialogue pour spécifier la politique globale d'affectation d'adresses client et pour configurer des ensembles d'adresses propres à l'interface. Vous pouvez également ajouter, modifier ou supprimer des ensembles d'adresses propres à l'interface à l'aide de cette boîte de dialogue. Le tableau au bas de la boîte de dialogue répertorie les ensembles d'adresses propres à l'interface configurés

- Global Client Address Assignment Policy (Politique globale d'affectation d'adresses client) : configure une politique qui affecte toutes les connexions des clients VPN IPsec et SSL (y compris les connexions Secure Client). L'ASA utilise les sources sélectionnées dans l'ordre, jusqu'à ce qu'il trouve une adresse :
  - Use authentication server (Utiliser le serveur d'authentification) : spécifie que l'ASA doit tenter d'utiliser le serveur d'authentification comme source d'adresse client.
  - Use DHCP (Utiliser DHCP) : spécifie que l'ASA doit tenter d'utiliser DHCP comme source d'adresse client.
  - Use address pool (Utiliser l'ensemble d'adresses) : spécifie que l'ASA doit tenter d'utiliser des ensembles d'adresses comme source d'adresse client.
- Interface-Specific IPv4 Address Pools (Ensembles d'adresses IPv4 propres à l'interface) : répertorie les ensembles d'adresses propres à l'interface configurés.
- Interface-Specific IPv6 Address Pools (Ensembles d'adresses IPv6 propres à l'interface) : répertorie les ensembles d'adresses propres à l'interface configurés.
- Add (Ajouter) : ouvre la boîte de dialogue Assign Address Pools to Interface (affecter des ensembles d'adresses à l'interface), dans laquelle vous pouvez choisir une interface et un ensemble d'adresses à affecter.
- Edit (Modifier) : ouvre la boîte de dialogue Assign Address Pools to Interface (affecter des ensembles d'adresses à l'interface) avec les champs de l'interface et de l'ensemble d'adresses remplis.
- Delete (Supprimer) : supprime l'ensemble d'adresses propre à l'interface sélectionné. Il n'y a ni confirmation ni annulation.

affecter des ensembles d'adresses à l'interface

Utilisez cette boîte de dialogue pour choisir une interface et affecter un ou plusieurs ensembles d'adresses à cette interface.

- Interface : sélectionnez l'interface à laquelle vous souhaitez affecter un ensemble d'adresses. La valeur par défaut est DMZ.
- Address Pools (Ensembles d'adresses) : spécifiez un ensemble d'adresses à affecter à l'interface spécifiée.
- Select (Sélectionner) : ouvre la boîte de dialogue Select Address Pools (Sélectionner des ensembles d'adresses), dans laquelle vous pouvez choisir un ou plusieurs ensembles d'adresses à affecter à cette interface. Votre sélection s'affiche dans le champ Address Pools (Ensembles d'adresses) de la boîte de dialogue Assign Address Pools to Interface (affecter des ensembles d'adresses à l'interface).

Select Address Pools (Sélectionner des ensembles d'adresses)

La boîte de dialogue Select Address Pools (Sélectionner des ensembles d'adresses) affiche le nom du regroupement, les adresses de début et de fin, ainsi que le masque de sous-réseau des ensembles d'adresses disponibles pour l'affectation d'adresses client et vous permet d'ajouter, de modifier ou de supprimer des entrées de cette liste.

- Add (Ajouter) : ouvre la boîte de dialogue Add IP Pool (Ajouter un ensemble d'adresses IP), dans laquelle vous pouvez configurer un nouvel ensemble d'adresses IP.
- Edit (Modifier) : ouvre la boîte de dialogue Edit IP Pool (Modifier un ensemble d'adresses IP), dans laquelle vous pouvez modifier un ensemble d'adresses IP sélectionné.
- Delete (Supprimer) : supprime l'ensemble d'adresses sélectionné. Il n'y a ni confirmation ni annulation.
- Assign (Affecter) : affiche les noms des ensembles d'adresses qui demeurent affectés à l'interface. Cliquez deux fois sur chaque ensemble non affecté que vous souhaitez ajouter à l'interface. Le champ Assign (Affecter) met à jour la liste des affectations d'ensembles d'adresses.

Add or Edit an IP Address Pool (Ajouter ou modifier un ensemble d'adresses IP)

Configure ou modifie un ensemble d'adresses IP.

- Name (Nom) : spécifie le nom affecté à l'ensemble d'adresses IP.
- Starting IP Address (Adresse IP de début) : spécifie la première adresse IP du groupe.
- Ending IP Address (Adresse IP de fin) : spécifie la dernière adresse IP du groupe.
- Subnet Mask (Masque de sous-réseau) : sélectionne le masque de sous-réseau à appliquer aux adresses du groupe.

Stratégies de groupe

Une stratégie de groupe est un ensemble de paires attribut/valeur orientées utilisateur stockées soit en interne sur l'ASA, soit à l'externe sur un serveur RADIUS ou LDAP. Une stratégie de groupe attribue des attributs à un client lorsqu'il établit une connexion VPN. Par défaut, les utilisateurs VPN n'ont aucune association de stratégie de groupe. Les informations de stratégie de groupe sont utilisées par les profils de connexion VPN (groupes de tunnels) et les comptes d'utilisateurs.

L'ASA fournit une stratégie de groupe par défaut nommée DfltGrpPolicy. Les paramètres de stratégie de groupe par défaut sont ceux qui sont les plus susceptibles d'être communs à tous les groupes et utilisateurs, ce qui peut aider à simplifier la tâche de configuration. Les nouveaux groupes peuvent « hériter » des paramètres de cette stratégie de groupe par défaut, et les utilisateurs peuvent « hériter » des paramètres de leur groupe ou de la stratégie de groupe par défaut. Vous pouvez remplacer ces paramètres lorsque vous configurez les groupes et les utilisateurs.

Vous pouvez configurer des stratégies de groupe internes et externes. Une stratégie de groupe interne est stockée localement, et une stratégie de groupe externe est stockée à l'externe sur un serveur RADIUS ou LDAP.

Dans les boîtes de dialogue Group Policy (Stratégie de groupe), vous configurez les types de paramètres suivants :

- Attributs généraux : nom, bannière, ensemble d'adresses, protocoles, filtrage et paramètres de connexion.

- Serveurs : serveurs DNS et WINS, portée de DHCP et nom de domaine par défaut.
- Attributs avancés : tunnellisation fractionnée, serveur proxy de navigateur IE et Secure Client, et client IPsec.

Avant de configurer ces paramètres, vous devez configurer :

- Heures d'accès (Général | Plus d'options | Heures d'accès).
- Filtres (Général | Plus d'options | Filtres).
- Associations de sécurité IPsec (Configuration | Gestion des politiques | Gestion du trafic | Associations de sécurité).
- Listes de réseaux pour le filtrage et la tunnellisation fractionnée (Configuration | Gestion des politiques | Gestion du trafic | Listes de réseaux).
- Les serveurs d'authentification des utilisateurs et le serveur d'authentification interne (Configuration | Système | Serveurs | Authentification).

Vous pouvez configurer ces types de stratégies de groupe :

- Stratégies de groupe externes, à la page 65 : Une stratégie de groupe externe oriente l'ASA vers le serveur RADIUS ou LDAP pour récupérer une grande partie des informations de stratégie qui seraient autrement configurées dans une stratégie de groupe interne. Les stratégies de groupe externes sont configurées de la même manière pour les connexions Network (Client) Access VPN (VPN d'accès réseau [client]) et les connexions Site-to-Site VPN (VPN de site à site).
- Stratégies de groupe internes, à la page 67 : Ces connexions sont initiées par un client VPN installé sur le terminal. Le client pour et le client VPN IPsec Cisco sont des exemples de clients VPN. Une fois le client VPN authentifié, les utilisateurs distants peuvent accéder aux réseaux ou aux applications d'entreprise comme s'ils étaient sur site. Le trafic de données entre les utilisateurs distants et le réseau d'entreprise est sécurisé par chiffrement lorsqu'il passe par Internet.
- Stratégies de groupe internes Secure Client, à la page 74
- Stratégies de groupe internes, de site à site, à la page 99

Champs du volet de la Stratégie de groupe

Le volet Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau [client]) > Group Policies (Stratégies de groupe) dans ASDM répertorie les stratégies de groupe actuellement configurées. Les boutons Add (Ajouter), Edit (Modifier) et Delete (Supprimer) vous aident à gérer les stratégies de groupe VPN, comme décrit ci-dessous.

- Add (Ajouter) : propose une liste déroulante dans laquelle vous pouvez choisir d'ajouter une stratégie de groupe interne ou externe. Si vous cliquez simplement sur Add (Ajouter), vous créez par défaut une stratégie de groupe interne. Cliquer sur Add (Ajouter) ouvre la boîte de dialogue Add Internal Group Policy (Ajouter une stratégie de groupe interne) ou la boîte de dialogue Add External Group Policy (Ajouter une stratégie de groupe externe), qui vous permettent d'ajouter une nouvelle stratégie de groupe à la liste. Cette boîte de dialogue comprend trois sections de menu. Cliquez sur chaque élément de menu pour afficher ses paramètres. Lorsque vous vous déplacez d'un élément à l'autre, ASDM conserve vos paramètres. Lorsque vous avez terminé de définir les paramètres dans toutes les sections du menu, cliquez sur **Apply** (Appliquer) ou **Cancel** (Annuler).

- Edit (Modifier) : affiche la boîte de dialogue Edit Group Policy (Modifier la stratégie de groupe), qui vous permet de modifier une stratégie de groupe existante.
- Delete (Supprimer) : vous permet de supprimer une stratégie de groupe AAA de la liste. Il n'y a ni confirmation ni annulation.
- Assign (Affecter) : vous permet d'affecter une stratégie de groupe à un ou plusieurs profils de connexion.
- Name (Nom) : répertorie le nom des stratégies de groupe actuellement configurées.
- Type : répertorie le type de chaque stratégie de groupe actuellement configurée.
- Tunneling Protocol (protocole de tunnellisation) : répertorie le protocole de tunnellisation utilisé par chaque stratégie de groupe actuellement configurée
- Profils de connexion/utilisateurs affectés à : répertorie les profils de connexion et les utilisateurs configurés directement sur l'ASA qui sont associés à cette stratégie de groupe.

Stratégies de groupe externes

Les stratégies de groupe externes récupèrent les valeurs d'attribut d'autorisation et d'authentification d'un serveur externe. La stratégie de groupe identifie le groupe de serveurs RADIUS ou LDAP que l'ASA peut interroger pour les attributs et spécifie le mot de passe à utiliser lors de la récupération de ces attributs.

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.

Avant de configurer l'ASA pour utiliser un serveur externe, vous devez configurer ce serveur avec les attributs d'autorisation ASA appropriés et, à partir d'un sous-ensemble de ces attributs, affecter des autorisations spécifiques aux utilisateurs individuels. Suivez les instructions dans la section « Serveur externe pour l'autorisation et l'authentification » pour configurer votre serveur externe.

Ces configurations RADIUS comprennent RADIUS avec authentification locale, RADIUS avec Active Directory/Kerberos Windows DC, RADIUS avec domaine NT/4.0 et RADIUS avec LDAP.

Champs de la stratégie de groupe externe

- Name (Nom) : identifie la stratégie de groupe à ajouter ou à modifier. Pour modifier la stratégie de groupe externe, ce champ est d'affichage uniquement.
- Server Group (Groupe de serveurs) : répertorie les groupes de serveurs disponibles auxquels appliquer cette politique.
- New (Nouveau) : ouvre une boîte de dialogue qui vous permet de choisir de créer un nouveau groupe de serveurs RADIUS ou un nouveau groupe de serveurs LDAP. L'une ou l'autre de ces options ouvre la boîte de dialogue Add AAA Server Group (Ajouter un groupe de serveurs AAA).
- Password (Mot de passe) : spécifie le mot de passe de cette stratégie de groupe de serveurs.

Pour en savoir plus sur la création et la configuration de serveurs AAA, consultez le *Guide de configuration d'ASDM pour les opérations générales Cisco ASA*, le chapitre sur les *serveurs AAA et la base de données locale*.

Gestion des mots de passe avec les serveurs AAA

L'ASA prend en charge la gestion des mots de passe pour les protocoles RADIUS et LDAP. Il prend en charge l'option « password-expire-in-days » uniquement pour LDAP. Les autres paramètres sont valides pour les serveurs AAA qui prennent en charge une telle notification; c'est-à-dire RADIUS, RADIUS avec un serveur NT et des serveurs LDAP. L'ASA ignore cette commande si l'authentification RADIUS ou LDAP n'a pas été configurée.

Remarque Certains serveurs RADIUS qui prennent en charge MS-CHAP ne prennent actuellement pas en charge MS-CHAPv2. Cette fonctionnalité nécessite MS-CHAPv2, veuillez donc vérifier auprès de votre fournisseur.

L'ASA prend généralement en charge la gestion des mots de passe pour les types de connexion suivants lors de l'authentification auprès de LDAP ou avec toute configuration RADIUS prenant en charge MS-CHAPv2 :

- Module AnyConnect VPN de Cisco Secure Client
- Client VPN IPsec
- Clients IPsec IKEv2

La gestion des mots de passe n'est *pas* prise en charge pour Kerberos/Active Directory (mot de passe Windows) ou le domaine NT 4.0. Certains serveurs RADIUS, par exemple Cisco ACS, peuvent transmettre la demande d'authentification à un autre serveur d'authentification. Cependant, du point de vue de l'ASA, il communique uniquement avec un serveur RADIUS.

Remarque 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.

Prise en charge des mots de passe avec Secure Client

L'ASA prend en charge les fonctionnalités de gestion de mot de passe suivantes pour Secure Client :

- Avis d'expiration du mot de passe, lorsque l'utilisateur tente de se connecter.
- Rappels d'expiration de mot de passe, avant l'expiration du mot de passe.
- Remplacement de l'expiration du mot de passe. L'ASA ignore les avis d'expiration de mot de passe du serveur AAA et autorise la connexion de l'utilisateur.

Lorsque la gestion des mots de passe est configurée, l'ASA informe les utilisateurs distants lorsqu'ils tentent de se connecter que leur mot de passe actuel a expiré ou est sur le point d'expirer. 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 l'ancien mot de passe et modifier le mot de passe ultérieurement.

Secure Client ne peut pas lancer une modification du mot de passe; il peut uniquement répondre à une demande de modification provenant du serveur AAA par l'intermédiaire de l'ASA. Le serveur AAA doit être un serveur RADIUS proxy vers AD ou un serveur LDAP.

L'ASA ne prend pas en charge la gestion des mots de passe dans les conditions suivantes :

- lors de l'utilisation de l'authentification locale (interne)
- lors de l'utilisation de l'autorisation LDAP
- lors de l'utilisation de l'authentification RADIUS uniquement et lorsque les utilisateurs résident sur la base de données du serveur RADIUS

La définition du remplacement de l'expiration du mot de passe indique à l'ASA d'ignorer les instructions de désactivation de compte d'un serveur AAA. Il peut s'agir d'un risque pour la sécurité. Par exemple, vous pouvez ne pas modifier le mot de passe des administrateurs.

L'activation de la gestion des mots de passe entraîne l'envoi par l'ASA de demandes d'authentification MS-CHAPv2 au serveur AAA.

Stratégies de groupe internes

Stratégies de groupe internes, attributs généraux

Dans le volet **Configuration> Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Group Policies (Stratégies de groupe)**, la boîte de dialogue Add or Edit Group Policy (Ajouter ou Modifier une stratégie de groupe) vous permet de préciser les protocoles de tunnellisation, les filtres, les paramètres de connexion et les serveurs pour la stratégie de groupe en cours d'ajout ou de modification. Pour chacun des champs de cette boîte de dialogue, cocher la case Inherit (Hériter) permet au paramètre correspondant de prendre sa valeur à partir de la stratégie de groupe par défaut. Inherit (Hériter) est la valeur par défaut de tous les attributs de cette boîte de dialogue.

Vous configurez les attributs généraux d'une stratégie de groupe interne dans ASDM en sélectionnant **Configuration (Configuration) > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Group Policies (Stratégies de groupe) > Add/Edit (Ajouter/Modifier) > General (Général).** Les attributs suivants s'appliquent aux sessions VPN SSL et IPsec. Ainsi, certains attributs sont présents pour un type de session, mais pas pour l'autre.

- **Name** (Nom) : spécifie le nom de cette stratégie de groupe, jusqu'à 64 caractères; les espaces sont autorisés. Pour la fonction d'édition, ce champ est en lecture seule.
- **Banner (Bannière)** : spécifie le texte de bannière à présenter aux utilisateurs lors de la connexion. La longueur peut aller jusqu'à 4 000 caractères. Il n'y a pas de valeur par défaut.

  Le client VPN IPsec prend en charge le langage HTML complet pour la bannière. Cependant, le portail sans client et Secure Client prennent en charge le HTML partiel. Pour vous assurer que la bannière s'affiche correctement pour les utilisateurs distants, suivez les directives suivantes :

  - Pour les utilisateurs du client IPsec, utilisez la balise /n.
  - Pour les utilisateurs Secure Client, utilisez la balise
.

- **SCEP forwarding URL (URL de transfert SCEP)** : adresse de l'autorité de certification, requise lorsque le proxy SCEP est configuré dans le profil client.
- **Address Pools (Ensembles d'adresses)** : spécifie le nom d'un ou de plusieurs ensembles d'adresses IPv4 à utiliser pour cette stratégie de groupe. Si la case Inherit (Hériter) est cochée, la stratégie de groupe utilise l'ensemble d'adresses IPv4 précisé dans la stratégie de groupe par défaut. Consultez la section pour obtenir des renseignements sur l'ajout ou la modification d'un ensemble d'adresses IPv4.

Remarque Vous pouvez spécifier un ensemble d'adresses IPv4 et IPv6 pour une Stratégie de groupe interne.

Select (Sélectionner) : décochez la case Inherit (Hériter) pour activer ce bouton. Cliquez sur **Select** (Sélectionner) pour ouvrir la boîte de dialogue Address Pools (Ensembles d'adresses), qui affiche le nom de l'ensemble, les adresses de début et de fin et le masque de sous-réseau des ensembles d'adresses disponibles pour l'affectation d'adresses client et vous permet de choisir, d'ajouter, de modifier, de supprimer et d'affecter des entrées de cette liste.

- **IPv6 Address Pools** (Ensembles d'adresses IPv6) : spécifie le nom d'un ou de plusieurs ensembles d'adresses IPv6 à utiliser pour cette stratégie de groupe.

  Select (Sélectionner) : décochez la case Inherit (Hériter) pour activer ce bouton. Cliquez sur **Select** (Sélectionner) pour ouvrir la boîte de dialogue Select Address Pools (Sélectionner des ensembles d'adresses), comme décrit précédemment. Consultez la section pour obtenir des renseignements sur l'ajout ou la modification d'un ensemble d'adresses IPv6.

- **More Options** (Plus d'options) : cliquez sur les flèches vers le bas à droite du champ pour afficher des options configurables supplémentaires pour cette stratégie de groupe.
- **Tunneling Protocols** (Protocoles de tunnellisation) : spécifie les protocoles de tunnellisation que ce groupe peut utiliser. Les utilisateurs ne peuvent utiliser que les protocoles sélectionnés. Voici les différents choix proposés :
  - **Clientless SSL VPN** (VPN SSL sans client) : spécifie l'utilisation du VPN par SSL/TLS, qui utilise un navigateur Web pour établir un tunnel d'accès à distance sécurisé vers un ASA; ne nécessite ni logiciel ni matériel client. Le VPN SSL sans client peut fournir un accès facile à un large éventail de ressources d'entreprise, y compris les sites Web d'entreprise, les applications Web, le partage de fichiers NT/AD (activé sur le Web), le courriel et d'autres applications basées sur TCP à partir de presque n'importe quel ordinateur qui peut atteindre les sites Internet HTTPS.
  - **SSL VPN Client** (Client VPN SSL) : spécifie l'utilisation du module VPN AnyConnect de Cisco Secure Client, du ou de l'ancien client VPN SSL. Si vous utilisez Secure Client, vous devez choisir ce protocole pour que la sécurité des utilisateurs mobiles (MUS) soit prise en charge.
  - **IPsec IKEv1** : protocole de sécurité IP. Considéré comme le protocole le plus sécurisé, IPsec fournit l'architecture la plus complète pour les tunnels VPN. Les connexions de site à site (homologue à homologue) et les connexions de client VPN Cisco à réseau local (LAN) peuvent utiliser IPsec IKEv1.
  - **IPsec IKEv2** : pris en charge par le Secure Client . Les connexions Secure Client utilisant IPsec avec IKEv2 fournissent des fonctionnalités avancées telles que les mises à jour logicielles, les profils clients, la localisation (traduction) et la personnalisation de l'interface graphique, Cisco Secure Desktop et le proxy SCEP.

- **L2TP sur IPsec (L2TP over IPsec)** : permet aux utilisateurs distants avec des clients VPN fournis avec plusieurs systèmes d'exploitation courants pour PC et PC mobiles d'établir des connexions sécurisées sur le réseau IP public avec l'appareil de sécurité et les réseaux privés d'entreprise. L2TP utilise PPP sur UDP (port 1701) pour tunnelliser les données. L'appareil de sécurité doit être configuré pour le mode de transport IPsec.

- **Filter** (Filtre) : spécifie la liste de contrôle d'accès à utiliser pour une connexion IPv4 ou IPv6, ou s'il faut hériter de la valeur de la stratégie de groupe. Les filtres se composent de règles qui déterminent s'il faut autoriser ou rejeter les paquets de données tunnelisés transitant par l'ASA, en fonction de critères tels que l'adresse source, l'adresse de destination et le protocole. 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. Pour configurer les filtres et les règles, cliquez sur **Manage** (Gérer).
- **NAC Policy** (Politique NAC) : sélectionne le nom d'une stratégie de contrôle d'admission au réseau à appliquer à cette stratégie de groupe. Vous pouvez affecter une politique NAC facultative à chaque Stratégie de groupe. La valeur par défaut est None (Aucun).
- **Manage** (Gérer) : ouvre la boîte de dialogue Configure NAC Policy (Configurer la politique NAC). Après avoir configuré une ou plusieurs politiques NAC, les noms de politiques NAC s'affichent sous forme d'options dans la liste déroulante à côté de l'attribut de politique NAC.
- **Access Hours** (Heures d'accès) : sélectionne le nom d'une politique d'heures d'accès existante, le cas échéant, appliquée à cet utilisateur ou crée une nouvelle politique d'heures d'accès. La valeur par défaut est Inherit (Hériter) ou, si la case Inherit (Hériter) n'est pas cochée, la valeur par défaut est Unrestricted (Non restreinte). Cliquez sur **Manage** (Gérer) pour ouvrir la boîte de dialogue Browse Time Range (Parcourir la plage temporelle), dans laquelle vous pouvez ajouter, modifier ou supprimer une plage temporelle.
- **Simultaneous Logins Per User** (Connexions simultanées par utilisateur) : précise le nombre maximal de connexions simultanées autorisées pour cet utilisateur. La valeur par défaut est 3. La valeur minimale est 0, ce qui désactive la connexion et empêche l'accès de l'utilisateur.

Remarque Bien qu'il n'y ait pas de limite maximale, autoriser plusieurs connexions simultanées peut compromettre la sécurité et affecter les performances.

- **Restrict Access to VLAN** (Restreindre l'accès au VLAN) : également appelé « mappage VLAN », ce paramètre spécifie l'interface VLAN de sortie des sessions auxquelles cette stratégie de groupe s'applique. L'ASA transfère tout le trafic de ce groupe vers le VLAN sélectionné. Utilisez cet attribut pour affecter un VLAN à la politique de groupe pour simplifier le contrôle d'accès. L'affectation d'une valeur à cet attribut est une alternative à l'utilisation de listes de contrôle d'accès pour filtrer le trafic sur une session. En plus de la valeur par défaut (Unrestricted) (non restreinte), la liste déroulante affiche uniquement les VLAN configurés dans cet ASA.

Remarque Cette fonctionnalité fonctionne pour les connexions HTTP, mais pas pour FTP et CIFS.

- **Connection Profile (Tunnel Group) Lock** (Verrouillage du profil de connexion [groupe de tunnels]) : ce paramètre permet l'accès VPN à distance uniquement avec le profil de connexion sélectionné (groupe

de tunnels) et empêche l'accès avec un profil de connexion différent. La valeur héritée par défaut est None (Aucun).

- **Maximum Connect Time** (Durée maximale de connexion) : si la case **Inherit** (Hériter) n'est pas cochée, ce paramètre définit la durée maximale de connexion de l'utilisateur en minutes.

  À la fin de cette durée, le système met fin à la connexion. La durée minimale est de 1 minute et la durée maximale est de 35 791 394 minutes. Pour autoriser une durée de connexion illimitée, cochez **Unlimited** (Illimité) (par défaut).

- **Idle Timeout** (Délai d'inactivité) : si la case **Inherit** (Hériter) n'est pas cochée, ce paramètre définit le délai d'inactivité en minutes.

  S'il n'y a aucune activité de communication sur la connexion pendant cette période, le système arrête la connexion. La durée minimale est de 1 minute, la durée maximale est de 10080 minutes et la valeur par défaut est de 30 minutes. Pour autoriser un temps de connexion illimité, cochez **Unlimited** (Illimité).

- **Security Group Tag (SGT)** (Balise du groupe de sécurité [SGT]) : saisissez la valeur numérique de la balise SGT qui sera affectée aux utilisateurs VPN se connectant avec cette stratégie de groupe.

- **On smart card remova**l (Lors du retrait de la carte à puce) : avec l'option par défaut Disconnect (Déconnecter), le client interrompt la connexion si la carte à puce utilisée pour l'authentification est retirée. Cliquez sur **Keep the connection** (Maintenir la connexion) si vous ne souhaitez pas exiger que les utilisateurs conservent leur carte à puce dans l'ordinateur pendant toute la durée de la connexion.

  La configuration du retrait des cartes à puce ne fonctionne que sur Microsoft Windows utilisant des cartes à puce RSA.

- **Disable Delete tunnel with no delay in Simultaneous Session preempt** (Désactiver la suppression du tunnel sans délai dans la préemption de session simultanée) : lorsqu'un utilisateur donné atteint la limite autorisée de **Simultaneous Logins** (Connexions simultanées), la prochaine tentative de connexion de l'utilisateur oblige le système à supprimer d'abord la session la plus ancienne. Cette suppression peut prendre quelques secondes, ce qui peut empêcher l'utilisateur d'établir immédiatement une nouvelle session. Sélectionnez cette option pour demander au système d'établir la nouvelle session sans attendre la fin de la suppression de la session la plus ancienne.

- **Maximum Connection Time Alert Interval** (Intervalle d'alerte du temps de connexion maximal) : intervalle de temps avant que le temps de connexion maximal ne soit atteint et qu'un message s'affiche pour l'utilisateur.

  Si vous décochez la case **Inherit** (Hériter), la case **Default** (Par défaut) est cochée automatiquement. Ainsi, l'intervalle d'alerte de session est défini à 30 minutes. Si vous souhaitez spécifier une nouvelle valeur, décochez **Default** (Par défaut) et spécifiez un intervalle d'alerte de session de 1 à 30 minutes.

- **Periodic Certificate Authentication Interval** (Intervalle d'authentification périodique du certificat) : intervalle de temps en heures avant que l'authentification du certificat soit relancée périodiquement.

  Si la case **Inherit** (Hériter) n'est pas cochée, vous pouvez définir l'intervalle d'exécution de la vérification périodique du certificat. La plage est comprise entre 1 et 168 heures, et la valeur par défaut est désactivée. Pour autoriser une vérification illimitée, cochez Unlimited (Illimité).

Configurer la stratégie de groupe interne, les attributs du serveur

Configurez les serveurs DNS, les serveurs WINS et la portée DHCP dans la fenêtre Group Policy > Servers (Stratégie de groupe > Serveurs). Les serveurs DNS et WINS sont appliqués uniquement aux clients de tunnel

complet (IPsec, Secure Client, SVC et L2TP/IPsec) et sont utilisés pour la résolution de noms. La portée DHCP est utilisée lorsque l'affectation d'adresses DHCP est en place.

Procédure

Étape 1 Choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Network (Client) Access (Accès réseau [client])** > **Group Policies (Stratégies de groupe)** > **Add/Edit (Ajouter/Modifier)** > **Servers (Serveurs)**.

Étape 2 Sauf si vous modifiez la DefaultGroupPolicy, décochez la case **DNS Servers Inherit** (Hériter des serveurs DNS) et ajoutez les adresses IPv4 ou IPv6 des serveurs DNS que vous souhaitez que ce groupe utilise. Vous pouvez spécifier deux adresses IPv4 et deux adresses IPv6.

Si vous spécifiez plusieurs serveurs DNS, le client d'accès à distance tente d'utiliser les serveurs DNS dans l'ordre que vous spécifiez dans ce champ.

Les modifications que vous apportez ici remplacent le paramètre DNS configuré dans ASDM dans la fenêtre **Configuration > Remote Access VPN (VPN d'accès à distance) > DNS** pour les clients utilisant cette stratégie de groupe.

Étape 3 Décochez la case WINS Servers **Inherit** (Hériter des serveurs WINS) et saisissez les adresses IP des serveurs WINS principal et secondaire. La première adresse IP que vous spécifiez est celle du serveur WINS principal. La deuxième adresse IP (facultative) que vous spécifiez est celle du serveur WINS secondaire. .

Étape 4 Développez la zone **More Options** (Plus d'options) en cliquant sur la double flèche vers le bas dans la barre More Options (Plus d'options).

Étape 5 Décochez **DHCP Scope Inherit** (Hériter de la portée DHCP) et définissez la portée DHCP.

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.

Étape 6 Si aucun domaine par défaut n'est spécifié dans la fenêtre **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **DNS**, vous devez préciser le domaine par défaut dans le champ **Default Domain** (Domaine par défaut). Utilisez le nom de domaine et le domaine de niveau supérieur par exemple, exemple.com.

Étape 7 Cliquez sur **OK**.

Étape 8 Cliquez sur **Apply** (Appliquer).

Stratégies de groupe internes, proxy de navigateur

Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Group Policies (Stratégies de groupe) > Add/Edit (Ajouter/Modifier) > Advanced (Avancé) > Browser Proxy (proxy de navigateur)

Cette boîte de dialogue configure les attributs qui seront transmis au client pour reconfigurer les paramètres de Microsoft Internet Explorer :

- Proxy Server Policy (Politique du serveur proxy) : configure les actions (« méthodes ») du serveur proxy du navigateur Microsoft Internet Explorer pour un PC client.
  - Do not modify client proxy settings (Ne pas modifier les paramètres proxy du client) : laisse inchangé le paramètre du serveur proxy du navigateur HTTP dans Internet Explorer pour ce PC client.
  - Do not use proxy (Ne pas utiliser de serveur proxy) : désactive le paramètre du serveur proxy HTTP dans Internet Explorer pour le PC client.
  - Select proxy server settings from the following (Sélectionner les paramètres du serveur proxy parmi les éléments suivants) : active les cases suivantes pour vos sélections : Auto detect proxy (Détecter automatiquement le proxy), Use proxy server settings given below (Utiliser les paramètres du serveur proxy indiqués ci-dessous) et Use proxy auto configuration (PAC) given below (Utiliser la configuration automatique du serveur proxy [PAC] indiquée ci-dessous).
  - Auto detect proxy (Détecter automatiquement le proxy) : active l'utilisation de la détection automatique du serveur proxy dans Internet Explorer pour le PC client.
  - Use proxy server settings specified below (Utiliser les paramètres du serveur proxy spécifiés ci-dessous) : définit le paramètre du serveur proxy HTTP dans Internet Explorer pour utiliser la valeur configurée dans le champ Proxy Server Name or IP Address (Nom ou adresse IP du serveur proxy).
  - Use proxy auto configuration (PAC) given below (Utiliser la configuration automatique du serveur proxy [PAC] indiquée ci-dessous) : spécifie l'utilisation du fichier précisé dans le champ Proxy Auto Configuration (PAC) comme source des attributs de configuration automatique.
- Proxy Server Settings (Paramètres du serveur proxy) : configure les paramètres du serveur proxy pour les clients Microsoft utilisant Microsoft Internet Explorer.
  - Server Address and Port (Adresse et port du serveur) : spécifie l'adresse IP ou le nom et le port d'un serveur Microsoft Internet Explorer appliqué à ce PC client.
  - Bypass Proxy Server for Local Addresses (Contourner le serveur proxy pour les adresses locales) : configure les paramètres de contournement local du navigateur Microsoft Internet Explorer pour un PC client. Cliquez sur **Yes** (Oui) pour activer le contournement local ou sur **No** (Non) pour désactiver le contournement local.
  - Exception List (Liste d'exceptions) : répertorie les noms de serveur et les adresses IP que vous souhaitez exclure de l'accès au serveur proxy. Saisissez la liste des adresses auxquelles vous ne souhaitez pas avoir accès par l'intermédiaire d'un serveur proxy. Cette liste correspond à la liste Exceptions dans la boîte de dialogue Proxy Settings (Paramètres proxy) dans Internet Explorer.
- Proxy Auto Configuration Settings (Paramètres de configuration automatique du serveur proxy) : l'URL PAC spécifie l'URL du fichier de configuration automatique. Ce fichier indique au navigateur où rechercher les informations du serveur proxy. Pour utiliser la fonctionnalité de configuration automatique du serveur proxy (PAC), l'utilisateur distant doit utiliser le module VPN de Cisco Secure Client.

De nombreux environnements réseau définissent des serveurs proxy HTTP qui connectent un navigateur Web à une ressource réseau particulière. Le trafic HTTP ne peut atteindre la ressource réseau que si le serveur proxy est spécifié dans le navigateur et si le client achemine le trafic HTTP vers le serveur proxy. Les tunnels SSLVPN compliquent la définition des serveurs proxy HTTP, car le serveur proxy requis lors de la tunnellisation vers un réseau d'entreprise peut différer de celui requis lorsqu'il est connecté à Internet par l'intermédiaire d'une connexion à large bande ou sur un réseau tiers.

En outre, les entreprises disposant de réseaux étendus peuvent devoir configurer plusieurs serveurs proxy et permettre aux utilisateurs de choisir entre eux, en fonction des conditions transitoires. En utilisant les fichiers .pac, un administrateur peut créer un seul fichier de script qui détermine lequel des nombreux serveurs proxy utiliser pour tous les ordinateurs clients de l'entreprise.

Voici quelques exemples de la façon dont vous pourriez utiliser un fichier PAC :

- Choix aléatoire d'un serveur proxy dans une liste pour l'équilibrage de charge.
- Rotation des serveurs proxy selon l'heure du jour ou le jour de la semaine pour s'adapter à un calendrier de maintenance de serveur.
- Spécifiez un serveur proxy de secours à utiliser en cas de défaillance du serveur proxy principal.
- Spécifiez le serveur proxy le plus proche pour les utilisateurs itinérants, selon le sous-réseau local.

Vous pouvez utiliser un éditeur de texte pour créer un fichier de configuration automatique du serveur proxy (.pac) pour votre navigateur. Un fichier .pac est un fichier JavaScript contenant une logique qui spécifie un ou plusieurs serveurs proxy à utiliser, selon le contenu de l'URL. Utilisez le champ PAC URL pour préciser l'URL à partir de laquelle récupérer le fichier .pac. Ensuite, le navigateur utilise le fichier .pac pour déterminer les paramètres du serveur proxy.

- Verrouillage du serveur proxy
  - Allow Proxy Lockdown for Client System (Autoriser le verrouillage du serveur proxy pour le système client) : l'activation de cette fonctionnalité masque l'onglet Connexions dans Microsoft Internet Explorer pendant la durée d'une session VPN Secure Client. En outre, à partir de Windows 10 version 1703 (ou version ultérieure), l'activation de cette fonctionnalité masque également l'onglet du serveur proxy système dans l'application Settings (Paramètres) pendant la durée d'une session VPN Secure Client . La désactivation de cette fonctionnalité laisse inchangé l'affichage de l'onglet Connexions dans Microsoft Internet Explorer et de l'onglet Proxy (Proxy) dans l'application Settings (Paramètres); le paramètre par défaut de ceux-ci peut être affiché ou masqué, selon les paramètres du registre utilisateur.

Remarque Le masquage de l'onglet du serveur proxy système dans l'application Settings (Paramètres) pendant la durée d'une session VPN Secure Client nécessite AnyConnect version 4.7.03052 ou une version ultérieure.

Stratégies de groupe internes Secure Client

Stratégies de groupe internes, Avancées, Secure Client

- Keep Installer on Client System (Conserver le programme d'installation sur le système client) : activez cette option pour permettre l'installation permanente du client sur l'ordinateur distant. L'activation désactive la fonction de désinstallation automatique du client. Le client reste installé sur l'ordinateur distant pour les connexions ultérieures, réduisant ainsi le temps de connexion pour l'utilisateur distant.
- Compression : la compression augmente les performances des communications entre l'appareil de sécurité et le client en réduisant la taille des paquets transférés.
- Datagram TLS — Datagram Transport Layer Security (Sécurité de couche de transport datagramme) : évite les problèmes de latence et de bande passante associés à certaines connexions SSL et améliore les performances des applications en temps réel sensibles aux retards de paquets.
- Ignore Don't Defrag (DF) Bit (Ignorer le bit Don't Defrag [DF]) : cette fonctionnalité permet la fragmentation forcée des paquets dont le bit DF est activé, leur permettant de passer par le tunnel. Un exemple de cas d'utilisation concerne les serveurs de votre réseau qui ne répondent pas correctement aux négociations TCP MSS.
- Client Bypass Protocol (Protocole de contournement client) : la fonctionnalité Client Protocol Bypass vous permet de configurer la façon dont Secure Client gère le trafic IPv4 lorsque l'ASA s'attend uniquement à du trafic IPv6 ou la façon dont il gère le trafic IPv6 lorsqu'il s'attend uniquement à du trafic IPv4.

  Lorsque Secure Client établit une connexion VPN avec l'ASA, l'ASA peut lui affecter une adresse IPv4, IPv6 ou à la fois une adresse IPv4 et IPv6. Si l'ASA attribue à la connexion Secure Client 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 affecté 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 une connexion Secure Client et que le terminal soit à 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.

- FQDN of This Device (Nom de domaine complet de ce périphérique) : ces informations sont utilisées par le client après l'itinérance réseau afin de résoudre l'adresse IP ASA utilisée pour rétablir la session VPN. Ce paramètre est essentiel pour prendre en charge l'itinérance entre des réseaux utilisant différents protocoles IP (comme IPv4 et IPv6).

Remarque Vous ne pouvez pas utiliser le FQDN de l'ASA présent dans le profil Secure Client 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 FQDN du périphérique n'est pas transmis au client, le client tente de se reconnecter à l'adresse IP précédemment établie par le tunnel. Afin de prendre en charge l'itinérance entre les réseaux de différents protocoles IP (de IPv4 à IPv6), Secure Client 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 FQDN ASA présent dans son profil lors de la connexion initiale. Lors des reconnexions de session ultérieures, il utilise toujours le FQDN du périphérique transmis par l'ASA (et configuré par l'administrateur dans la stratégie de groupe), lorsqu'il est disponible. Si le FQDN n'est pas configuré, l'ASA dérive le FQDN du périphérique (et l'envoie au client) à partir de ce qui est défini sous 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.

- MTU : ajuste la taille MTU pour les connexions SSL. Saisissez une valeur en octets, comprise entre 256 et 1 410 octets. Par défaut, la taille MTU est ajustée automatiquement en fonction de la MTU de l'interface utilisée par la connexion, moins la surcharge IP/UDP/DTLS.
- Keepalive Messages (Messages Keepalive) : saisissez une valeur comprise entre 15 et 600 secondes dans le champ Interval (Intervalle) afin d'activer et d'ajuster l'intervalle des messages Keepalive pour garantir qu'une connexion par l'intermédiaire d'un serveur proxy, d'un pare-feu ou d'un périphérique NAT reste ouverte, même si le périphérique limite la durée d'inactivité de la connexion. L'ajustement de l'intervalle garantit également que le client 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.
- **Optional Client Modules to Download** (Modules client facultatifs à télécharger) : pour réduire le temps de téléchargement, Secure Client demande uniquement les téléchargements (à partir de l'ASA) des modules dont il a besoin pour chaque fonctionnalité prise en charge. Vous devez préciser les noms des modules qui activent d'autres fonctionnalités. Secure Client comprend les modules suivants (certaines versions antérieures ont moins de modules) :
  - Secure ClientDART : Diagnostic Reporting Tool (DART) (outil de rapport de diagnostic [DART]) Secure Client capture un instantané des journaux système et d'autres renseignements diagnostiques et crée un fichier .zip sur votre bureau afin que vous puissiez facilement envoyer des renseignements de dépannage au centre d'assistance technique Cisco.
  - Secure Client Network Access Manager (Gestionnaire d'accès réseau) : anciennement appelé Cisco Secure Services Client, ce module fournit la norme 802.1X (couche 2) et l'authentification des périphériques pour l'accès aux réseaux câblés et sans fil.
  - Secure Client SBL—Start Before Logon (SBL) (Démarrer avant la connexion [SBL]) : force l'utilisateur à se connecter à l'infrastructure de l'entreprise par l'intermédiaire d'une connexion VPN avant de se connecter à Windows en démarrant Secure Client avant l'affichage de la boîte de dialogue de connexion Windows.
  - Secure Firewall Posture Module (Module de posture de pare-feu sécurisé) : anciennement appelé fonctionnalité Cisco Secure Desktop HostScan, le module de posture est intégré dans Secure Client et permet Secure Client de recueillir des renseignements d'authentification pour l'évaluation de la posture avant de créer une connexion d'accès à distance avec l'ASA.
  - ISE Posture (Posture ISE) : utilise la bibliothèque OPSWAT v3 pour effectuer des vérifications de posture afin d'évaluer la conformité d'un terminal. Vous pouvez ensuite restreindre l'accès réseau jusqu'à ce que le terminal soit conforme ou élever les privilèges de l'utilisateur local.

- AMP Enabler (Facilitateur AMP) : utilisé comme moyen de déployer Advanced Malware Protection (AMP) pour les terminaux. Il pousse le logiciel AMP for Endpoints vers un sous-ensemble de terminaux à partir d'un serveur hébergé localement dans l'entreprise et installe les services AMP auprès de sa base d'utilisateurs existante.
- Network Visibility Module (Module de visibilité du réseau) : améliore la capacité de l'administrateur d'entreprise à effectuer la planification de capacité et des services, l'audit, la conformité et l'analyse de sécurité. NVM recueille les données de télémétrie du terminal et consigne les données de flux et la réputation de fichier dans le journal système et exporte également les enregistrements de flux vers un collecteur (un prestataire tiers), qui effectue l'analyse des fichiers et fournit une interface utilisateur.
- Umbrella Roaming Security Module (Module de sécurité d'itinérance Umbrella) : fournit une sécurité de couche DNS lorsqu'aucun VPN n'est actif. Il fournit un abonnement soit au service Cisco Umbrella Roaming soit aux services OpenDNS Umbrella, qui ajoutent des fonctionnalités Intelligent Proxy et IP-Layer Enforcement. Le profil Umbrella Security Roaming associe chaque déploiement au service correspondant et active automatiquement le niveau de protection correspondant (filtrage de contenu, politiques multiples, rapports robustes, intégration Active Directory ou sécurité de base de couche DNS).

- Always-On VPN (VPN permanent) : déterminez si le paramètre d'indicateur VPN permanent dans le profil de service Secure Client est désactivé ou si le paramètre du profil de service Secure Client doit être utilisé. La fonctionnalité VPN permanent permet à AnyConnect d'établir automatiquement une session VPN après l'ouverture de session de l'utilisateur sur un ordinateur. La session VPN reste active jusqu'à la fermeture de session de l'utilisateur sur l'ordinateur. Si la connexion physique est perdue, la session reste active et Secure Client tente continuellement de rétablir la connexion physique avec l'appareil de sécurité adaptatif afin de reprendre la session VPN.

  Le VPN permanent permet d'appliquer les politiques d'entreprise afin de protéger le périphérique contre les menaces de sécurité. Vous pouvez l'utiliser pour vous assurer que Secure Client établit une session VPN chaque fois que le terminal ne se trouve pas dans un réseau de confiance. Si elle est activée, une politique est configurée pour déterminer comment la connectivité réseau est gérée en l'absence de connexion.

Remarque Le VPN permanent nécessite une version Secure Client qui prend en charge les fonctionnalités Secure Client .

- Client Profiles to Download (Profils client à télécharger) : un profil est un groupe de paramètres de configuration que Secure Client utilise pour configurer les paramètres VPN, Network Access Manager (Gestionnaire d'accès réseau), Web Security (Sécurité Web), ISE Posture (Posture ISE), AMP Enabler (Facilitateur AMP), Network Visibility Module (Module de visibilité du réseau) et Umbrella Roaming Security (Module de sécurité Umbrella Roaming). Cliquez sur **Add** (Ajouter) pour lancer la fenêtre Select Profiles (Sélectionner les profils) Secure Client, dans laquelle vous pouvez spécifier les profils créés précédemment pour cette stratégie de groupe.

Configurer la tunnellisation fractionnée pour le trafic Secure Client

La tunnellisation fractionnée dirige une partie du trafic réseau Secure Client dans le tunnel VPN (chiffré) et le trafic réseau restant à l'extérieur du tunnel VPN (non chiffré ou « en clair »).

La tunnellisation fractionnée est configurée en créant une politique de tunnellisation fractionnée, en configurant une liste de contrôle d'accès pour cette politique et en ajoutant la politique de tunnellisation fractionnée à une Stratégie de groupe. Lorsque la Stratégie de groupe est envoyée au client, ce client utilise les listes de contrôle d'accès de la politique de tunnellisation fractionnée pour décider par où diriger le trafic réseau.

Remarque La tunnellisation 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 tunnellisation fractionnée.

Pour les clients Windows, les règles de pare-feu de l'ASA sont évaluées en premier, puis celles du client. Pour Mac OS X, les règles de pare-feu et de filtre du client ne sont pas utilisées. Pour les systèmes Linux, à partir d'AnyConnect version 3.1.05149, vous pouvez configurer Secure Client pour évaluer les règles de pare-feu et de filtre du client en ajoutant un attribut personnalisé nommé circumvent-host-filtering à un profil de groupe et en le définissant à true.

Lorsque vous créez des listes d'accès

- Vous pouvez spécifier des adresses IPv4 et IPv6 dans une liste de contrôle d'accès.
- Si vous utilisez une liste de contrôle d'accès standard, une seule adresse ou un seul réseau est utilisé.
- Si vous utilisez des listes de contrôle d'accès étendues, le réseau source est le réseau de tunnellisation fractionnée. Le réseau de destination est ignoré.
- Les listes d'accès configurées avec any ou avec une inclusion ou exclusion fractionnée de 0.0.0.0/0.0.0.0 ou ::/0 ne seront pas envoyées au client. Pour envoyer tout le trafic dans le tunnel, choisissez **Tunnel All Networks**pour le split-tunnel **Policy**.
- L'adresse 0.0.0.0/255.255.255.255 ou ::/128 est envoyée au client uniquement lorsque la politique de tunnellisation fractionnée est **Exclude Network List Below**. Cette configuration indique au client de ne pas tunneliser le trafic destiné aux sous-réseaux locaux.
- Secure Client transmet le trafic à tous les sites spécifiés dans la politique de tunnellisation fractionnée et à tous les sites appartenant au même sous-réseau que l'adresse IP affectée par l'ASA. Par exemple, si l'adresse IP affectée par l'ASA est 10.1.1.1 avec un masque 255.0.0.0, le périphérique terminal transmet tout le trafic destiné à 10.0.0.0/8, quelle que soit la politique de tunnellisation fractionnée. Par conséquent, utilisez un masque réseau pour l'adresse IP affectée qui fait correctement référence au sous-réseau local attendu.

Avant de commencer

- Vous devez créer une liste d'accès avec les ACE appropriées.
- Si vous avez créé une politique de tunnelisation fractionnée pour les réseaux IPv4 et une autre pour les réseaux IPv6, la liste d'accès que vous spécifiez est utilisée pour les deux protocoles. Ainsi, la liste d'accès doit contenir des entrées de contrôle d'accès (ACE) pour le trafic IPv4 et IPv6. Si vous n'avez pas créé ces listes de contrôle d'accès, consultez le guide de configuration sur les opérations générales.

Dans la procédure suivante, dans tous les cas où une case Inherit (Hériter) se trouve à côté d'un champ, laisser la case Inherit (Hériter) cochée signifie que la stratégie de groupe que vous configurez utilise les mêmes valeurs pour ce champ que la stratégie de groupe par défaut. Décochez la case Inherit (Hériter) pour spécifier de nouvelles valeurs propres à votre stratégie de groupe.

Procédure

Étape 1 Connectez-vous à l'ASA à l'aide d'ASDM et accédez à Configuration **(Configuration)** > **Remote Access VPN (VPN d'accès à distance)** > **Network (Client) Access (Accès réseau [client])** > **Group Policies (Stratégies de groupe)**.

Étape 2 Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle stratégie de groupe ou choisissez une stratégie de groupe existante et cliquez sur **Edit** (Modifier).

Étape 3 Sélectionnez **Advanced (Avancé)** > **Split Tunneling (Tunnellisation fractionnée)**.

Étape 4 Dans le champ **DNS Names** (Noms DNS), saisissez les noms de domaine qui doivent être résolus par Secure Client via le tunnel. Ces noms correspondent à des hôtes dans le réseau privé. Si la tunnellisation fractionnée par inclusion est configurée, la liste de réseaux doit inclure les serveurs DNS spécifiés. Vous pouvez saisir un nom de domaine pleinement qualifié, une adresse IPv4 ou IPv6 dans le champ.

Un nom de domaine de tunnellisation fractionnée dynamique nécessite au moins une étiquette de nom de domaine à côté du domaine de niveau supérieur. Étant donné que la tunnellisation fractionnée dynamique est destinée à cibler les flux correspondant à des noms de domaine spécifiques, préciser uniquement un domaine de niveau supérieur (comme *org*) est inacceptable. Vous devez saisir le domaine de niveau supérieur et au moins une étiquette de nom de domaine (comme *domain.org)*.

Étape 5 Pour désactiver la tunnellisation fractionnée, cliquez sur **Yes** (Oui) pour activer **Send All DNS Lookups Through Tunnel** (Envoyer toutes les recherches DNS par le tunnel). Cette option garantit que le trafic DNS n'est pas transmis à l'adaptateur physique; il refuse le trafic en clair. Si la résolution DNS échoue, l'adresse reste non résolue et Secure Client ne tente pas de résoudre l'adresse en dehors du VPN.

Pour activer la tunnellisation fractionnée, choisissez **No** (Non) (valeur par défaut). Ce paramètre indique au client d'envoyer des requêtes DNS sur le tunnel conformément à la politique de tunnellisation fractionnée.

Étape 6 Pour configurer la tunnellisation fractionnée, décochez la case **Inherit** (Hériter) et choisissez une politique de tunnellisation fractionnée. Si vous ne décochez pas la case **Inherit** (Hériter), votre stratégie de groupe utilise les paramètres de tunnellisation fractionnée définis dans la stratégie de groupe par défaut, **DfltGrpPolicy**. Le paramètre de politique de tunnellisation fractionnée par défaut dans la stratégie de groupe par défaut est Tunnel All Networks (Tunneliser tous les réseaux).

Pour définir la politique de tunnellisation fractionnée, choisissez dans les listes déroulantes **Policy** (Politique) et **IPv6 Policy** (Politique IPv6). Le champ Policy (Politique) définit la politique de tunnellisation fractionnée pour le trafic réseau IPv4. Le champ IPv6 Policy (Politique IPv6) sélectionne la politique de tunnellisation fractionnée pour le trafic réseau IPv6. À part cette différence, ces champs ont le même objet.

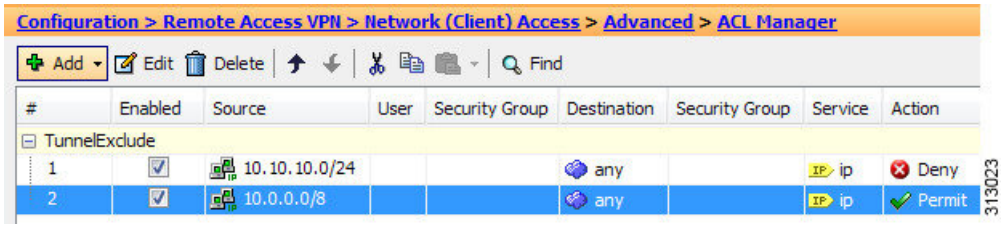
Décochez la case **Inherit** (Hériter) pour choisir l'une de ces options de politique :

- **Exclude Network List Below** (Exclure la liste de réseaux ci-dessous) : définit une liste de réseaux vers lesquels le trafic est envoyé en clair. Cette fonctionnalité est utile pour les utilisateurs distants qui souhaitent accéder aux périphériques de leur réseau local, tels que les imprimantes, lorsqu'ils sont connectés au réseau d'entreprise par l'intermédiaire d'un tunnel.
- **Tunnel Network List Below** (Tunneliser la liste de réseaux ci-dessous) : tunnelise tout le trafic en provenance ou à destination des réseaux spécifiés dans Network List (Liste de réseaux). Le trafic vers les adresses dans la liste d'inclusion des réseaux est tunnelisé. Les données de toutes les autres adresses cheminent en clair et sont acheminées par le fournisseur de services Internet de l'utilisateur distant.

  Pour les versions d'ASA 9.1.4 et supérieures, lorsque vous spécifiez une liste d'inclusion, vous pouvez également spécifier une liste d'exclusion qui est un sous-réseau dans la plage d'inclusion. Ces sous-réseaux

exclus ne sont pas tunnellisés, comme le reste des réseaux de la liste d'inclusion le sont. Les réseaux dans la liste d'exclusion qui ne sont pas un sous-ensemble de la liste d'inclusion sont ignorés par le client. Pour Linux, vous devez ajouter un attribut personnalisé à la stratégie de groupe pour prendre en charge les sous-réseaux exclus.

Par exemple :



Remarque
Si le réseau d'inclusion fractionnée est une correspondance exacte d'un sous-réseau local (comme 192.168.1.0/24), le trafic correspondant est tunnelisé. Si le réseau d'inclusion fractionnée est un surensemble d'un sous-réseau local (comme 192.168.0.0/16), le trafic correspondant, à l'exception du trafic du sous-réseau local, est tunnellisé. Pour tunnelliser également le trafic du sous-réseau local, vous devez ajouter un réseau fractionné (inclure) correspondant (préciser à la fois 192.168.1.0/24 et 192.168.0.0/16 comme réseaux fractionnés inclure).

Si le réseau d'inclusion fractionnée n'est pas valide, comme 0.0.0.0/0.0.0.0, la tunnellisation fractionnée est désactivée (tout est tunnelisé).

- **Tunnel All Networks** (Tunneliser tous les réseaux) : cette politique spécifie que tout le trafic est tunnelisé. Cela désactive en effet la tunnellisation fractionnée. Les utilisateurs distants accèdent aux réseaux Internet par l'intermédiaire du réseau de l'entreprise et n'ont pas accès aux réseaux locaux. Il s'agit de l'option par défaut.

Étape 7 Dans le champ **Network List** (Liste de réseaux), choisissez la liste de contrôle d'accès pour la politique de tunnellisation fractionnée. Si la case Inherit (Hériter) est cochée, la stratégie de groupe utilise la liste de réseaux spécifiée dans la stratégie de groupe par défaut.

Sélectionnez le bouton de commande **Manage** (Gérer) pour ouvrir la boîte de dialogue ACL Manager (Gestionnaire d'ACL), dans laquelle vous pouvez configurer les listes de contrôle d'accès à utiliser comme listes de réseaux. Pour plus d'informations sur la création ou la modification d'une liste de réseaux, consultez le guide de configuration sur les opérations générales.

Les listes d'ACL étendues peuvent contenir des adresses IPv4 et IPv6.

Étape 8 Le **Intercept DHCP Configuration Message** (Message de configuration DHCP Intercept) des clients Microsoft révèle des paramètres supplémentaires spécifiques à DHCP Intercept. DHCP Intercept (Interception DHCP) permet aux clients Microsoft XP d'utiliser la tunnellisation fractionnée avec l'ASA.

- Intercept (Interception) : spécifie s'il faut autoriser l'interception DHCP. Si vous ne choisissez pas Inherit (Hériter), le paramètre par défaut est No (Non).
- Subnet Mask (Masque de sous-réseau) : sélectionne le masque de sous-réseau à utiliser.

Étape 9 Cliquez sur **OK**.

Configurer la tunnellisation fractionnée dynamique

Avec la tunnellisation fractionnée dynamique, vous pouvez provisionner dynamiquement des exclusions de tunnellisation fractionnée après l'établissement du tunnel, en fonction du nom de domaine DNS de l'hôte La tunnellisation 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 tunnellisation fractionnée dynamique pour obtenir plus d'explications.

Procédure

Étape 1 Accédez à l'écran **Configuration > Remote Access VPN (VPN d'accès distant) > Network (Client) Access (Accès réseau [client]) > Advanced (Avancé)** > Secure Client**Custom Attributes (Attributs personnalisés)**.

Étape 2 Cliquez sur **Add** (Ajouter), saisissez `dynamic-split-exclude-domains` comme type d'attribut, puis saisissez une description.

Étape 3 Après avoir cliqué pour appliquer ce nouvel attribut, cliquez sur le lien **Secure ClientCustom Attribute Names** (Noms d'attributs personnalisés) en haut de l'écran de l'interface utilisateur.

Étape 4 Ajoutez les noms d'attributs personnalisés correspondants pour chaque service en nuage ou Web qui doit être accessible par le client depuis l'extérieur du tunnel VPN. Par exemple, ajoutez Google_domains pour représenter une liste de noms de domaine DNS relatifs aux services Web de Google. Définissez ces domaines dans la partie Value (Valeur) de l'écran Secure Client Custom Attribute Names (Noms d'attributs personnalisés), en utilisant le format de valeurs séparées par des virgules (CSV), qui sépare les domaines par une virgule. Secure Client ne prend en compte que les 20 000 premiers caractères, à l'exception des caractères de séparation (environ 300 noms de domaine de taille typique). Les noms de domaine au-delà de cette limite sont ignorés.

Un attribut personnalisé ne peut pas dépasser 421 caractères. Si une valeur plus élevée est saisie, aSDM la divise en plusieurs valeurs limitées à 421 caractères. Toutes les valeurs d'un type et d'un nom d'attribut sont concaténées par l'ASA lorsque la configuration est transmise au client.

Étape 5 Associez les attributs de tunnellisation d'exclusion fractionnée dynamique à une stratégie de groupe donnée en accédant à **Configuration > Remote Access VPN > Network (Client) Access > Group Policies (Configuration > VPN d'accès à distance > Accès au réseau (client) > Stratégies de groupe)**.

Étape 6 Vous pouvez soit créer une nouvelle stratégie de groupe, soit cliquer sur **Edit** (Modifier) pour gérer une stratégie de groupe existante.

Prochaine étape

Si la tunnellisation 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 tunnellisation.

Configurer la tunnellisation d'exclusion fractionnée dynamique

Suivez ces étapes de configuration pour activer la tunnellisation d'exclusion fractionnée dynamique à l'aide d'ASDM. Lorsque les domaines d'exclusion et d'inclusion dynamiques sont définis, la tunnellisation d'exclusion dynamique améliorée avec le nom de domaine correspondant est activée. Par exemple, un administrateur pourrait configurer tout le trafic vers example.com pour être exclu, sauf www.example.com. *Exemple.com* est le domaine d'exclusion dynamique et *www.example.com* est le domaine d'inclusion dynamique.

Remarque Vous devez avoir AnyConnect version 4.5 (ou ultérieure) pour utiliser la tunnellisation d'exclusion fractionnée dynamique. En outre, la version 4.6 d'AnyConnect (et les versions ultérieures) a ajouté un raffinement pour l'inclusion et l'exclusion fractionnées dynamiques améliorées lorsque les domaines pour les deux sont configurés. L'exclusion fractionnée dynamique s'applique à toutes les configurations Tunnel All Networks, d'exclusion fractionnée et d'inclusion fractionnée.

Avant de commencer

Reportez-vous à la section *Tunnellisation fractionnée dynamique* pour connaître les exigences Secure Client.

Procédure

Étape 1 Accédez à l'écran **Configuration > Remote Access VPN > Network (Client) Access > Advanced >** Secure Client**Custom Attributes (Configuration > VPN d'accès à distance > Accès au réseau (client) > Avancé > Attributs personnalisés)**.

Étape 2 Cliquez sur **Add** (Ajouter), saisissez `dynamic-split-exclude-domains` comme type d'attribut, puis saisissez une description.

Étape 3 Après avoir cliqué pour appliquer ce nouvel attribut, cliquez sur le lien **Secure ClientCustom Attribute Names** (Noms d'attributs personnalisés) en haut de l'écran de l'interface utilisateur.

Étape 4 Ajoutez les noms d'attributs personnalisés correspondants pour chaque service en nuage ou Web qui doit être accessible par le client depuis l'extérieur du tunnel VPN. Par exemple, ajoutez Google_domains pour représenter une liste de noms de domaine DNS relatifs aux services Web de Google. Définissez ces domaines dans la partie Value (Valeur) de l'écran Secure Client Custom Attribute Names (Noms d'attributs personnalisés), en utilisant le format de valeurs séparées par des virgules (CSV), qui sépare les domaines par une virgule. Secure Client ne prend en compte que les 5 000 premiers caractères, à l'exception des caractères de séparation (environ 300 noms de domaine de taille typique). Les noms de domaine au-delà de cette limite sont ignorés.

Un attribut personnalisé ne peut pas dépasser 421 caractères. Si une valeur plus élevée est saisie, aSDM la divise en plusieurs valeurs limitées à 421 caractères. Toutes les valeurs d'un type et d'un nom d'attribut sont concaténées par l'ASA lorsque la configuration est transmise au client.

Étape 5 Associez les attributs de tunnellisation d'exclusion fractionnée dynamique à une stratégie de groupe donnée en accédant à **Configuration > Remote Access VPN > Network (Client) Access > Group Policies (Configuration > VPN d'accès à distance > Accès au réseau (client) > Stratégies de groupe)**.

Étape 6 Vous pouvez soit créer une nouvelle stratégie de groupe, soit cliquer sur **Edit** (Modifier) pour gérer une stratégie de groupe existante.

Étape 7 Dans le menu de gauche, cliquez sur **Advanced >** Secure Client **> Custom Attributes** (Avancé > Attributs personnalisés) et choisissez votre type d'attribut dans la liste déroulante.

Configurer la tunnellisation fractionnée dynamique

Suivez ces étapes de configuration pour activer la tunnellisation fractionnée dynamique à l'aide d'ASDM. Lorsque les domaines d'exclusion et d'inclusion dynamiques sont définis, la tunnellisation d'inclusion dynamique améliorée avec le nom de domaine correspondant est activée. Par exemple, un administrateur peut configurer tout le trafic vers domain.com pour qu'il soit inclus, à l'exception de www.domain.com. *Domain.com* est le domaine d'inclusion dynamique et *www.domain.com* est le domaine d'exclusion dynamique.

Remarque Vous devez avoir AnyConnect version 4.6 (ou ultérieure) pour utiliser la tunnellisation d'inclusion fractionnée dynamique. En outre, la version 4.6 d'AnyConnect (et les versions ultérieures) a ajouté un raffinement pour l'inclusion et l'exclusion fractionnées dynamiques améliorées lorsque les domaines pour les deux sont configurés. L'inclusion dynamique de fractionnement s'applique uniquement à la configuration d'inclusion fractionnée.

Avant de commencer

Reportez-vous à la section *Tunnellisation fractionnée dynamique* pour connaître les exigences Secure Client.

Procédure

Étape 1 Accédez à l'écran **Configuration > Remote Access VPN (VPN d'accès distant) > Network (Client) Access (Accès réseau [client]) > Advanced (Avancé)** > Secure Client**Custom Attributes (Attributs personnalisés)**.

Étape 2 Cliquez sur **Add** (Ajouter) et saisissez `dynamic-split-include-domains` comme type d'attribut, puis saisissez une description.

Étape 3 Après avoir cliqué pour appliquer ce nouvel attribut, cliquez sur le lien **Secure ClientCustom Attribute Names** (Noms d'attributs personnalisés) en haut de l'écran de l'interface utilisateur.

Étape 4 Ajoutez les noms d'attributs personnalisés correspondants pour chaque service en nuage ou Web qui doit être accessible par le client depuis l'extérieur du tunnel VPN. Par exemple, ajoutez Google_domains pour représenter une liste de noms de domaine DNS relatifs aux services Web de Google. Définissez ces domaines dans la partie Value (Valeur) de l'écran Secure Client Custom Attribute Names (Noms d'attributs personnalisés), en utilisant le format de valeurs séparées par des virgules (CSV), qui sépare les domaines par une virgule. Secure Client ne prend en compte que les 5 000 premiers caractères, à l'exception des caractères de séparation (environ 300 noms de domaine de taille typique). Les noms de domaine au-delà de cette limite sont ignorés.

Un attribut personnalisé ne peut pas dépasser 421 caractères. Si une valeur plus élevée est saisie, aSDM la divise en plusieurs valeurs limitées à 421 caractères. Toutes les valeurs d'un type et d'un nom d'attribut sont concaténées par l'ASA lorsque la configuration est transmise au client.

Étape 5 Associez les attributs de tunnellisation fractionnée et incluse dynamique à une stratégie de groupe donnée en accédant à **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** (Configuration> VPN d'accès à distance> Accès au réseau (client)> Stratégies de groupe).

Étape 6 Vous pouvez soit créer une nouvelle stratégie de groupe, soit cliquer sur **Edit** (Modifier) pour gérer une stratégie de groupe existante.

Étape 7 Dans le menu de gauche, cliquez sur **Advanced (Avancé) >** Secure Client**Custom Attributes** (Attributs personnalisés) et choisissez votre type d'attribut dans la liste déroulante.

Configurer le 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 appareils rarement connectés par l'utilisateur, via le VPN, au réseau d'entreprise. Les scripts de connexion du système d'exploitation des terminaux qui nécessitent une connectivité au réseau d'entreprise en bénéficient 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. Reportez-vous au Guide d'administration du Secure Client de Cisco 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 Vous devez configurer la méthode d'authentification du groupe de tunnels sur « certificate only » en accédant à **(Configuration)** > **Remote Access VPN (VPN d'accès distant) > Network (Client) Access (Accès réseau [client]) >** Secure Client**Connection Profiles (Profils de connexion) > Add/Edit** (Ajouter/Modifier), puis en la sélectionnant dans la liste déroulante Method (Méthode) sous Authentication (Authentification).

Étape 2 Ensuite, à partir de cette même fenêtre, choisissez **Advanced (Avancé) > Group Alias/Group URL** (Alias de groupe/URL de groupe) et ajoutez l'URL de groupe à spécifier dans le profil VPN de gestion.

Étape 3 La stratégie de groupe de ce groupe de tunnels doit avoir la tunnellisation fractionnée d'inclusion configurée pour tous les protocoles IP disposant d'un ensemble d'adresses configuré dans le groupe de tunnels : choisissez Tunnel Network List Below (Liste des réseaux de tunnels ci-dessous) dans **Remote Access VPN (VPN d'accès distant)** > **Network (Client) Access (Accès réseau [client]) > Group Policies (Stratégies de groupe) > Edit (Modifier) > Advanced (Avancé) > Split Tunneling (Tunnellisation fractionnée)**.

Étape 4 (Facultatif) Le tunnel VPN de gestion nécessite une configuration de tunnellisation fractionnée, par défaut, pour éviter d'avoir une incidence sur la communication réseau initiée par l'utilisateur (car elle est destinée à être transparente). Vous pouvez remplacer ce comportement en configurant l'attribut personnalisé dans la stratégie de groupe utilisée par la connexion du tunnel de gestion : Attributs personnalisés Secure Client , à la page 165.
Si aucun ensemble d'adresses n'est configuré dans le groupe de tunnels pour les deux protocoles IP, vous devez activer *Client Bypass Protocol* (Protocole de contournement client) dans la stratégie de groupe afin que le trafic correspondant au protocole IP sans ensemble d'adresses ne soit pas interrompu par le tunnel VPN de gestion.

Étape 5 Créez le profil et choisissez le tunnel VPN de gestion pour l'utilisation du profil : Configurer les profils Secure Client, à la page 148.

Configurer Linux pour prendre en charge les sous-réseaux exclus

Lorsque **Tunnel Network List Below** (Liste de réseaux tunnel ci-dessous) est configuré pour la tunnellisation fractionnée, Linux nécessite une configuration supplémentaire pour prendre en charge les sous-réseaux exclus. Vous devez créer un attribut personnalisé nommé circumvent-host-filtering, le définir sur true et l'associer à la stratégie de groupe configurée pour la tunnellisation fractionnée.

Procédure

Étape 1 Connectez-vous à l'ASDM et accédez à **Configuration** > **Remote Access VPN (VPN d'accès à distance) >** > **Network (Client) Access** > **(Accès réseau [client]) >** > **Advanced** (Avancé) > **Custom Attributes (Attributs personnalisés)** Secure Client**.**

Étape 2 Cliquez sur **Add** (Ajouter), créez un attribut personnalisé nommé **circumvent-host-filtering** et définissez la valeur sur **true**.

Étape 3 Modifiez la stratégie de groupe que vous prévoyez utiliser pour le pare-feu client et accédez à **Advanced** > **(Avancé) >** > **Custom Attributes** > **(Attributs personnalisés)** > .

Étape 4 Ajoutez l'attribut personnalisé que vous avez créé, **circumvent-host-filtering**, à la stratégie de groupe que vous utiliserez pour la tunnellisation fractionnée.

Stratégies de groupe internes, Attributs Secure Client

Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Group Policies (Stratégies de groupe) > Add/Edit (Ajouter/Modifier) > Advanced (Avancé) Secure Client> contient des attributs configurables pour Secure Client dans cette stratégie de groupe.

- Conserver le programme d'installation sur le système client — activez l'installation permanente du client sur l'ordinateur distant. L'activation désactive la fonction de désinstallation automatique du client. Le client reste installé sur l'ordinateur distant pour les connexions ultérieures, réduisant ainsi le temps de connexion pour l'utilisateur distant.

Remarque Laisser le programme d'installation sur le système client n'est pas pris en charge après la version 2.5 de Secure Client.

- Datagram Transport Layer Security (DTLS) (Sécurité de couche de transport datagramme [DTLS]) : évite les problèmes de latence et de bande passante associés à certaines connexions SSL et améliore les performances des applications en temps réel sensibles aux retards de paquets.
- DTLS Compression (Compression DTLS) : configure la compression pour DTLS.
- SSL Compression (Compression SSL) : configure la compression pour SSL/TLS.
- Ignore Don't Defrag (DF) Bit (Ignorer le bit Don't Defrag [DF]) : cette fonctionnalité permet la fragmentation forcée des paquets dont le bit DF est activé, leur permettant de passer par le tunnel. Un exemple de cas d'utilisation concerne les serveurs de votre réseau qui ne répondent pas correctement aux négociations TCP MSS.

- Client Bypass Protocol (Protocole de contournement client) : configure la façon dont Secure Client gère le trafic IPv4 lorsque l'ASA s'attend uniquement à du trafic IPv6, ou la façon dont il gère le trafic IPv6 lorsqu'il s'attend uniquement à du trafic IPv4.

  Lorsque Secure Client établit une connexion VPN avec l'ASA, celui-ci peut lui affecter une adresse IPv4, IPv6 ou à la fois une adresse IPv4 et IPv6. Client Bypass Protocol (Protocole de contournement client) détermine s'il faut abandonner le trafic pour lequel l'ASA n'a pas affecté d'adresse IP ou autoriser ce trafic à contourner l'ASA et à être envoyé par le client non chiffré ou « en clair ».

  Par exemple, supposons que l'ASA attribue uniquement une adresse IPv4 à une connexion Secure Client et que le terminal soit à 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.

- FQDN of This Device (Nom de domaine complet de ce périphérique) : ces informations sont utilisées par le client après l'itinérance réseau afin de résoudre l'adresse IP ASA utilisée pour rétablir la session VPN. Ce paramètre est essentiel pour prendre en charge l'itinérance entre des réseaux utilisant différents protocoles IP (comme IPv4 et IPv6).

Remarque Vous ne pouvez pas utiliser le FQDN ASA présent dans le profil Secure Client pour dériver l'adresse IP ASA après l'itinérance. Les adresses peuvent ne pas correspondre au bon périphérique (celui vers lequel le tunnel a été établi) dans le scénario d'équilibrage de charge.

  Si le FQDN du périphérique n'est pas transmis au client, le client tente de se reconnecter à l'adresse IP précédemment établie par le tunnel. Afin de prendre en charge l'itinérance entre des réseaux utilisant différents protocoles IP (d'IPv4 à IPv6), Secure Client 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 FQDN ASA présent dans son profil lors de la connexion initiale. Lors des reconnexions de session ultérieures, il utilise toujours le FQDN du périphérique transmis par l'ASA (et configuré par l'administrateur dans la stratégie de groupe), lorsqu'il est disponible. Si le FQDN n'est pas configuré, l'ASA dérive le FQDN du périphérique (et l'envoie au client) à partir de ce qui est défini sous 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.

- MTU : ajuste la taille MTU pour les connexions SSL. Saisissez une valeur en octets, comprise entre 256 et 1 410 octets. Par défaut, la taille MTU est ajustée automatiquement en fonction de la MTU de l'interface utilisée par la connexion, moins la surcharge IP/UDP/DTLS.

- Keepalive Messages (Messages Keepalive) : saisissez une valeur comprise entre 15 et 600 secondes dans le champ Interval (Intervalle) afin d'activer et d'ajuster l'intervalle des messages Keepalive pour garantir qu'une connexion par l'intermédiaire d'un serveur proxy, d'un pare-feu ou d'un périphérique NAT reste ouverte, même si le périphérique limite la durée d'inactivité de la connexion. L'ajustement de l'intervalle garantit également que le client 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.

- Optional Client Modules to Download (Modules client facultatifs à télécharger) : pour réduire le temps de téléchargement, Secure Client demande uniquement les téléchargements (à partir de l'ASA) des

modules dont il a besoin pour chaque fonctionnalité prise en charge. Vous devez préciser les noms des modules qui activent d'autres fonctionnalités. Secure Client, version 4.0, comprend les modules suivants (les versions précédentes comportent moins de modules) :

- Secure ClientDART : Diagnostic Reporting Tool (DART) (outil de rapport de diagnostic [DART]) Secure Client capture un instantané des journaux système et d'autres renseignements diagnostiques et crée un fichier .zip sur votre bureau afin que vous puissiez facilement envoyer des renseignements de dépannage au centre d'assistance technique Cisco.
- Secure Client Network Access Manager (Gestionnaire d'accès réseau) : anciennement appelé Cisco Secure Services Client, ce module fournit la norme 802.1X (couche 2) et l'authentification des périphériques pour l'accès aux réseaux câblés et sans fil.
- Secure Client SBL—Start Before Logon (SBL) (Démarrer avant la connexion [SBL]) : force l'utilisateur à se connecter à l'infrastructure de l'entreprise par l'intermédiaire d'une connexion VPN avant de se connecter à Windows en démarrant Secure Client avant l'affichage de la boîte de dialogue de connexion Windows.
- Secure Client Web Security Module (Module de sécurité Web) : anciennement appelé ScanSafe Hostscan, ce module est intégré dans Secure Client. Il déconstruit les éléments d'une page Web afin de pouvoir analyser chaque élément simultanément. Il peut ensuite autoriser le contenu acceptable et bloquer le contenu malveillant ou inacceptable en fonction d'une politique de sécurité définie.
- Secure Client Telemetry Module (Module de télémétrie) : envoie des renseignements sur l'origine du contenu malveillant à l'infrastructure de filtrage Web de l'appliance Cisco IronPort Web Security Appliance (WSA), qui utilise ces données pour fournir de meilleures règles de filtrage d'URL.

Remarque La télémétrie n'est pas prise en charge par AnyConnect 4.0.

- ASA Posture Module (Module de posture ASA) : anciennement appelé fonctionnalité Cisco Secure Desktop HostScan, le module de posture est intégré dans Secure Client et permet Secure Client de recueillir des renseignements d'authentification pour l'évaluation de la posture avant de créer une connexion d'accès à distance avec l'ASA.
- ISE Posture (Posture ISE) : utilise la bibliothèque OPSWAT v3 pour effectuer des vérifications de posture afin d'évaluer la conformité d'un terminal. Vous pouvez ensuite restreindre l'accès réseau jusqu'à ce que le terminal soit conforme ou élever les privilèges de l'utilisateur local.
- AMP Enabler (Facilitateur AMP) : utilisé comme moyen de déployer Advanced Malware Protection (AMP) pour les terminaux. Il pousse le logiciel AMP for Endpoints vers un sous-ensemble de terminaux à partir d'un serveur hébergé localement dans l'entreprise et installe les services AMP auprès de sa base d'utilisateurs existante.
- Network Visibility Module (Module de visibilité du réseau) : améliore la capacité de l'administrateur d'entreprise à effectuer la planification de capacité et des services, l'audit, la conformité et l'analyse de sécurité. NVM recueille les données de télémétrie du terminal et consigne les données de flux et la réputation de fichier dans le journal système et exporte également les enregistrements de flux vers un collecteur (un prestataire tiers), qui effectue l'analyse des fichiers et fournit une interface utilisateur.
- Umbrella Roaming Security Module (Module de sécurité d'itinérance Umbrella) : fournit une sécurité de couche DNS lorsqu'aucun VPN n'est actif. Il fournit un abonnement soit au service Cisco Umbrella Roaming soit aux services OpenDNS Umbrella, qui ajoutent des fonctionnalités Intelligent

Proxy et IP-Layer Enforcement. Le profil Umbrella Security Roaming associe chaque déploiement au service correspondant et active automatiquement le niveau de protection correspondant (filtrage de contenu, politiques multiples, rapports robustes, intégration Active Directory ou sécurité de base de couche DNS).

- Always-On VPN (VPN permanent) : déterminez si le paramètre d'indicateur VPN permanent dans le profil de service Secure Client est désactivé ou si le paramètre du profil de service Secure Client doit être utilisé. La fonctionnalité VPN permanent permet à AnyConnect d'établir automatiquement une session VPN après l'ouverture de session de l'utilisateur sur un ordinateur. La session VPN reste active jusqu'à la fermeture de session de l'utilisateur sur l'ordinateur. Si la connexion physique est perdue, la session reste active et Secure Client tente continuellement de rétablir la connexion physique avec l'appareil de sécurité adaptatif afin de reprendre la session VPN.

  Le VPN permanent permet d'appliquer les politiques d'entreprise afin de protéger le périphérique contre les menaces de sécurité. Vous pouvez l'utiliser pour vous assurer que Secure Client établit une session VPN chaque fois que le terminal ne se trouve pas dans un réseau de confiance. Si elle est activée, une politique est configurée pour déterminer comment la connectivité réseau est gérée en l'absence de connexion.

Remarque Le VPN permanent nécessite une version Secure Client qui prend en charge les fonctionnalités Secure Client .

- Client Profiles to Download (Profils client à télécharger) : un profil est un groupe de paramètres de configuration que Secure Client utilise pour configurer les paramètres VPN, Network Access Manager (Gestionnaire d'accès réseau), Web Security (Sécurité Web), ISE Posture (Posture ISE), AMP Enabler (Facilitateur AMP), Network Visibility Module (Module de visibilité du réseau) et Umbrella Roaming Security Module (Module de sécurité d'itinérance Umbrella). Cliquez sur **Add** (Ajouter) pour lancer la fenêtre Select Profiles (Sélectionner les profils) Secure Client, dans laquelle vous pouvez spécifier les profils créés précédemment pour cette stratégie de groupe.

Stratégies de groupe internes, paramètres de connexion Secure Client

Dans le volet **Advanced >** Secure Client **> Login Setting** de la stratégie de groupe interne vous pouvez activer l'ASA pour inviter les utilisateurs distants à télécharger Secure Client, ou à diriger la connexion vers une page de portail VPN SSL sans client.

- Post Login Setting (Paramètre après connexion) : choisissez d'inviter l'utilisateur et de définir le délai d'expiration pour effectuer la sélection par défaut après la connexion.
- Default Post Login Selection (Sélection après connexion par défaut) : choisissez une action à effectuer après la connexion.

Utilisation du pare-feu client pour activer la prise en charge des périphériques locaux pour le VPN

Dans le volet **Advanced (Avancé) > Secure Client > Client Firewall** (Pare-feu client) de la stratégie de groupe interne, vous pouvez configurer des règles à envoyer au pare-feu du système client qui affectent la façon dont les réseaux publics et privés sont gérés par le client.

Lorsque les utilisateurs distants se connectent à l'ASA, tout le trafic est tunnelisé par la connexion VPN, de sorte que les utilisateurs ne peuvent pas accéder aux ressources sur leur réseau local. Cela inclut les imprimantes, les appareils photo et les périphériques Windows Mobile (périphériques utilisant la fonctionnalité de connexion) qui se synchronisent avec l'ordinateur local. L'activation de l'accès LAN local dans le profil client résout ce problème, mais elle peut présenter un problème de sécurité ou de politique pour certaines entreprises en raison d'un accès non restreint au réseau local. Vous pouvez configurer l'ASA pour déployer des règles de pare-feu du système d'exploitation du terminal qui restreignent l'accès à des types particuliers de ressources locales, telles que les imprimantes et les périphériques utilisant la fonctionnalité de connexion.

Pour ce faire, activez les règles de pare-feu client pour des ports spécifiques pour l'impression. Le client fait la distinction entre les règles de trafic entrant et sortant. Pour les capacités d'impression, le client ouvre les ports requis pour les connexions sortantes, mais bloque tout le trafic entrant.

Remarque Sachez que les utilisateurs connectés en tant qu'administrateurs ont la possibilité de modifier les règles de pare-feu déployées sur le client par l'ASA. Les utilisateurs dont les privilèges sont limités ne peuvent pas modifier les règles. Pour l'un ou l'autre des utilisateurs, le client réapplique les règles de pare-feu à la fin de la connexion.

Si vous configurez le pare-feu client et que l'utilisateur s'authentifie auprès d'un serveur Active Directory (AD), le client applique toujours les politiques de pare-feu de l'ASA. Cependant, les règles définies dans les stratégies de groupe AD prévalent sur les règles du pare-feu client.

Lorsque les règles de pare-feu client sont configurées sur l'ASA et que la connexion VPN est établie sur le terminal,

- L'ASA envoie les informations des règles de pare-feu au client.
- Le client appliquera ensuite les règles de pare-feu au besoin.

Les sections suivantes décrivent la marche à suivre :

- Déploiement d'un pare-feu client pour la prise en charge des périphériques locaux, à la page 89
- Configurer la prise en charge des périphériques connectés pour le VPN, à la page 91

Remarques d'utilisation relatives au comportement du pare-feu

Les notes suivantes précisent comment Secure Client utilise le pare-feu :

- L'adresse IP source n'est pas utilisée pour les règles de pare-feu. Le client ignore les informations d'adresse IP source dans les règles de pare-feu envoyées par l'ASA. Le client détermine l'adresse IP source selon que les règles sont publiques ou privées. Les règles publiques sont appliquées à toutes les interfaces du client. Les règles privées sont appliquées à l'adaptateur virtuel.
- L'ASA prend en charge de nombreux protocoles pour les règles d'ACL. Cependant, la fonctionnalité de pare-feu Secure Client ne prend en charge que les protocoles TCP, UDP, ICMP et IP. Si le client reçoit une règle avec un protocole différent, il la traite comme une règle de pare-feu non valide, puis désactive la tunnelisation fractionnée et utilise la tunnelisation complète pour des raisons de sécurité.
- À partir d'ASA 9.0, Public Network Rule (Règle de réseau public) et Private Network Rule (Règle de réseau privé) prennent en charge les listes de contrôle d'accès unifiées. Ces listes de contrôle d'accès peuvent être utilisées pour définir le trafic IPv4 et IPv6 dans la même règle.

Gardez à l'esprit les différences de comportement suivantes pour chaque système d'exploitation :

- Pour les ordinateurs Windows, les règles de refus prévalent sur les règles d'autorisation dans le pare-feu Windows. Si l'ASA applique une règle d'autorisation au client Secure Client, mais que l'utilisateur a créé une règle de refus personnalisée, la règSecure Client n'est pas appliquée.
- Sous Windows Vista, lors de la création d'une règle de pare-feu, Vista prend la plage de numéros de port sous forme d'une chaîne séparée par des virgules. La plage de ports peut aller jusqu'à 300 ports. Par exemple, de 1 à 300 ou de 5 000 à 5 300. Si vous spécifiez une plage supérieure à 300 ports, la règle de pare-feu s'applique uniquement aux 300 premiers ports.
- Les utilisateurs de Windows dont le service de pare-feu doit être démarré par le client Secure Client (et non démarré automatiquement par le système) peuvent connaître une augmentation sensible du temps nécessaire pour établir une connexion VPN.
- Sur les ordinateurs Mac, le client Secure Client applique les règles de manière séquentielle dans le même ordre que l'ASA les applique. Les règles globales doivent toujours être en dernier.
- Pour les pare-feu tiers, le trafic est transmis uniquement si le pare-feu Secure Client et le pare-feu tiers autorisent ce type de trafic. Si le pare-feu tiers bloque un type de trafic spécifique que le client Secure Client autorise, le client bloque le trafic.

Déploiement d'un pare-feu client pour la prise en charge des périphériques locaux

L'ASA prend en charge la fonctionnalité de pare-feu Secure Client avec l'ASA version 8.3(1) ou ultérieure, et la version 6.3(1) ou ultérieure d'ASDM. Cette section décrit comment configurer le pare-feu client pour autoriser l'accès aux imprimantes locales et comment configurer le profil client pour utiliser le pare-feu en cas d'échec de la connexion VPN.

Limites et restrictions du pare-feu client

Les limites et restrictions suivantes s'appliquent à l'utilisation du pare-feu client pour restreindre l'accès au réseau local (LAN) local :

- La règle privée *deny ip any any* n'est pas autorisée.
- En raison des limites du système d'exploitation, la politique de pare-feu client sur les ordinateurs exécutant Windows XP est appliquée pour le trafic entrant uniquement. Les règles sortantes et les règles bidirectionnelles sont ignorées. Cela inclura les règles de pare-feu telles que « permit ip any any ».
- HostScan (maintenant nommé Secure Firewall Posture) et certains pare-feu tiers peuvent interférer avec le pare-feu.

Le tableau suivant précise quelle direction du trafic est affectée par les paramètres de port source et de destination :

Port source	Port de destination	Direction du trafic
Numéro de port spécifique	Numéro de port spécifique	Entrant et sortant.
Une plage ou « Tout » (valeur de 0)	Une plage ou « Tout » (valeur de 0)	Entrant et sortant
Numéro de port spécifique	Une plage ou « Tout » (valeur de 0)	Entrant seulement

Port source	Port de destination	Direction du trafic
Une plage ou « Tout » (valeur de 0)	Numéro de port spécifique	Sortant uniquement

Exemple de règles d'ACL pour l'impression locale

La liste de contrôle d'accès Secure Client_Local_Print est fournie avec ASDM pour faciliter la configuration du pare-feu client. Lorsque vous choisissez cette liste de contrôle d'accès pour la règle de réseau public dans le volet de pare-feu client d'une stratégie de groupe, cette liste contient les clés de contrôle d'accès suivantes :

.

Tableau 3 : Règles d'ACL dans Secure Client_Local_Print

Description	Autorisation	Interface	Protocole	Port de la source	Adresse de destination	Port de la destination
Tout refuser	Refuser	Public	N'importe lequel	Par défaut	N'importe lequel	Par défaut
LPD	Autoriser	Public	TCP	Par défaut	N'importe lequel	515
IPP	Autoriser	Public	TCP	Par défaut	N'importe lequel	631
Imprimeur	Autoriser	Public	TCP	Par défaut	N'importe lequel	9100
mDNS	Autoriser	Public	UDP	Par défaut	224.0.0.251	5353
LLMNR	Autoriser	Public	UDP	Par défaut	224.0.0.252	5355
NetBIOS	Autoriser	Public	TCP	Par défaut	N'importe lequel	137
NetBIOS	Autoriser	Public	UDP	Par défaut	N'importe lequel	137
Remarque La plage par défaut est de 1 à 65 535.						

Remarque Pour activer l'impression locale, vous devez activer la fonction d'accès au réseau local (LAN) dans le profil client avec une règle ACL définie autoriser Any Any.

Configurer la prise en charge des impressions locales pour le VPN

Pour permettre aux utilisateurs finaux d'imprimer sur leur imprimante locale, créez une liste de contrôle d'accès standard dans la stratégie de groupe. L'ASA envoie cette liste de contrôle d'accès au client VPN, et le client VPN modifie la configuration du pare-feu du client.

Procédure

Étape 1 Activer le pare-feu Secure Client dans une stratégie de groupe. Allez à **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau (client)) > Group Policies (Stratégies de groupe)**.

Étape 2 Sélectionnez une stratégie de groupe et cliquez sur **Edit** (Modifier).

Étape 3 Sélectionnez **Advanced** (Avancé) > **Client Firewall** (Pare-feu client) Secure Client. Cliquez sur **Manage** (Gérer) pour la règle de réseau privé.

Étape 4 Créez une liste de contrôle d'accès contenant les ACE décrites ci-dessus. Ajoutez cette liste de contrôle d'accès en tant que règle de réseau privé.

Étape 5 Si vous avez activé la politique VPN automatique permanente et spécifié une politique fermée, en cas de défaillance du VPN, les utilisateurs n'ont pas accès aux ressources locales. Vous pouvez appliquer les règles de pare-feu dans ce scénario en accédant à **Preferences (Part 2)** (Préférences [partie 2]) dans l'éditeur de profils et en cochant la case **Apply last local VPN resource rules** (Appliquer les dernières règles de ressources VPN locales).

Configurer la prise en charge des périphériques connectés pour le VPN

Pour prendre en charge les périphériques connectés et protéger le réseau d'entreprise, créez une liste de contrôle d'accès standard dans la stratégie de groupe, en précisant les adresses de destination dans la plage utilisée par les périphériques connectés. Précisez ensuite l'ACL pour la tunnellisation fractionnée en tant que liste de réseaux à exclure du trafic VPN tunnelisé. Vous devez également configurer le profil client pour utiliser les dernières règles de ressources VPN locales en cas de défaillance du VPN.

Remarque Pour les périphériques Windows Mobile qui doivent se synchroniser avec l'ordinateur exécutant Secure Client, spécifiez l'adresse de destination IPv4 169.254.0.0 ou l'adresse de destination IPv6 fe80::/64 dans l'ACL.

Procédure

Étape 1 Dans ASDM, accédez à **Group Policy (Stratégie de groupe) > Advanced (Avancé) > Split Tunneling (Tunnellisation fractionnée)**.

Étape 2 Décochez la case **Inherit** (Hériter) à côté du champ Network List (Liste de réseaux) et cliquez sur Manage (Gérer).

Étape 3 Cliquez sur l'onglet **Extended ACL** (Liste de contrôle d'accès étendue).

Étape 4 Cliquez sur **Add (Ajouter) > Add ACL (Ajouter une liste de contrôle d'accès)**. Spécifiez un nom pour la nouvelle liste de contrôle d'accès.

Étape 5 Choisissez la nouvelle liste de contrôle d'accès dans le tableau et cliquez sur **Add** (Ajouter), puis sur **Add ACE** (Ajouter ACE).

Étape 6 Pour **Action**, choisissez le bouton radio **Permit** (Autoriser).

Étape 7 Dans la zone des critères de destination, spécifiez l'adresse de destination IPv4 169.254.0.0 ou l'adresse de destination IPv6 fe80::/64.

Étape 8 Pour **Service**, choisissez IP.

Étape 9 Cliquez sur **OK**.

Étape 10 Cliquez sur **OK** pour enregistrer la liste de contrôle d'accès.

Étape 11 Dans le volet Split Tunneling (Tunnellisation fractionnée) de la stratégie de groupe interne, décochez la case Inherit (Hériter) pour Policy (Politique) ou IPv6 Policy (Politique IPv6), selon l'adresse IP que vous avez spécifiée à l'étape 7, puis choisissez **Exclude Network List Below** (Exclure la liste de réseaux ci-dessous). Pour Network List (Liste de réseaux), choisissez l'ACL que vous avez créée.

Étape 12 Cliquez sur **OK**.

Étape 13 Cliquez sur **Apply** (Appliquer).

Stratégies de groupe internes, régénération de clé Secure Client

La négociation de renouvellement a lieu lorsque l'ASA et le client effectuent un renouvellement et renégocient les clés de chiffrement et les vecteurs d'initialisation, augmentant ainsi la sécurité de la connexion.

Dans le volet **Advanced (Avancé) > Secure Client > Key Regeneration (Régénération de clé)** de la stratégie de groupe interne, vous configurez les paramètres de renouvellement :

- Intervalle de renégociation : décochez la case **Unlimited** (Illimité) pour préciser le nombre de minutes entre le début de la session et le renouvellement, de 1 à 10 080 (1 semaine).
- Méthode de renégociation : décochez la case Inherit (Hériter) pour spécifier une méthode de renégociation différente de la stratégie de groupe par défaut. Sélectionnez le bouton radio **None** (Aucun) pour désactiver le renouvellement, choisissez le bouton radio **SSL** ou **New Tunnel** (Nouveau tunnel) pour établir un nouveau tunnel pendant le renouvellement.

Remarque Configurer la méthode de renégociation comme **SSL** ou **New Tunnel** (Nouveau 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**.

Stratégie de groupe interne, Secure Client, Détection d'homologue mort

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 Secure Client ou la passerelle ASA exécute la DPD, procédez comme suit :

Avant de commencer

- Cette fonctionnalité s'applique uniquement à la connectivité entre la passerelle ASA et le client SSL VPN Secure Client. Elle 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.

- Accédez à **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau [client]) > Group Policies (Stratégies de groupe)**, puis **Add** (Ajouter) ou **Edit** (Modifier) la stratégie de groupe souhaitée, puis ouvrez le volet **Advanced (Avancé) >** Secure Client **> Dead Peer Detection (Détection d'homologue mort)**.
- Ou, pour accéder à la stratégie d'un utilisateur spécifique, accédez à **Configuration > Device Management (Gestion du périphérique) > Users/AAA (Utilisateurs/AAA) > User Accounts (Comptes d'utilisateurs)**, puis Add (Ajouter) ou Edit (Modifier) le compte d'utilisateur souhaité ; ouvrez ensuite le volet **VPN Policy (Stratégie VPN) >** Secure Client **> Dead Peer Detection (Détection d'homologue mort).**.

Étape 2 Définir la détection côté passerelle.

Décochez la case **Disable** (Désactiver) pour préciser que le DPD est effectué par l'appareil de sécurité (passerelle). Saisissez l'intervalle, de 30 (par défaut) à 3 600 secondes, pendant lequel l'appareil de sécurité effectue DPD. Une valeur de 300 est conseillée.

Étape 3 Définir la détection côté client.

Décochez la case **Disable** (Désactiver) pour préciser que le DPD est effectué par le client. Saisissez ensuite l'intervalle, de 30 (par défaut) à 3 600 secondes, pendant lequel le client effectue DPD. Une valeur de 30 secondes est conseillée.

Stratégies de groupe internes, Personnalisation du portail sans client Secure Client

Dans le volet **Advanced (Avancé) > Secure Client > Customization (Personnalisation)** de la stratégie de groupe interne, vous pouvez personnaliser la page de connexion du portail sans client pour une stratégie de groupe.

- Portal Customization (Personnalisation du portail) : sélectionne la personnalisation à appliquer à la page du portail Secure Client/VPN SSL. Vous pouvez choisir un objet de personnalisation de portail

préconfiguré ou accepter la personnalisation fournie dans la stratégie de groupe par défaut. La valeur par défaut est DfltCustomization.

- Manage (Gérer) : ouvre la boîte de dialogue Configure GUI Customization Objects (Configurer les objets de personnalisation de l'interface graphique), dans laquelle vous pouvez préciser que vous souhaitez ajouter, modifier, supprimer, importer ou exporter un objet de personnalisation.

- Homepage URL (optional) (URL de la page d'accueil (facultatif)) : spécifie une URL de page d'accueil à afficher dans le portail sans client pour les utilisateurs associés à la stratégie de groupe. La chaîne doit commencer par http:// ou https://. Les utilisateurs sans client sont immédiatement dirigés vers cette page après une authentification réussie. Secure Client lance le navigateur Web par défaut sur cette URL lors de l'établissement réussi de la connexion VPN.

Remarque Secure Client ne prend pas actuellement en charge ce champ sur la plateforme Linux, les appareils mobiles Android et les appareils mobiles Apple iOS. S'il est défini, il est ignoré par ces Secure Client.

- Use Smart Tunnel for Homepage (Utiliser le tunnel intelligent pour la page d'accueil) : crée un tunnel intelligent pour se connecter au portail au lieu d'utiliser le transfert de port.
- Access Deny Message (Message de refus d'accès) : pour créer un message à afficher aux utilisateurs auxquels l'accès est refusé, saisissez-le dans ce champ.

Configurer les attributs personnalisés Secure Client dans une stratégie de groupe interne

Le volet **Advanced > Secure Client > Custom Attributes (Avancé > Attributs personnalisés)** de la stratégie de groupe interne répertorie les attributs personnalisés actuellement affectés à cette stratégie. Dans cette boîte de dialogue, vous pouvez associer des attributs personnalisés définis précédemment à cette stratégie, ou définir des attributs personnalisés, puis les associer à cette stratégie.

Les attributs personnalisés sont envoyés à et utilisés par Secure Client pour configurer des fonctionnalités telles que la mise à niveau retardée. Un attribut personnalisé a un type et une valeur nommée. Le type de l'attribut est défini en premier, puis une ou plusieurs valeurs nommées de ce type peuvent être définies. Pour en savoir plus sur les attributs personnalisés à configurer pour une fonctionnalité, consultez le *Guide de l'administrateur de Cisco* pour la version Secure Client que vous utilisez.

Les attributs personnalisés peuvent également être prédéfinis dans **Configuration > Remote Access VPN > Network (Client) Access > Advanced > Secure Client Custom Attributes** and **Secure Client Custom Attribute Names** (Configuration > VPN d'accès à distance > Accès au réseau [client] > Avancé > Attributs personnalisés et Noms d'attributs personnalisés). Les attributs personnalisés prédéfinis sont utilisés par les politiques d'accès dynamique et les stratégies de groupe.

Utilisez cette procédure pour ajouter ou modifier un attribut personnalisé. Vous pouvez également supprimer un attribut personnalisé configuré, mais les attributs personnalisés ne peuvent pas être modifiés ou supprimés s'ils sont également associés à une autre stratégie de groupe.

Procédure

Étape 1 Accédez à **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** > **Add/Edit** > **Advanced** > Secure Client > **Custom Attributes** (Configuration > VPN d'accès à distance > Accès au réseau [client] > Stratégies de groupe > Ajouter/Modifier > Avancé > Attributs personnalisés).

Étape 2 Cliquez sur **Add** (Ajouter) pour ouvrir le volet **Create Custom Attribute** (Créer un attribut personnalisé).

Étape 3 Sélectionnez un **type d'attribut** prédéfini dans la liste déroulante ou configurez le type d'attribut en procédant comme suit :

a) Cliquez sur **Manage** (Gérer), puis, dans le volet **Configure Custom Attribute Types** (Configurer les types d'attributs personnalisés), cliquez sur **Add** (Ajouter).

b) Dans le volet **Create Custom Attribute Type** (Créer un type d'attribut personnalisé), saisissez le nouveau **Type** et la **Description** de l'attribut ; les deux champs sont obligatoires. Pour les options d'attributs personnalisés Secure Client, consultez Attributs personnalisés Secure Client , à la page 165.

c) Cliquez sur **OK** pour fermer ce volet, puis cliquez à nouveau sur **OK** pour choisir le type d'attribut personnalisé nouvellement défini.

Étape 4 Choisissez **Select Value** (Sélectionner une valeur).

Étape 5 Sélectionnez une valeur nommée prédéfinie dans la liste déroulante **Select Value** (Sélectionner une valeur) ou configurez une nouvelle valeur nommée en procédant comme suit :

a) Cliquez sur **Manage** (Gérer), puis, dans le volet Configure Custom Attributes (Configurer les attributs personnalisés), cliquez sur **Add** (Ajouter).

b) Dans le volet **Create Custom Attribute Name** (Créer un nom d'attribut personnalisé), choisissez le **Type** d'attribut que vous avez précédemment sélectionné ou configuré, puis saisissez le **Name** (Nom) et la **Value** (Valeur) de l'attribut ; les deux champs sont obligatoires.

Pour ajouter une valeur, cliquez sur **Add** (Ajouter), saisissez la valeur et cliquez sur **OK**. La valeur ne peut pas dépasser 420 caractères. Si votre valeur dépasse cette longueur, ajoutez plusieurs valeurs pour le contenu de valeur supplémentaire. Les valeurs configurées sont concaténées avant d'être envoyées à Secure Client.

c) Cliquez sur **OK** pour fermer ce volet, puis cliquez à nouveau sur **OK** pour choisir la valeur nommée nouvellement définie de cet attribut.

Étape 6 Cliquez sur **OK** dans le volet **Create Custom Attribute** (Créer un attribut personnalisé).

Stratégies de groupe internes du client IPsec (IKEv1)

Stratégies de groupe internes, attributs généraux pour le client IPsec (IKEv1)

La boîte de dialogue **Configuration > Remote Access > Network (Client) Access > Group Policies > Advanced > IPsec (IKEv1) Client Add or Edit Group Policy > IPsec** (Configuration > Accès à distance > Accès réseau [client] > Stratégies de groupe > Avancé > IPsec [IKEv1] Client Ajouter ou Modifier une Stratégie de groupe > IPsec) vous permet de préciser les protocoles de tunnellisation, les filtres, les paramètres de connexion et les serveurs pour la stratégie de groupe en cours d'ajout ou de modification:

- Re-Authentication on IKE Re-Key (Re-authentification lors du renouvellement IKE) : active ou désactive la réauthentification lorsque le renouvellement IKE se produit, à moins que la case Inherit (Hériter) ne

soit cochée. L'utilisateur a 30 secondes pour saisir les informations d'authentification et jusqu'à trois tentatives avant que la SA n'expire à environ deux minutes et que le tunnel ne se termine.

- Allow entry of authentication credentials until SA expires (Autoriser l'entrée des informations d'authentification jusqu'à l'expiration de la SA) : permet aux utilisateurs de réintroduire les informations d'authentification jusqu'à la durée de vie maximale de la SA configurée.
- IP Compression (Compression IP) : active ou désactive la Compression IP, à moins que la case Inherit (Hériter) ne soit cochée.
- Perfect Forward Secrecy (Confidentialité persistante parfaite) : active ou désactive la confidentialité persistante parfaite (PFS), sauf si la case Inherit (Hériter) est cochée. Le protocole PFS garantit que la clé d'une SA IPsec donnée n'est pas dérivée d'un autre secret (comme certaines autres clés). En d'autres termes, si personne ne parvenait à casser une clé, le protocole PFS garantit que l'agresseur ne pourrait pas obtenir d'autres clés. Si le protocole PFS n'était pas activé, une personne pourrait éventuellement casser la clé secrète IKE SA, copier toutes les données protégées IPsec, puis utiliser la connaissance du secret IKE SA pour compromettre les SA IPsec configurées par cette SA IKE. Avec PFS, la rupture d'IKE ne donnerait pas à un agresseur un accès immédiat à IPsec. L'agresseur devrait casser chaque SA IPsec individuellement.
- Store Password on Client System (Stocker le mot de passe sur le système client) : active ou désactive le stockage du mot de passe sur le système client.

Remarque Le stockage du mot de passe sur un système client peut constituer un risque potentiel pour la sécurité.

- IPsec over UDP (IPsec sur UDP) : active ou désactive l'utilisation d'IPsec sur UDP.
- IPsec over UDP Port (Port IPsec sur UDP) : spécifie le port UDP à utiliser pour IPsec sur UDP.
- Tunnel Group Lock (Verrouillage du groupe de tunnels) : verrouille le groupe de tunnels choisi, à moins que la case Inherit (Hériter) ou la valeur None (Aucun) ne soit sélectionnée.
- IPsec Backup Servers (Serveurs de sauvegarde IPsec) : active les champs Server Configuration (Configuration du serveur) et Server IP Addresses (Adresses IP du serveur), afin que vous puissiez préciser les serveurs de sauvegarde UDP à utiliser si ces valeurs ne sont pas héritées.
  - Server Configuration (Configuration du serveur) : répertorie les options de configuration du serveur à utiliser comme serveur de sauvegarde IPsec. Les options disponibles sont les suivantes : Keep Client Configuration (Conserver la configuration du client) [par défaut], Use the Backup Servers Below (Utiliser les serveurs de sauvegarde ci-dessous) et Clear Client Configuration (Effacer la configuration du client).
  - Server Addresses (space delimited) [Adresses du serveur (délimitées par des espaces)] : spécifie les adresses IP des serveurs de sauvegarde IPsec. Ce champ est disponible uniquement lorsque la valeur de la sélection Server Configuration (Configuration du serveur) est Use the Backup Servers Below (Utiliser les serveurs de sauvegarde ci-dessous).

À propos des règles d'accès pour le client IPsec (IKEv1) dans une stratégie de groupe interne

Le tableau des règles d'accès client dans cette boîte de dialogue vous permet d'afficher jusqu'à 25 règles d'accès client. Configurez les champs suivants lors de l'ajout d'une règle d'accès client :

- Priorité : sélectionnez une priorité pour cette règle.
- Action : autoriser ou refuser l'accès en fonction de cette règle.
- Type de client VPN : précisez le type de client VPN auquel cette règle s'applique, logiciel ou matériel, et pour les clients logiciels, tous les clients Windows ou un sous-ensemble en texte libre.
- Version du client VPN : précisez la version ou les versions du client VPN auquel cette règle s'applique. Cette colonne contient une liste d'images de logiciels ou de micrologiciel séparées par des virgules appropriées pour ce client. L'entrée est du texte de forme libre et ***** correspond à n'importe quelle version.

Définitions des règles d'accès client

- Si vous ne définissez aucune règle, l'ASA autorise tous les types de connexion. Toutefois, les utilisateurs peuvent toujours hériter des règles qui existent dans la politique de groupe par défaut.
- 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.
- Le caractère * est un caractère générique, que vous pouvez saisir plusieurs fois dans chaque règle.
- Il y a une limite de 255 caractères pour un ensemble complet de règles.
- Vous pouvez saisir **s.o.** pour les clients qui n'envoient pas le type de client et/ou la version.

Stratégies de groupe internes, pare-feu du client pour le client IPsec (IKEv1)

La boîte de dialogue Add or Edit Group Policy Client Firewall (Ajouter ou Modifier le pare-feu client de la stratégie de groupe) 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. 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).

Les utilisateurs distants se connectant à l'ASA avec le client VPN peuvent choisir l'option de pare-feu appropriée.

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 de pare-feu s'appelle Êtes-vous là (AYT), car le client VPN surveille le pare-feu en lui envoyant périodiquement « êtes-vous là?» messages ; si aucune réponse ne parvient, le client VPN sait que le pare-feu est en panne 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 tunnellisation 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.

Configuration > Remote Access > Network (Client) Access > Group Policies > Advanced > IPsec (IKEv1) Client > Client Firewall (Configuration > Accès à distance > Accès au réseau [client] > Stratégies de groupe > Avancé > Client IPsec [IKEv1] > Pare-feu client)

Champs

- **Inherit** (Hériter) : détermine si la stratégie de groupe obtient son paramètre de pare-feu client à partir de la stratégie de groupe par défaut. Il s'agit du paramètre par défaut. Lorsqu'il est défini, il remplace les attributs restants dans cette boîte de dialogue et estompe leurs noms.
- **Client Firewall Attributes** (Attributs de pare-feu client) : spécifie les attributs du pare-feu client, y compris le type de pare-feu (le cas échéant) mis en œuvre et la politique de pare-feu pour ce pare-feu.
- **Firewall Setting** (Paramètre de pare-feu) : indique si un pare-feu existe et, si oui, s'il est obligatoire ou facultatif. Si vous choisissez No Firewall (Aucun pare-feu) [par défaut], aucun des champs restants dans cette boîte de dialogue n'est actif. Si vous souhaitez que les utilisateurs de ce groupe soient protégés par un pare-feu, choisissez le paramètre Firewall Required (Pare-feu requis) ou Firewall Optional (Pare-feu facultatif).

  Si vous choisissez **Firewall Required** (Pare-feu requis), tous les utilisateurs de ce groupe doivent utiliser le pare-feu désigné. L'ASA abandonne toute session qui tente de se connecter sans que le pare-feu désigné et pris en charge soit installé et en cours d'exécution. Dans ce cas, l'ASA informe le client VPN que la configuration de son pare-feu ne correspond pas.

Remarque Si vous avez besoin d'un pare-feu pour un groupe, assurez-vous que le groupe ne comprend aucun client autre que les clients VPN Windows. Aucun autre client dans le groupe (y compris ASA 5505 en mode client) ne peut se connecter.

  Si vous avez des utilisateurs distants dans ce groupe qui ne disposent pas encore de la capacité de pare-feu, choisissez **Firewall Optional** (Pare-feu facultatif). Le paramètre Firewall Optional (Pare-feu facultatif) permet à tous les utilisateurs du groupe de se connecter. Ceux qui ont un pare-feu peuvent l'utiliser; les utilisateurs qui se connectent sans pare-feu reçoivent un message d'avertissement. Ce paramètre est utile si vous créez un groupe dans lequel certains utilisateurs ont une prise en charge de pare-feu et d'autres non. Par exemple, vous pouvez avoir un groupe en transition progressive, dans lequel certains membres ont configuré la capacité de pare-feu et d'autres ne l'ont pas encore fait.

- **Firewall Type** (Type de pare-feu) : répertorie les pare-feu de plusieurs fournisseurs, y compris Cisco. Si vous choisissez Custom Firewall (Pare-feu personnalisé), les champs sous Custom Firewall (Pare-feu personnalisé) deviennent actifs. Le pare-feu que vous désignez doit correspondre aux stratégies de pare-feu disponibles. Le pare-feu que vous configurez détermine les options de stratégie de pare-feu prises en charge.
- **Custom Firewall** (Pare-feu personnalisé) : spécifie l'ID du fournisseur, l'ID de produit et la description du pare-feu personnalisé.
  - **Vendor ID (ID du fournisseur)** : spécifie le fournisseur du pare-feu personnalisé pour cette stratégie de groupe.
  - **Product ID (ID de produit)** : spécifie le nom de produit ou de modèle du pare-feu personnalisé en cours de configuration pour cette stratégie de groupe.
  - **Description** : (facultatif) décrit le pare-feu personnalisé.

- **Firewall Policy** (Stratégie de pare-feu) : spécifie le type et la source de la stratégie de pare-feu personnalisée.
  - **Policy defined by remote firewall (AYT)** (Stratégie définie par le pare-feu distant [AYT]) : spécifie que la stratégie de pare-feu est définie par le pare-feu distant (Are You There). La stratégie définie par le pare-feu distant (AYT) signifie que les utilisateurs distants de ce groupe ont des pare-feu situés sur leur PC. Le pare-feu local applique la stratégie de pare-feu sur le client VPN. L'ASA permet aux clients VPN de ce groupe de se connecter uniquement si le pare-feu désigné est installé et en cours d'exécution. Si le pare-feu désigné n'est pas en cours d'exécution, la connexion échoue. Une fois la connexion établie, le client VPN interroge le pare-feu toutes les 30 secondes pour s'assurer qu'il est toujours en cours d'exécution. Si le pare-feu arrête de s'exécuter, le client VPN met fin à la session.
  - **Policy pushed (CPP)** (Stratégie poussée [CPP]) : spécifie que la stratégie est poussée par l'homologue. Si vous choisissez cette option, les listes Inbound Traffic Policy (Stratégie de trafic entrant) et Outbound Traffic Policy (Stratégie de trafic sortant), ainsi que le bouton Manage (Gérer), deviennent actifs. L'ASA applique aux clients VPN de ce groupe les règles de gestion du trafic définies par le filtre que vous choisissez dans la liste déroulante Policy Pushed (CPP) [Stratégie poussée (CPP)]. Les choix disponibles dans le menu sont des filtres définis dans cet ASA, y compris les filtres par défaut. Gardez à l'esprit que l'ASA applique ces règles au client VPN. Vous devez donc créer et définir ces règles par rapport au client VPN, et non à l'ASA. Par exemple, « in » et « out » (sortie) font référence au trafic entrant dans le client VPN ou sortant du client VPN. Si le client VPN dispose également d'un pare-feu local, la stratégie transmise par l'ASA fonctionne avec la stratégie du pare-feu local. Tout paquet bloqué par les règles de l'un ou l'autre des pare-feu est abandonné.
  - **Inbound Traffic Policy** (Stratégie de trafic entrant) : répertorie les stratégies poussées disponibles pour le trafic entrant.
  - **Outbound Traffic Policy** (Stratégie de trafic sortant) : répertorie les stratégies poussées disponibles pour le trafic sortant.
  - **Manage** (Gérer) : affiche la boîte de dialogue ACL Manager (Gestionnaire ACL), dans laquelle vous pouvez configurer les listes de contrôle d'accès (ACL).

Stratégies de groupe internes, de site à site

La stratégie de groupe pour les connexions VPN de site à site spécifie les protocoles de tunnellisation, les filtres et les paramètres de connexion. Pour chacun des champs de cette boîte de dialogue, cocher la case Inherit (Hériter) permet au paramètre correspondant de prendre sa valeur à partir de la stratégie de groupe par défaut. Inherit (Hériter) est la valeur par défaut de tous les attributs de cette boîte de dialogue.

Champs

Les attributs suivants apparaissent dans la boîte de dialogue Add Internal Group Policy (Ajouter une stratégie de groupe interne) > General (Général). Ils s'appliquent aux sessions VPN SSL et IPsec. Ainsi, plusieurs sont présents pour un type de session, mais pas pour l'autre.

- Name (Nom) : spécifie le nom de cette stratégie de groupe. Pour la fonction d'édition, ce champ est en lecture seule.

- Tunneling Protocols (Protocoles de tunnellisation) : spécifie les protocoles de tunnellisation autorisés par ce groupe. Les utilisateurs ne peuvent utiliser que les protocoles sélectionnés. Voici les différents choix proposés :
  - Clientless SSL VPN (VPN SSL sans client) : spécifie l'utilisation du VPN par SSL/TLS, qui utilise un navigateur Web pour établir un tunnel d'accès à distance sécurisé vers un ASA ; ne nécessite ni logiciel ni matériel client. Le VPN SSL sans client peut fournir un accès facile à un large éventail de ressources d'entreprise, y compris les sites Web d'entreprise, les applications Web, le partage de fichiers NT/AD (activé sur le Web), le courriel et d'autres applications basées sur TCP à partir de presque n'importe quel ordinateur qui peut atteindre les sites Internet HTTPS.
  - SSL VPN Client (Client VPN SSL) : spécifie l'utilisation du module VPN AnyConnect du client ou de l'ancien client VPN SSL. Si vous utilisez Secure Client, vous devez choisir ce protocole pour que MUS soit pris en charge.
  - IPsec IKEv1 : protocole de sécurité IP. Considéré comme le protocole le plus sécurisé, IPsec fournit l'architecture la plus complète pour les tunnels VPN. Les connexions de site à site (homologue à homologue) et les connexions de client VPN Cisco à réseau local (LAN) peuvent utiliser IPsec IKEv1.
  - IPsec IKEv2 : pris en charge par le client . Les connexions Secure Client utilisant IPsec avec IKEv2 fournissent des fonctionnalités avancées telles que les mises à jour logicielles, les profils clients, la localisation et la personnalisation de l'interface graphique (traduction) et la personnalisation, Cisco Secure Desktop et le serveur proxy SCEP.
  - L2TP sur IPsec (L2TP over IPsec) : permet aux utilisateurs distants avec des clients VPN fournis avec plusieurs systèmes d'exploitation courants pour PC et PC mobiles d'établir des connexions sécurisées sur le réseau IP public avec l'appareil de sécurité et les réseaux privés d'entreprise. L2TP utilise PPP sur UDP (port 1701) pour tunneliser les données. L'appareil de sécurité doit être configuré pour le mode de transport IPsec.

- **Filter** (Filtre) : (accès réseau (client) uniquement) spécifie la liste de contrôle d'accès à utiliser ou s'il faut hériter de la valeur de la stratégie de groupe. Les filtres consistent en des règles qui déterminent s'il faut autoriser ou rejeter les paquets de données tunnellisés en fonction de critères comme l'adresse source, l'adresse de destination et le protocole. 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. Pour configurer les filtres et les règles, consultez la boîte de dialogue de la politique de groupe. Cliquez sur **Manage** (Gérer) pour ouvrir le gestionnaire d'ACL, où vous pouvez afficher et configurer les listes de contrôle d'accès.
- **Idle Timeout** (Délai d'inactivité) : si la case **Inherit** (Hériter) n'est pas cochée, ce paramètre définit le délai d'inactivité en minutes.

  S'il n'y a aucune activité de communication sur la connexion pendant cette période, le système arrête la connexion. La durée minimale est de 1 minute, la durée maximale est de 10080 minutes et la valeur par défaut est de 30 minutes. Pour autoriser un temps de connexion illimité, cochez **Unlimited** (Illimité).
- **Maximum Connect Time** (Durée maximale de connexion) : si la case **Inherit** (Hériter) n'est pas cochée, ce paramètre définit la durée maximale de connexion de l'utilisateur en minutes.

  À la fin de cette durée, le système met fin à la connexion. La durée minimale est de 1 minute et la durée maximale est de 35 791 394 minutes. Pour autoriser une durée de connexion illimitée, cochez **Unlimited** (Illimité) (par défaut).

- **Periodic Certificate Authentication Interval** (Intervalle d'authentification périodique du certificat) : intervalle de temps en heures avant que l'authentification du certificat soit relancée périodiquement.

  Si la case **Inherit** (Hériter) n'est pas cochée, vous pouvez définir l'intervalle d'exécution de la vérification périodique du certificat. La plage est comprise entre 1 et 168 heures, et la valeur par défaut est désactivée. Pour autoriser une vérification illimitée, cochez Unlimited (Illimité).

Configurer les attributs de politique VPN pour un utilisateur local

Cette procédure décrit comment modifier un utilisateur existant. Pour ajouter un utilisateur, choisissez **Configuration > Remote Access VPN (VPN d'accès à distance) > AAA/Local Users (AAA/Utilisateurs locaux) > Local Users (Utilisateurs locaux)** et cliquez sur **Add**(Ajouter). Consultez le guide de configuration des opérations générales pour plus d'informations.

Avant de commencer

Par défaut, le compte d'utilisateur hérite de la valeur de chaque paramètre de la stratégie de groupe par défaut, DfltGrpPolicy. Pour remplacer chaque paramètre, décochez la case **Inherit** (Hériter) et saisissez une nouvelle valeur.

Procédure

Étape 1 Démarrez ASDM et choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **AAA/Local Users (AAA/Utilisateurs locaux)** > **Local Users (Utilisateurs locaux)**.

Étape 2 Sélectionnez l'utilisateur que vous souhaitez configurer et cliquez sur **Edit** (Modifier).

Étape 3 Dans le volet de gauche, cliquez sur **VPN Policy** (Politique VPN).

Étape 4 Précisez une stratégie de groupe pour l'utilisateur. La politique d'utilisateur héritera des attributs de cette stratégie de groupe. S'il y a d'autres champs sur cet écran qui sont définis sur **Inherit the configuration from the Default Group Policy** (Hériter de la configuration de la stratégie de groupe par défaut), les attributs spécifiés dans cette stratégie de groupe prévaudront sur ceux définis dans la stratégie de groupe par défaut.

Étape 5 Précisez quels Tunneling Protocols (Protocoles de tunnellisation) sont disponibles pour l'utilisateur ou si la valeur est héritée de la stratégie de groupe.

Cochez les cases **Tunneling Protocols** (Protocoles de tunnellisation) souhaitées pour choisir l'un des protocoles de tunnellisation suivants :

- Le client VPN SSL permet aux utilisateurs de se connecter après avoir téléchargé l'application Secure Client. Les utilisateurs utilisent une connexion VPN SSL sans client pour télécharger cette application la première fois. Les mises à jour du client se produisent ensuite automatiquement en cas de besoin chaque fois que l'utilisateur se connecte.
- IPsec IKEv1 : protocole de sécurité IP. Considéré comme le protocole le plus sécurisé, IPsec fournit l'architecture la plus complète pour les tunnels VPN. Les connexions de site à site (homologue à homologue) et les connexions de client VPN Cisco à réseau local (LAN) peuvent utiliser IPsec IKEv1.
- IPsec IKEv2 : pris en charge par Secure Client. Les connexions Secure Client utilisant IPsec avec IKEv2 fournissent des fonctionnalités avancées telles que les mises à jour logicielles, les profils clients, la localisation et la personnalisation de l'interface graphique (traduction) et la personnalisation, Cisco Secure Desktop et le serveur proxy SCEP.

- L2TP sur IPsec permet aux utilisateurs distants avec des clients VPN fournis avec plusieurs systèmes d'exploitation courants de PC et de PC mobiles d'établir des connexions sécurisées sur le réseau IP public avec l'ASA et les réseaux privés d'entreprise.

Remarque
Si aucun protocole n'est sélectionné, un message d'erreur s'affiche.

Étape 6 Précisez le filtre (IPv4 ou IPv6) à utiliser ou s'il faut hériter de la valeur de la stratégie de groupe.

Les filtres consistent en des règles qui déterminent s'il faut autoriser ou rejeter les paquets de données tunnellisés en fonction de critères comme l'adresse source, l'adresse de destination et le protocole. 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.

a) Pour configurer des filtres et des règles, choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Network (Client) Access (Accès réseau (client))** > **Group Policies (Stratégies de groupe)** > **Add/Edit (Ajouter/Modifier)** > **General (Général)** > **More Options (Plus d'options)** > **Filter (Filtre).**
b) Cliquez sur **Manage** (Gérer) pour afficher le volet ACL Manager, dans lequel vous pouvez ajouter, modifier et supprimer des listes de contrôle d'accès (ACL) et des entrées de contrôle d'accès (ACE).

Étape 7 Précisez s'il faut hériter du verrouillage de profil de connexion (groupe de tunnels) ou utiliser le verrouillage de groupe de tunnels sélectionné, le cas échéant.

La sélection d'un verrouillage spécifique restreint les utilisateurs à l'accès à distance par l'intermédiaire de ce groupe uniquement. Le verrouillage de groupe de tunnel restreint les utilisateurs en vérifiant si le groupe configuré dans le client VPN est le même que le groupe affecté aux utilisateurs. Si ce n'est pas le cas, l'ASA empêche l'utilisateur de se connecter. Si la case Inherit (Hériter) n'est pas cochée, la valeur par défaut est None (Aucun).

Étape 8 Précisez s'il faut hériter du paramètre Store Password on Client System (Stockage du mot de passe sur le système client) du groupe.

Décochez la case **Inherit** (Hériter) pour activer les boutons radio Yes (Oui) et No (Non). Cliquez sur **Yes** (Oui) pour stocker le mot de passe de connexion sur le système client (éventuellement une option moins sécurisée). Cliquez sur **No** (Non) (valeur par défaut) pour exiger que l'utilisateur saisisse le mot de passe à chaque connexion. Pour une sécurité maximale, nous vous recommandons de ne pas autoriser le stockage de mots de passe.

Étape 9 Configuration des **paramètres de connexion**.

a) Précisez une politique d'heures d'accès à appliquer à cet utilisateur, créez une nouvelle politique d'heures d'accès pour l'utilisateur ou laissez la case Inherit (Hériter) cochée. La valeur par défaut est Inherit (Hériter) ou, si la case Inherit (Hériter) n'est pas cochée, la valeur par défaut est Unrestricted (Non restreinte).

Cliquez sur **Manage** (Gérer) pour ouvrir la boîte de dialogue Add Time Range (Ajouter une plage temporelle), dans laquelle vous pouvez spécifier un nouvel ensemble d'heures d'accès.

b) Précisez le nombre de connexions simultanées par l'utilisateur. Le paramètre Simultaneous Logins (Connexions simultanées) spécifie le nombre maximal de connexions simultanées autorisées pour cet utilisateur. La valeur par défaut est 3. La valeur minimale est 0, ce qui désactive la connexion et empêche l'accès de l'utilisateur.

Remarque
Bien qu'il n'y ait pas de limite maximale, autoriser plusieurs connexions simultanées peut compromettre la sécurité et affecter les performances.

c) Précisez le **Maximum Connect Time** (Délai de connexion maximal) pour la connexion VPN en minutes. À la fin de ce délai, le système met fin à la connexion.

Si la case **Inherit** (Hériter) n'est pas cochée, ce paramètre spécifie la durée maximale de connexion d'utilisateur en minutes. La durée minimale est de 1 minute et le maximum est de 35 791 394 minutes (plus de 4 000 ans). Pour autoriser un temps de connexion illimité, cochez **Unlimited** (Illimité) (valeur par défaut).

d) Précisez l'**Idle Timeout** (Délai d'inactivité) pour la connexion VPN en minutes. S'il n'y a aucune activité de communication sur la connexion pendant cette période, le système met fin à la connexion.

Si la case **Inherit** (Hériter) n'est pas cochée, ce paramètre spécifie le délai d'inactivité en minutes. La durée minimale est de 1 minute, la durée maximale est de 10 080 minutes et la valeur par défaut est de 30 minutes. Pour autoriser un temps de connexion illimité, cochez la case **Unlimited** (Illimité).

Étape 10 Configuration des **alertes de délai d'expiration**.

a) Précisez le **Maximum Connection Time Alert Interval** (Intervalle d'alerte de durée de connexion maximale).

Si vous décochez la case **Inherit** (Hériter), la case **Default** (Par défaut) est cochée automatiquement. Cela définit l'intervalle d'alerte de connexion maximal à 30 minutes. Si vous souhaitez spécifier une nouvelle valeur, décochez **Default** (Par défaut) et spécifiez un intervalle d'alerte de session de 1 à 30 minutes.

b) Précisez l'**Idle Alert Interval** (Intervalle d'alerte d'inactivité).

Si vous décochez la case **Inherit** (Hériter), la case **Default** (Par défaut) est cochée automatiquement. Cela définit l'intervalle d'alerte de connexion maximal à 30 minutes. Si vous souhaitez spécifier une nouvelle valeur, décochez **Default** (Par défaut) et spécifiez un intervalle d'alerte de session de 1 à 30 minutes.

Étape 11 Pour définir une adresse IPv4 dédiée à cet utilisateur, saisissez une adresse IPv4 et un masque de sous-réseau dans la zone **Adresse IPv4 dédiée (facultatif)**.

Étape 12 Pour définir une adresse IPv6 dédiée à cet utilisateur, saisissez une adresse IPv6 avec un préfixe IPv6 dans la zone **Adresse IPv6 dédiée (facultatif)**. Le préfixe IPv6 indique le sous-réseau sur lequel se trouve l'adresse IPv6.

Étape 13 Configurez des paramètres spécifiques Secure Client en cliquant sur ces options dans le volet de gauche. Pour remplacer chaque paramètre, décochez la case **Inherit** (Hériter) et saisissez une nouvelle valeur.

Étape 14 Cliquez sur **OK** pour appliquer les modifications à la configuration en cours d'exécution.

Profils de connexion

Les profils de connexion, également appelés groupes de tunnels, configurent les attributs de connexion pour les connexions VPN. Ces attributs s'appliquent au module VPN AnyConnect de Cisco Secure Client, aux connexions VPN SSL sans client et aux clients VPN tiers IKEv1 et IKEv2.

Profil de connexion Secure Client, Volet principal

Dans le volet principal du profil de connexion Secure Client, vous pouvez activer l'accès client sur les interfaces et ajouter, modifier et supprimer des profils de connexion. Vous pouvez également préciser si vous souhaitez autoriser un utilisateur à choisir une connexion particulière lors de la connexion.

- Access Interfaces (Interfaces d'accès) : vous permet de choisir dans un tableau les interfaces sur lesquelles activer l'accès. Les champs de ce tableau comprennent le nom de l'interface et des cases à cocher précisant s'il faut autoriser l'accès.
  - Dans le tableau Interface, sur la ligne de l'interface que vous configurez pour les connexions Secure Client, cochez les protocoles que vous souhaitez activer sur l'interface. Vous pouvez autoriser l'accès SSL, l'accès IPsec ou les deux.

    Lorsque vous cochez SSL, DTLS (Datagram Transport Layer Security) est activé par défaut. 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.

    Lorsque vous cochez l'accès IPsec (IKEv2), les services clients sont activés par défaut. Les services clients comprennent des fonctionnalités Secure Client améliorées, notamment les mises à jour logicielles, les profils clients, la localisation (traduction) et la personnalisation de l'interface graphique, Cisco Secure Desktop et le proxy SCEP. Si vous désactivez les services clients, Secure Client établit toujours des connexions IPsec de base avec IKEv2.
  - Device Certificate (Certificat de périphérique) : vous permet de préciser un certificat pour l'authentification pour une clé RSA ou une clé ECDSA. Consultez Préciser le certificat du périphérique, à la page 105.
  - Port Setting (Paramètre de port) : configurez les numéros de port pour les connexions HTTPS et DTLS (client d'accès à distance uniquement). Consultez Profils de connexion, paramètres de port, à la page 106.
  - Bypass interface access lists for inbound VPN sessions (Contourner les listes d'accès d'interface pour les sessions VPN entrantes) : Enable inbound VPN sessions to bypass interface ACLs (Activer les sessions VPN entrantes pour contourner les ACL d'interface) est cochée par défaut. L'appareil de sécurité permet à tout le trafic VPN de passer par les listes de contrôle d'accès de l'interface. Par exemple, même si l'ACL de l'interface externe ne permet pas au trafic déchiffré, l'appareil de sécurité fait confiance au réseau privé distant et permet aux paquets déchiffrés de passer. Vous pouvez modifier ce comportement. Si vous souhaitez que l'ACL de l'interface inspecte le trafic protégé par le VPN, décochez cette case.

- Paramètres de la page de connexion
  - Autorisez l'utilisateur à choisir un profil de connexion, identifié par son alias, sur la page de connexion. Si vous ne cochez pas cette case, le profil de connexion par défaut est DefaultWebVPNGroup.
  - Shutdown portal login page (Page de connexion du portail désactivée) : affiche la page Web lorsque la connexion est désactivée.

- Connection Profiles (Profils de connexion) : configurez les attributs propres au protocole pour les connexions (groupes de tunnels).
  - Add/Edit (Ajouter/modifier) : cliquez pour ajouter ou modifier un profil de connexion (groupe de tunnels).
  - Name (Nom) : nom du profil de connexion.
  - Aliases (Alias) : autres noms par lesquels le profil de connexion est connu.
  - SSL VPN Client Protocol (Protocole client VPN SSL : spécifie si le client VPN SSL a accès.

- Group Policy (Stratégies de groupe) : affiche la stratégie de groupe par défaut pour ce profil de connexion.
- Allow user to choose connection, identified by alias in the table above, at login page (Autoriser l'utilisateur à choisir la connexion, identifiée par l'alias dans le tableau ci-dessus, sur la page de connexion) : cochez cette option pour activer l'affichage des alias de profil de connexion (groupe de tunnels) sur la page de connexion.

- Laissez l'URL de groupe prendre le pas si l'URL de groupe et la carte de certificat correspondent à différents profils de connexion. Sinon, le profil de connexion correspondant à la carte de certificat sera utilisé : cette option précise la préférence relative de l'URL de groupe et des valeurs de certificat pendant le processus de sélection du profil de connexion. Si l'ASA ne parvient pas à correspondre à la valeur préférée, il choisit le profil de connexion qui correspond à l'autre valeur. Cochez cette option uniquement si vous souhaitez vous baser sur la préférence utilisée par de nombreuses versions logicielles ASA plus anciennes pour faire correspondre l'URL de groupe spécifiée par le terminal VPN au profil de connexion qui spécifie la même URL de groupe. Cette option est décochée par défaut. Si cette option n'est pas cochée, l'ASA préfère faire correspondre la valeur de champ de certificat spécifiée dans le profil de connexion à la valeur de champ du certificat utilisé par le point terminal pour affecter le profil de connexion.

Préciser le certificat du périphérique

Le volet **Specify Device Certificate** (Préciser le certificat du périphérique) vous permet de préciser un certificat qui identifie l'ASA auprès du client lorsqu'il tente de créer une connexion. Cet écran concerne les profils de connexion Secure Client et les profils de connexion sans client. Certaines fonctionnalités Secure Client, telles qu'Always-on IPsec/IKEv2, nécessitent qu'un certificat de périphérique valide et approuvé soit disponible sur l'ASA.

À partir de la version 9.4.1 d'ASA, les certificats ECDSA peuvent être utilisés pour les connexions SSL (à partir des connexions SSL avec Secure Client et SSL sans client). Avant cette version, les certificats ECDSA n'étaient pris en charge et configurés que pour les connexions Secure Client IPsec.

Procédure

Étape 1 (Pour les connexions VPN uniquement) Dans la zone **Certificat avec clé RSA**, effectuez l'une des tâches suivantes :

- Cochez la case **Use the same device certificate for SSL and IPsec IKEv2** (Utiliser le même certificat de périphérique pour SSL et IPsec IKEv2) si vous souhaitez choisir un certificat pour authentifier les clients utilisant l'un ou l'autre de ces protocoles. Vous pouvez choisir le certificat parmi ceux disponibles dans la zone de liste ou cliquer sur **Manage** (Gérer) pour créer un certificat d'identité à utiliser.
- Décochez la case **Use the same device certificate for SSL and IPsec IKEv2** (Utiliser le même certificat de périphérique pour SSL et IPsec IKEv2) pour préciser des certificats distincts pour les connexions SSL ou les connexions IPsec.

Étape 2 Choisissez un certificat dans la zone de liste **Device Certificate** (Certificat de périphérique).

Si vous ne voyez pas le certificat souhaité, cliquez sur le bouton **Manage** (Gérer) pour gérer les certificats d'identité sur l'ASA.

Étape 3 (Pour les connexions VPN uniquement) Dans le champ Certificate with ECDSA key (Certificat avec clé ECDSA), choisissez le certificat ECDSA dans la zone de liste ou cliquez sur **Manage** (Gérer) pour créer un certificat d'identité ECDSA.

Étape 4 Cliquez sur **OK**.

Profils de connexion, paramètres de port

Configurez les numéros de port des connexions SSL et DTLS (accès à distance uniquement) dans les volets de profil de connexion d'ASDM :

Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Connection Profiles (Profils de connexion)vSecure Client

Champs

- HTTPS Port (Port HTTPS) : port à activer pour les connexions SSL HTTPS (basées sur le navigateur). La plage est comprise entre 1 et 65 535. La valeur par défaut du port est 443.
- DTLS Port (Port DTLS) : port UDP à activer pour les connexions DTLS. La plage est comprise entre 1 et 65 535. La valeur du port par défaut est 443.

Profil de connexion Secure Client, attributs de base

Pour définir les attributs de base d'un module VPN AnyConnect de Cisco Secure Client, choisissez Add (Ajouter) ou Edit (Modifier) dans la section Connection Profiles (Profils de connexion) Secure Client. La boîte de dialogue Add (Ajouter) (ou Edit (Modifier)) Connection Profile (Profil de connexion) Secure Client > Basic (Base) s'ouvre.

- Name (nom) : pour ajouter, précisez le nom du profil de connexion que vous ajoutez. Pour modifier, ce champ n'est pas modifiable.
- Alias : (facultatif) saisissez un ou plusieurs noms alternatifs pour la connexion. Vous pouvez ajouter des espaces ou des signes de ponctuation pour séparer les noms.
- Authentication (authentification) : choisissez l'une des méthodes suivantes à utiliser pour authentifier la connexion et préciser le groupe de serveurs AAA à utiliser dans l'authentification.
  - Le protocole d'authentification a été étendu pour définir un échange de protocole pour l'authentification à certificats multiples et l'utiliser pour les deux types de sessions. Vous pouvez valider plusieurs certificats par session avec les protocoles client Secure Client SSL et IKEv2. Choisissez le type d'authentification à utiliser : AAA, AAA and certificate (AAA et certificat), Certificate only (Certificat uniquement), SAML (SAML), Multiple certificates and AAA (Plusieurs certificats et AAA), Multiple certificates (Plusieurs certificats), SAML and certificate (SAML et certificat) ou Multiple certificates and SAML (Plusieurs certificats et SAML). Selon votre sélection, vous devrez peut-être fournir un certificat pour vous connecter.
  - AAA Server Group (Groupe de serveurs AAA) : choisissez un groupe de serveurs AAA dans la liste déroulante. Le paramètre par défaut est LOCAL, ce qui spécifie que l'ASA gère l'authentification. Avant de faire une sélection, vous pouvez cliquer sur **Manage** (Gérer) pour ouvrir une boîte de dialogue par-dessus celle-ci afin d'afficher ou de modifier la configuration ASA des groupes de serveurs AAA.

- Choisir autre chose que LOCAL rend disponible la case à cocher Use LOCAL if Server Group Fails (Utiliser LOCAL si le groupe de serveurs échoue).
- Use LOCAL if Server Group Fails (Utiliser LOCAL si le groupe de serveurs échoue) : cochez cette option pour activer l'utilisation de la base de données locale si le groupe spécifié par l'attribut Authentication Server Group (Groupe de serveurs d'authentification) échoue.

- SAML Identity Provider (Fournisseur d'identité SAML) : choisissez le serveur fournisseur d'identité SAML pour l'authentification par connexion unique (SSO).
  - SAML Server (Serveur SAML) : sélectionnez le serveur SAML dans la liste déroulante pour l'authentification par connexion unique Secure Client ou cliquez sur **Manage** (Gérer) pour ajouter un serveur SSO et configurer les paramètres suivants :
    - **IDP Entity ID** (ID d'entité IDP) : l'ID d'entité du fournisseur d'identité SAML.
    - **Sign In URL** (URL de connexion) : URL de connexion au fournisseur d'identité. La valeur de l'URL doit contenir de 4 à 500 caractères.
    - **Sign Out URL (URL** de déconnexion) : (facultatif) URL vers laquelle rediriger lors de la déconnexion du fournisseur d'identité. La valeur de l'URL doit contenir de 4 à 500 caractères.
    - **Base URL** (URL de base) : (facultatif) URL fournie aux 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**.
    - **Identity Provider Certificate** (Certificat du fournisseur d'identité) : spécifie le point de confiance qui contient le certificat du fournisseur d'identité pour que l'ASA vérifie les assertions SAML. Choisissez un point de confiance précédemment configuré.
    - **Service Provider Certificate** (Certificat du fournisseur de services) : (facultatif) spécifie le point de confiance 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. Choisissez un point de confiance précédemment configuré.
    - **Request Signature (demander la signature)** : utilisez la liste déroulante pour choisir la méthode de signature que vous préférez pour le serveur fournisseur d'identité de SAML. Vous pouvez choisir rsa-sha1, rsa-sha256, rsa-sha384 ou rsa-sha512.
    - **Request Timeout** (Délai d'expiration de la demande) : (facultatif) délai d'expiration de la demande SAML en secondes. La plage est comprise entre 1 et 7 200.

      Si ce paramètre est spécifié, il 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.

- **Enable IDP only accessible on internal network** (Activer le fournisseur d'identité uniquement accessible sur le réseau interne) : cochez cette case pour activer le fournisseur d'identité uniquement s'il est accessible sur le réseau interne.
- **Request IDP reauthentication at login** (Demander la réauthentification du fournisseur d'identité à la connexion) : cochez cette case pour activer la réauthentification du fournisseur d'identité à la connexion.
- **Clock-skew** (Décalage d'horloge) : décalage d'horloge qui tolère les assertions SAML NotBefore et NotOnOrAfter. Par défaut, le décalage d'horloge doit être désactivé. La valeur par défaut est de 1 seconde et la plage est comprise entre 1 et 180 secondes.

- SAML IDP TrustPoint (Point de confiance du fournisseur d'identité SAML) : choisissez le point de confiance du fournisseur d'identité SAML pour l'authentification par connexion unique (SSO).
  - IDP TrustPoint (Point de confiance IDP) : sélectionnez le point de confiance du fournisseur d'identité SAML qui contient le certificat du fournisseur d'identité pour que l'ASA vérifie les assertions SAML.
- SAML Login Experience (Expérience de connexion SAML) : choisissez le SAML IdP TrustPoint (Point de confiance du fournisseur d'identité SAML) pour l'authentification par connexion unique (SSO).
  - VPN Client Embedded Browser (Navigateur intégré du client VPN) : le client VPN utilise son navigateur intégré pour l'authentification Web; l'authentification s'applique donc uniquement à la connexion VPN.
  - Default OS Browser (Navigateur du système d'exploitation par défaut) : le client VPN utilise le navigateur par défaut du système pour l'authentification Web. Cette option active l'authentification unique (SSO) et prend en charge les méthodes d'authentification Web, telles que l'authentification biométrique, qui ne peuvent pas être exécutées dans le navigateur intégré.

    Lorsque vous choisissez le navigateur du système d'exploitation par défaut pour l'authentification SSO, vous devez configurer un progiciel de navigateur externe pour Secure Client utiliser le navigateur par défaut. Consultez Progiciel SAML Secure Client du navigateur externe, à la page 146.
- SAML UserName Match (Correspondance de nom d'utilisateur SAML) : sélectionnez cette option pour faire correspondre le nom d'utilisateur du certificat au nom d'utilisateur SAML.
- Client Address Assignment (Affectation d'adresses client) : choisissez les serveurs DHCP, les ensembles d'adresses client et les ensembles d'adresses IPv6 client à utiliser.
- Client Address Assignment (affectation d'adresses client) : choisissez les serveurs DHCP, les ensembles d'adresses clients et les ensembles d'adresses IPv6 clients à utiliser.
  - DHCP Servers (Serveurs DHCP) : saisissez le nom ou l'adresse IP d'un serveur DHCP à utiliser.
  - Client Address Pools (Ensembles d'adresses client) : saisissez le nom d'un ensemble d'adresses IPv4 disponible et configuré à utiliser pour l'affectation d'adresses client. Avant d'effectuer une sélection, vous pouvez cliquer sur **Select** (Sélectionner) pour ouvrir une boîte de dialogue dans cette boîte de dialogue afin d'afficher ou de modifier les ensembles d'adresses. Consultez la section pour obtenir plus d'informations sur l'ajout ou la modification d'un ensemble d'adresses IPv4.
  - Client IPv6 Address Pools (Ensembles d'adresses IPv6 client) : saisissez le nom d'un ensemble d'adresses IPv6 disponible et configuré à utiliser pour l'affectation d'adresses client. Avant d'effectuer une sélection, vous pouvez cliquer sur **Select** (Sélectionner) pour ouvrir une boîte de dialogue dans

cette boîte de dialogue afin d'afficher ou de modifier les ensembles d'adresses. Consultez la section pour en savoir plus sur l'ajout ou la modification d'un ensemble d'adresses IPv6.

•

- Default Group Policy (Stratégie de groupe par défaut) : sélectionnez la stratégie de groupe à utiliser.
  - Group Policy (Stratégie de groupe) : sélectionnez la stratégie de groupe VPN que vous souhaitez utiliser comme stratégie de groupe par défaut pour cette connexion. Une stratégie de groupe VPN est un ensemble de paires attribut-valeur d'utilisateur qui peuvent être stockées en interne sur le périphérique ou en externe sur un serveur RADIUS. La valeur par défaut est DfltGrpPolicy. Vous pouvez cliquer sur **Manage** (Gérer) pour ouvrir une boîte de dialogue par-dessus celle-ci afin d'apporter des modifications à la configuration de la stratégie de groupe.
  - Enable SSL VPN client protocol (Activer le protocole du client VPN SSL) : cochez cette option pour activer SSL pour cette connexion VPN.
  - Enable IPsec (IKEv2) client protocol (Activer le protocole client IPsec (IKEv2)) : cochez cette option pour activer IPsec à l'aide d'IKEv2 pour cette connexion.
  - DNS Servers (Serveurs DNS) : saisissez les adresses IP des serveurs DNS pour cette stratégie.
  - WINS Servers (Serveurs WINS) : saisissez les adresses IP des serveurs WINS pour cette stratégie.
  - Domain Name (Nom de domaine) : saisissez un nom de domaine par défaut.
- Find (Rechercher) : saisissez une étiquette d'interface graphique ou une commande CLI à utiliser comme chaîne de recherche, puis cliquez sur **Next** (Suivant) ou **Previous** (Précédent) pour commencer la recherche.

Profil de connexion, attributs avancés

Les éléments de menu Avancé et leurs boîtes de dialogue configurent les caractéristiques suivantes pour cette connexion :

- Attributs généraux
- Attributs de l'adressage du client
- Attributs d'authentification
- Attributs d'autorisation
- Attributs de gestion de comptes
- Attributs du serveur de noms

Remarque Les attributs SSL VPN et d'authentification secondaire s'appliquent uniquement aux profils de connexion VPN SSL.

Profil de connexion Secure Client, attributs généraux

- Activer l'inscription de certificat simple (SCEP) pour ce profil de connexion
- Supprimez le domaine du nom d'utilisateur avant de le transmettre au serveur AAA
- Supprimez le groupe du nom d'utilisateur avant de le transmettre au serveur AAA
- Délimiteur de groupe
- Activer Password Management (Gestion des mots de passe) : vous permet de configurer les paramètres pertinents pour informer les utilisateurs de l'expiration du mot de passe.
  - Notify user __ days prior to password expiration (Aviser l'utilisateur __ jours avant l'expiration du mot de passe) : spécifie qu'ASDM doit aviser l'utilisateur lors de la connexion un nombre précis de jours avant l'expiration du mot de passe. La valeur par défaut est d'envoyer une notification à l'utilisateur 14 jours avant l'expiration du mot de passe et chaque jour par la suite jusqu'à ce que l'utilisateur modifie le mot de passe. La plage est comprise entre 1 et 180 jours.
  - Notify user on the day password expires (Aviser l'utilisateur le jour de l'expiration du mot de passe) : avise l'utilisateur uniquement le jour où le mot de passe expire.

    Dans les deux cas, et, si le mot de passe expire sans être modifié, l'ASA offre à l'utilisateur la possibilité de modifier le mot de passe. Si le mot de passe actuel n'a pas expiré, l'utilisateur peut toujours se connecter en utilisant ce mot de passe.

    Cela ne modifie pas le nombre de jours avant l'expiration du mot de passe, mais active la notification. Si vous choisissez cette option, vous devez également préciser le nombre de jours.

- Translate Assigned IP Address to Public IP Address (Traduire l'adresse IP affectée en adresse IP publique) : dans de rares cas, vous pouvez utiliser l'adresse IP réelle d'un homologue VPN sur le réseau interne au lieu d'une adresse IP locale affectée. Normalement, avec le VPN, l'homologue reçoit une adresse IP locale attribuée pour accéder au réseau interne. Cependant, vous pouvez traduire l'adresse IP locale en adresse IP publique réelle de l'homologue si, par exemple, vos serveurs internes et la sécurité du réseau sont basés sur l'adresse IP réelle de l'homologue. Vous pouvez activer cette fonctionnalité sur une interface par groupe de tunnels.
  - Enable the address translation on interface (Activer la traduction d'adresses sur l'interface) : active la traduction d'adresses et vous permet de choisir l'interface sur laquelle l'adresse apparaît. *Outside* est l'interface à laquelle Secure Client se connecte et *inside* est l'interface spécifique au nouveau groupe de tunnels.

Remarque En raison de problèmes de routage et d'autres limites, nous ne recommandons pas l'utilisation de cette fonctionnalité, sauf si vous savez que vous en avez besoin.

- Find (Rechercher) : saisissez une étiquette d'interface graphique ou une commande CLI à utiliser comme chaîne de recherche, puis cliquez sur **Next** (Suivant) ou **Previous** (Précédent) pour commencer la recherche.

Profil de connexion, adressage du client

Le volet Client Addressing (Adressage du client) sur un profil de connexion attribue des ensembles d'adresses IP sur des interfaces spécifiques à utiliser avec ce profil de connexion. Le volet Client Addressing (Adressage du client) est commun à tous les profils de connexion client et est disponible à partir des chemins ASDM suivants :

- **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau (client)) > Secure Client/AnyConnect Connection Profiles (Profils de connexion Secure Client/)**
- **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau (client)) > IPsec(IKEv1) Connection Profiles (Profils de connexion IPsec(IKEv1))**
- **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau (client)) > IPsec(IKEv2) Connection Profiles (Profils de connexion IPsec(IKEv2))**

Les ensembles d'adresses que vous configurez ici peuvent également être configurés dans le volet Basic (Base) du profil de connexion.

Le profil de connexion Secure Client peut affecter des ensembles d'adresses IPv6 et IPv4.

Pour configurer l'adressage des clients, ouvrez un profil de connexion client d'accès à distance (Secure ClientIKEv1 ou IKEv2) et sélectionnez **Advanced** (Avancé) > **Client Addressing (Adressage du client)**.

- Pour afficher ou modifier la configuration des ensembles d'adresses, cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) dans la boîte de dialogue. La boîte de dialogue Affecter des ensembles d'adresses à l'interface s'ouvre. Cette boîte de dialogue vous permet d'affecter des ensembles d'adresses IP aux interfaces configurées sur l'ASA. Cliquez sur **Select** (sélectionner). Utilisez cette boîte de dialogue pour afficher la configuration des ensembles d'adresses. Vous pouvez modifier la configuration de leur ensemble d'adresses comme suit :
  - Pour ajouter un ensemble d'adresses à l'ASA, cliquez sur **Add** (Ajouter). La boîte de dialogue Add IP Pool (Ajouter un ensemble d'adresses IP) s'ouvre.
  - Pour modifier la configuration d'un ensemble d'adresses sur l'ASA, cliquez sur **Edit** (Modifier). La boîte de dialogue Edit IP Pool (Modifier le regroupement d'adresses IP) s'ouvre si les adresses dans le regroupement ne sont pas utilisées.

    Vous ne pouvez pas modifier un ensemble d'adresses s'il est déjà utilisé. Si vous cliquez sur **Edit** (Modifier) et que l'ensemble d'adresses est utilisé, ASDM affiche un message d'erreur et répertorie les noms de connexion et les noms d'utilisateurs qui utilisent les adresses dans l'ensemble.
  - Pour supprimer un ensemble d'adresses sur l'ASA, choisissez l'entrée dans le tableau et cliquez sur **Delete** (Supprimer).

    Vous ne pouvez pas supprimer un ensemble d'adresses s'il est déjà utilisé. Si vous cliquez sur **Delete** (Supprimer) et que l'ensemble d'adresses est utilisé, ASDM affiche un message d'erreur et répertorie les noms de connexion qui utilisent les adresses de l'ensemble.
- Pour affecter des ensembles d'adresses à une interface, cliquez sur **Add** (Ajouter). La boîte de dialogue Affecter des ensembles d'adresses à l'interface s'ouvre. Sélectionnez l'interface à laquelle un ensemble d'adresses doit être affecté. Cliquez sur **Select** (Sélectionner) à côté du champ Address Pools (Ensembles d'adresses). La boîte de dialogue Sélectionner les ensembles d'adresses s'ouvre. Double-cliquez sur chaque ensemble non affecté que vous souhaitez affecter à l'interface ou choisissez chaque ensemble non affecté et cliquez sur **Assign** (Affecter). Le champ adjacent affiche la liste des affectations

d'ensembles. Cliquez sur **OK** pour remplir le champ Address Pools (Ensembles d'adresses) avec les noms de ces ensembles d'adresses, puis **OK** à nouveau pour terminer la configuration de l'affectation.

- Pour modifier les ensembles d'adresses affectés à une interface, double-cliquez sur l'interface ou choisissez l'interface et cliquez sur **Edit** (Modifier). La boîte de dialogue Affecter des ensembles d'adresses à l'interface s'ouvre. Pour supprimer des ensembles d'adresses, cliquez deux fois sur chaque nom de regroupement et appuyez sur le bouton **Delete** (Supprimer) du clavier. Cliquez sur **Select** (Sélectionner) à côté du champ Address Pools (Ensembles d'adresses) si vous souhaitez affecter des ensembles d'adresses supplémentaires à l'interface. La boîte de dialogue Sélectionner les ensembles d'adresses s'ouvre. Notez que le champ Assign (Affecter) affiche les noms des ensembles d'adresses qui restent affectés à l'interface. Double-cliquez sur chaque ensemble non affecté que vous souhaitez ajouter à l'interface. Le champ Assign (Affecter) met à jour la liste des affectations d'ensembles. Cliquez sur **OK** pour modifier le champ Address Pools (Ensembles d'adresses) avec les noms de ces ensembles d'adresses, puis **OK** à nouveau pour terminer la configuration de l'affectation.
- Pour supprimer une entrée, choisissez l'entrée et cliquez sur **Delete** (Supprimer).

Sujets connexes

Profil de connexion, adressage du client, ajouter ou modifier, à la page 112
Profil de connexion, ensemble d'adresses, à la page 112
Profil de connexion, niveau avancé, ajouter ou modifier un ensemble d'adresses IP, à la page 113

Profil de connexion, adressage du client, ajouter ou modifier

Pour affecter des réserves d'adresses au profil de connexion, sélectionnez **Avancé > Adressage client**, puis sélectionnez **Ajouter** ou **Modifier**.

- Interface : sélectionnez l'interface à laquelle vous souhaitez affecter un ensemble d'adresses. La valeur par défaut est DMZ.
- Address Pools (Ensembles d'adresses) : spécifiez un ensemble d'adresses à affecter à l'interface spécifiée.
- Select (Sélectionner) : ouvre la boîte de dialogue Select Address Pools (Sélectionner des ensembles d'adresses), dans laquelle vous pouvez choisir un ou plusieurs ensembles d'adresses à affecter à cette interface. Votre sélection s'affiche dans le champ Address Pools (Ensembles d'adresses) de la boîte de dialogue Assign Address Pools to Interface (affecter des ensembles d'adresses à l'interface).

Profil de connexion, ensemble d'adresses

La boîte de dialogue Select Address Pools (Sélectionner des réserves d'adresses) dans Profil de connexion > Avancé affiche le nom de la réserve, les adresses de début et de fin, ainsi que le masque de sous-réseau des réserves d'adresses disponibles pour l'affectation d'adresses client. Vous pouvez ajouter, modifier ou supprimer des profils de connexion dans cette liste.

- Add (Ajouter) : ouvre la boîte de dialogue Add IP Pool (Ajouter un ensemble d'adresses IP), dans laquelle vous pouvez configurer un nouvel ensemble d'adresses IP.
- Edit (Modifier) : ouvre la boîte de dialogue Edit IP Pool (Modifier un ensemble d'adresses IP), dans laquelle vous pouvez modifier un ensemble d'adresses IP sélectionné.
- Delete (Supprimer) : supprime l'ensemble d'adresses sélectionné. Il n'y a ni confirmation ni annulation.

- Assign (Affecter) : affiche les noms des ensembles d'adresses qui demeurent affectés à l'interface. Double-cliquez sur chaque ensemble non affecté que vous souhaitez ajouter à l'interface. Le champ Assign (Affecter) met à jour la liste des affectations d'ensembles.

Profil de connexion, niveau avancé, ajouter ou modifier un ensemble d'adresses IP

La boîte de dialogue Ajouter ou Modifier une réserve d'IP dans Profil de connexion > Avancé vous permet de préciser ou de modifier une plage d'adresses IP pour l'affectation d'adresses client.

- Name (Nom) : spécifie le nom affecté à l'ensemble d'adresses IP.
- Starting IP Address (Adresse IP de début) : spécifie la première adresse IP du groupe.
- Ending IP Address (Adresse IP de fin) : spécifie la dernière adresse IP du groupe.
- Subnet Mask (Masque de sous-réseau) : sélectionne le masque de sous-réseau à appliquer aux adresses du groupe.

Profil de connexion Secure Client, attributs d'authentification

Dans l'onglet Connection Profile (Profil de connexion) > Advanced (Avancé) > Authentication (Authentification), vous pouvez configurer les champs suivants :

- Interface-specific Authentication Server Groups (Groupes de serveurs d'authentification spécifiques à l'interface) : gère l'affectation des groupes de serveurs d'authentification à des interfaces spécifiques.
  - Add (Ajouter) ou Edit (Modifier) : ouvre la boîte de dialogue Assign Authentication Server Group to Interface (Affecter un groupe de serveurs d'authentification à une interface), dans laquelle vous pouvez préciser l'interface et le groupe de serveurs, et préciser s'il faut autoriser le retour à la base de données LOCAL en cas d'échec du groupe de serveurs sélectionné. Le bouton Manage (Gérer) dans cette boîte de dialogue ouvre la boîte de dialogue Configure AAA Server Groups (Configurer les groupes de serveurs AAA). Vos sélections s'affichent dans le tableau Interface/Server Group (Interface/Groupe de serveurs).
  - Delete (Supprimer) : supprime le groupe de serveurs sélectionné du tableau. Il n'y a ni confirmation ni annulation.
- Username Mapping from Certificate (Mappage du nom d'utilisateur à partir du certificat) : permet de préciser les méthodes et les champs d'un certificat numérique à partir desquels extraire le nom d'utilisateur.

Remarque Cette fonctionnalité n'est pas prise en charge en mode contexte multiple.

  - Pre-fill Username from Certificate (Préremplir le nom d'utilisateur à partir du certificat) : extrait le nom d'utilisateur du champ de certificat spécifié et l'utilise pour l'authentification et l'autorisation par nom d'utilisateur et mot de passe, en fonction des options suivantes dans ce panneau.
  - Hide username from end user (Masquer le nom d'utilisateur de l'utilisateur final) : spécifie de ne pas afficher le nom d'utilisateur extrait à l'utilisateur final.
  - Use script to choose username (Utiliser un script pour choisir le nom d'utilisateur) : spécifie le nom du script à utiliser pour choisir un nom d'utilisateur dans un certificat numérique. La valeur par défaut est --None (Aucun)--.

- Add or Edit (Ajouter ou Modifier) : ouvre la boîte de dialogue Add or Edit Script Content (Ajouter ou modifier le contenu du script) à utiliser pour mapper le nom d'utilisateur du certificat.
- Delete (Supprimer) : supprime le script sélectionné. Il n'y a ni confirmation ni annulation.
- Use the Entire DN as the Username (Utiliser le DN entier comme nom d'utilisateur) : spécifie que vous souhaitez utiliser l'intégralité du champ Distinguished Name du certificat comme nom d'utilisateur.
- Specify the Certificate Fields to Be Used as the Username (Préciser les champs du certificat à utiliser comme nom d'utilisateur) : spécifie un ou plusieurs champs à combiner dans le nom d'utilisateur.

  Les valeurs possibles pour les attributs principaux et secondaires sont les suivantes :

Attribut	Définition
C	Country (Pays) : l'abréviation du pays à deux lettres. Ces codes sont conformes aux abréviations de pays ISO 3166.
NC	Common Name (Nom commun) : le nom d'une personne, d'un système ou d'une autre entité. Non disponible en tant qu'attribut secondaire.
DNQ	Domain Name Qualifier (Qualificatif du nom de domaine).
CE	E-mail Address (Adresse e-mail).
GENQ	Generational Qualifier (Qualificatif de génération).
GN	Given Name (Prénom).
I	Initials (Initiales).
L	Locality (Localité) : la ville ou la localité où se trouve l'organisation.
N	Name (Nom).
O	Organization (Organisation) : le nom de l'entreprise, de l'établissement, de l'agence, de l'association ou de toute autre entité.
OU	Organizational Unit (Unité organisationnelle) : le sous-groupe dans l'organisation (O).
SER	Numéro de série.
SN	Surname (Nom de famille).
SP	State/Province (État/Province) : l'état ou la province où se trouve l'organisation
T	Title (Titre).
UID	User Identifier (Identifiant d'utilisateur).
UPN	User Principal Name (Nom d'utilisateur principal).

- Primary Field (Champ principal) : sélectionne le premier champ à utiliser dans le certificat pour le nom d'utilisateur. Si cette valeur est trouvée, le champ secondaire est ignoré.

- Secondary Field (Champ secondaire) : sélectionne le champ à utiliser si le champ principal est introuvable.

- Certificate Mapping for Multi-Certificate Authentication (Mappage de certificat pour l'authentification multi-certificat) : gère l'affectation du certificat à utiliser pour l'authentification principale.
  - First Certificate (Premier certificat) : cliquez sur cette option si vous souhaitez que le certificat émis par la machine soit utilisé pour l'authentification principale.
  - Second Certificate (Deuxième certificat) : cliquez sur cette option si vous souhaitez que le certificat utilisateur émis par le client soit utilisé pour l'authentification principale.

- Find (Rechercher) : saisissez une étiquette d'interface graphique ou une commande CLI à utiliser comme chaîne de recherche, puis cliquez sur **Next** (Suivant) ou **Previous** (Précédent) pour commencer la recherche.

Profil de connexion, attributs d'authentification secondaire

Secondary Authentication (Authentification secondaire) sous Connection Profile (Profil de connexion) > Advanced (Avancé) vous permet de configurer l'authentification secondaire, également appelée double authentification. Lorsque l'authentification secondaire est activée, l'utilisateur final doit présenter deux ensembles d'informations d'authentification valides pour se connecter. Vous pouvez utiliser l'authentification secondaire conjointement avec le préremplissage du nom d'utilisateur à partir d'un certificat. Les champs dans cette boîte de dialogue sont similaires à ceux que vous configurez pour l'authentification principale, mais ces champs sont liés uniquement à l'authentification secondaire.

Lorsque la double authentification est activée, ces attributs choisissent un ou plusieurs champs dans un certificat à utiliser comme nom d'utilisateur. La configuration du nom d'utilisateur secondaire à partir de l'attribut de certificat force l'appareil de sécurité à utiliser le champ de certificat spécifié comme deuxième nom d'utilisateur pour la deuxième authentification par nom d'utilisateur/mot de passe.

Remarque Si vous spécifiez également le groupe de serveurs d'authentification secondaire, ainsi que le nom d'utilisateur secondaire du certificat, seul le nom d'utilisateur principal est utilisé pour l'authentification.

- Secondary Authorization Server Group (Groupe de serveurs d'autorisation secondaire) : spécifie un groupe de serveurs d'autorisation à partir duquel extraire les informations d'authentification secondaires.
  - Server Group (Groupe de serveurs) : sélectionnez un groupe de serveurs d'autorisation à utiliser comme groupe AAA de serveurs secondaires. La valeur par défaut est «none». Le groupe de serveurs secondaire ne peut pas être un groupe de serveurs SDI.
  - Manage (Gérer) : ouvre la boîte de dialogue Configure AAA Server Groups (Configurer les groupes de serveurs AAA).
  - Use LOCAL if Server Group fails (Utiliser LOCAL si le groupe de serveurs échoue) : spécifie d'utiliser la base de données LOCAL comme solution de repli si le groupe de serveurs spécifié échoue.
  - Use primary username (Utiliser le nom d'utilisateur principal) : spécifie que la boîte de dialogue de connexion ne doit demander qu'un seul nom d'utilisateur.

- Attributes Server (Serveur d'attributs) : sélectionnez s'il s'agit du serveur d'attributs principal ou secondaire.

Remarque Si vous spécifiez également un serveur d'autorisation pour ce profil de connexion, les paramètres du serveur d'autorisation prévalent : l'ASA ignore ce serveur d'authentification secondaire.

- Session Username Server (Serveur de nom d'utilisateur de session) : sélectionnez s'il s'agit du serveur de nom d'utilisateur de session principal ou secondaire.

- Interface-Specific Authorization Server Groups (Groupes de serveurs d'autorisation spécifiques à l'interface) : gère l'affectation de groupes de serveurs d'autorisation à des interfaces spécifiques.
  - Add or Edit (Ajouter ou Modifier) : ouvre la boîte de dialogue Assign Authentication Server Group to Interface (Affecter un groupe de serveurs d'authentification à l'interface), dans laquelle vous pouvez spécifier l'interface et le groupe de serveurs, et préciser s'il faut autoriser le retour à la base de données LOCAL en cas d'échec du groupe de serveurs sélectionné. Le bouton Manage (Gérer) dans cette boîte de dialogue ouvre la boîte de dialogue Configure AAA Server Groups (Configurer les groupes de serveurs AAA). Vos sélections s'affichent dans le tableau Interface/Server Group (Interface/Groupe de serveurs).
  - Delete (Supprimer) : supprime le groupe de serveurs sélectionné du tableau. Il n'y a ni confirmation ni annulation.

- Username Mapping from Certificate (Mappage du nom d'utilisateur à partir du certificat) : précisez les champs d'un certificat numérique à partir desquels extraire le nom d'utilisateur.
- Pre-fill Username from Certificate (Préremplir le nom d'utilisateur à partir du certificat) : cochez cette option pour extraire les noms à utiliser pour l'authentification secondaire à partir des champs principal et secondaire spécifiés dans ce panneau. Vous devez configurer la méthode d'authentification pour AAA et les certificats avant de sélectionner cet attribut. Pour ce faire, revenez au panneau Basic (Base) dans la même fenêtre et cochez **Both** (Les deux) à côté de Method (Méthode).
- Hide username from end user (Masquer le nom d'utilisateur de l'utilisateur final) : cochez cette option pour masquer le nom d'utilisateur à utiliser pour l'authentification secondaire de l'utilisateur VPN.
- Fallback when a certificate is unavailable (Utiliser l'option de rechange lorsqu'un certificat n'est pas disponible) : cet attribut n'est configurable que si Hide username from end user (Masquer le nom d'utilisateur de l'utilisateur final) est sélectionné. Utilise les données HostScan (maintenant appelées Secure Firewall Posture) pour préremplir le nom d'utilisateur pour l'authentification secondaire si un certificat n'est pas disponible.
- Password (Mot de passe) : choisissez l'une des méthodes suivantes pour récupérer le mot de passe à utiliser pour l'authentification secondaire :
  - Prompt (Invite) : invitez l'utilisateur à saisir le mot de passe.
  - Use Primary (Utiliser le mot de passe d'authentification principal) : réutilise le mot de passe d'authentification principal pour toutes les authentifications secondaires.
  - Use (Utiliser) : saisissez un mot de passe secondaire commun pour toutes les authentifications secondaires.

- Specify the certificate fields to be used as the username (Préciser les champs de certificat à utiliser comme nom d'utilisateur) : spécifie un ou plusieurs champs à mettre en correspondance comme nom d'utilisateur. Pour utiliser ce nom d'utilisateur dans la fonctionnalité Pre-fill Username from Certificate (Préremplir le nom d'utilisateur à partir du certificat) pour l'authentification ou l'autorisation secondaire de nom d'utilisateur/mot de passe, vous devez également configurer pre-fill-username et secondary-pre-fill-username.
  - Primary Field (Champ principal) : sélectionne le premier champ du certificat à utiliser pour le nom d'utilisateur. Si cette valeur est trouvée, le champ secondaire est ignoré.
  - Secondary Field (Champ secondaire) : sélectionne le champ à utiliser si le champ principal est introuvable.

Les options pour les attributs de champ principal et secondaire sont les suivantes :

Attribut	Définition
C	Country (Pays) : l'abréviation du pays à deux lettres. Ces codes sont conformes aux abréviations de pays ISO 3166.
NC	Common Name (Nom commun) : le nom d'une personne, d'un système ou d'une autre entité. Non disponible en tant qu'attribut secondaire.
DNQ	Domain Name Qualifier (Qualificatif du nom de domaine).
CE	E-mail Address (Adresse e-mail).
GENQ	Generational Qualifier (Qualificatif de génération).
GN	Given Name (Prénom).
I	Initials (Initiales).
L	Locality (Localité) : la ville ou la localité où se trouve l'organisation.
N	Name (Nom).
O	Organization (Organisation) : le nom de l'entreprise, de l'établissement, de l'agence, de l'association ou de toute autre entité.
OU	Organizational Unit (Unité organisationnelle) : le sous-groupe dans l'organisation (O).
SER	Numéro de série.
SN	Surname (Nom de famille).
SP	State/Province (État/Province) : l'état ou la province où se trouve l'organisation
T	Title (Titre).
UID	User Identifier (Identifiant d'utilisateur).
UPN	User Principal Name (Nom d'utilisateur principal).

- Use the entire DN as the username (Utiliser le DN entier comme nom d'utilisateur) : utilise le DN entier du sujet (RFC1779) pour obtenir un nom et une requête d'autorisation à partir d'un certificat numérique.
- Use script to select username (Utiliser le script pour sélectionner le nom d'utilisateur) : nomme le script à partir duquel extraire le nom d'utilisateur d'un certificat numérique. La valeur par défaut est --None (Aucun)--.
  - Add or Edit (Ajouter ou Modifier) : ouvre la boîte de dialogue Add or Edit Script Content (Ajouter ou modifier le contenu du script) à utiliser pour mapper le nom d'utilisateur du certificat.
  - Delete (Supprimer) : supprime le script sélectionné. Il n'y a ni confirmation ni annulation.
- Certificate Mapping for Multi-Certificate Authentication (Mappage de certificat pour l'authentification multi-certificat) : gère l'affectation du certificat à utiliser pour l'authentification secondaire.
  - First Certificate (Premier certificat) : cliquez sur cette option si vous souhaitez que le certificat émis par la machine soit utilisé pour l'authentification secondaire.
  - Second Certificate (Deuxième certificat) : cliquez sur cette option si vous souhaitez que le certificat utilisateur émis par le client soit utilisé pour l'authentification secondaire.

Profil de connexion Secure Client, attributs d'autorisation

La boîte de dialogue Autorisation dans un profil de connexion Secure Client vous permet d'afficher, d'ajouter, de modifier ou de supprimer des groupes de serveurs d'autorisation propres à l'interface. Chaque ligne du tableau dans cette boîte de dialogue affiche l'état d'un groupe de serveurs spécifique à l'interface : le nom de l'interface, le groupe de serveurs associé et si le retour à la base de données locale est activé en cas d'échec du groupe de serveurs sélectionné.

Les champs de ce volet sont identiques pour les profils de connexion Secure Client, IKEv1, IKEv2 et SSL sans client.

- Authorization Server Group (Groupe de serveurs d'autorisation) : spécifie un groupe de serveurs d'autorisation à partir duquel extraire les paramètres d'autorisation.
  - Server Group (Groupe de serveurs) : sélectionne un groupe de serveurs d'autorisation à utiliser. La valeur par défaut est «none».
  - Manage (Gérer) : ouvre la boîte de dialogue Configure AAA Server Groups (Configurer les groupes de serveurs AAA).
  - Users Must Exist in the Authorization Database to Connect (Les utilisateurs doivent exister dans la base de données d'autorisation pour se connecter) : cochez cette case pour exiger que les utilisateurs répondent à ce critère
- Interface-Specific Authorization Server Groups (Groupes de serveurs d'autorisation spécifiques à l'interface) : gère l'affectation de groupes de serveurs d'autorisation à des interfaces spécifiques.
  - Add or Edit (Ajouter ou Modifier) : ouvre la boîte de dialogue Assign Authentication Server Group to Interface (Affecter un groupe de serveurs d'authentification à l'interface), dans laquelle vous pouvez spécifier l'interface et le groupe de serveurs, et préciser s'il faut autoriser le retour à la base de données LOCAL en cas d'échec du groupe de serveurs sélectionné. Le bouton Manage (Gérer) dans cette boîte de dialogue ouvre la boîte de dialogue Configure AAA Server Groups (Configurer

les groupes de serveurs AAA). Vos sélections s'affichent dans le tableau Interface/Server Group (Interface/Groupe de serveurs).

- Delete (Supprimer) : supprime le groupe de serveurs sélectionné du tableau. Il n'y a ni confirmation ni annulation.

- Username Mapping from Certificate (Mappage du nom d'utilisateur à partir du certificat) : précisez les champs d'un certificat numérique à partir desquels extraire le nom d'utilisateur.
  - Use Script to Select Username (Utiliser un script pour sélectionner le nom d'utilisateur) : spécifie le nom d'un script à utiliser pour choisir un nom d'utilisateur à partir d'un certificat numérique. La valeur par défaut est --None (Aucun)--. Pour plus d'informations sur la création de scripts afin de sélectionner créer un nom d'utilisateur à partir des champs de certificat, consultez
  - Add or Edit (Ajouter ou Modifier) : ouvre la boîte de dialogue Add or Edit Script Content (Ajouter ou modifier le contenu du script) à utiliser pour mapper le nom d'utilisateur du certificat.
  - Delete (Supprimer) : supprime le script sélectionné. Il n'y a ni confirmation ni annulation.
  - Use the Entire DN as the Username (Utiliser le DN entier comme nom d'utilisateur) : spécifie que vous souhaitez utiliser l'intégralité du champ Distinguished Name du certificat comme nom d'utilisateur.
  - Specify the Certificate Fields to Be Used as the Username (Préciser les champs du certificat à utiliser comme nom d'utilisateur) : spécifie un ou plusieurs champs à combiner dans le nom d'utilisateur.
  - Primary Field (Champ principal) : sélectionne le premier champ du certificat à utiliser pour le nom d'utilisateur. Si cette valeur est trouvée, le champ secondaire est ignoré.
  - Secondary Field (Champ secondaire) : sélectionne le champ à utiliser si le champ principal est introuvable.

- Find (Rechercher) : saisissez une étiquette d'interface graphique ou une commande CLI à utiliser comme chaîne de recherche, puis cliquez sur Next (Suivant) ou Previous (Précédent) pour commencer la recherche.

Profil de connexion Secure Client, autorisation, ajouter le contenu du script pour sélectionner le nom d'utilisateur

Si vous sélectionnez **Use a script to select username** (Utiliser un script pour sélectionner le nom d'utilisateur) dans le volet Authorization (Autorisation) de Secure Client et que vous cliquez sur le bouton Add or Edit (Ajouter ou Modifier), vous verrez les champs suivants.

Les scripts peuvent utiliser des champs de certificat pour l'autorisation qui ne sont pas répertoriés dans les autres options de mappage.

Remarque Secure Client et le WebVPN sans client affichent « Inconnu » dans le champ du nom d'utilisateur lorsque le préremplissage du nom d'utilisateur à partir du certificat à l'aide d'un script ne parvient pas à trouver le nom d'utilisateur dans le certificat client.

- Script Name (Nom du script) : spécifiez le nom du script. Le nom du script doit être le même dans les versions d'autorisation et d'authentification. Vous définissez le script ici, et l'interface de ligne de commande utilise le même script pour effectuer cette fonction.

- Select script parameters (Sélectionner les paramètres de script) : spécifiez les attributs et le contenu du script.
- Value for Username (Valeur pour le nom d'utilisateur) : sélectionnez un attribut dans la liste déroulante des attributs DN standard à utiliser comme nom d'utilisateur (DN de l'objet).
- No Filtering (Aucun filtrage) : spécifiez que vous souhaitez utiliser le nom distinctif complet spécifié.
- Filter by substring (Filtrer par sous-chaîne) : spécifiez l'index de départ (la position dans la chaîne du premier caractère à mettre en correspondance) et l'index de fin (nombre de caractères à rechercher). Si vous choisissez cette option, l'index de départ ne peut pas être vide. Si vous laissez l'index de fin vide, la valeur par défaut est -1, indiquant que la chaîne complète est analysée pour une correspondance.

  Par exemple, supposons que vous ayez sélectionné l'attribut DN Common Name (CN) (Nom commun [CN]), qui contient une valeur hôte/utilisateur. Le tableau suivant présente quelques manières possibles de filtrer cette valeur à l'aide de l'option sous-chaîne pour obtenir diverses valeurs de retour. La valeur de retour est ce qui est réellement prérempli comme nom d'utilisateur.

Tableau 4 : Filtrage par sous-chaîne

Index de départ	Index de fin	Valeur de retour
1	5	hôte/
6	10	utilisateur
6	-1	utilisateur

L'utilisation d'un index négatif, comme dans la troisième ligne de ce tableau, spécifie de compter à partir de la fin de la chaîne vers l'arrière jusqu'à la fin de la sous-chaîne, dans ce cas, le « r » de « user ».

Lorsque vous utilisez le filtrage par sous-chaîne, vous devez connaître la longueur de la sous-chaîne que vous recherchez. Dans les exemples suivants, utilisez soit la mise en correspondance d'expressions régulières, soit le script personnalisé au format Lua :

- Exemple 1 : correspondance d'expression régulière : saisissez une expression régulière à appliquer à la recherche dans le champ Regular Expression (Expression régulière). Les opérateurs d'expression régulière standard s'appliquent. Par exemple, supposons que vous souhaitiez utiliser une expression régulière pour filtrer tout ce qui précède le symbole @ de la valeur DN « Adresse courriel (EA) ». L'expression régulière ^[^@]* serait une façon de le faire. Dans cet exemple, si la valeur DN contient la valeur user1234@example.com, la valeur de retour après l'expression régulière sera user1234.
- Exemple 2 : utiliser un script personnalisé au format LUA : spécifiez un script personnalisé écrit dans le langage de programmation LUA pour analyser les champs de recherche. La sélection de cette option met à disposition un champ dans lequel vous pouvez saisir votre script LUA personnalisé; par exemple, le script :

```
return cert.subject.cn..'/'..cert.subject.l
```

  combine deux champs DN, le nom d'utilisateur (cn) et la localité (l), pour les utiliser comme nom d'utilisateur unique et insère le caractère barre oblique (/) entre les deux champs.

  Le tableau ci-dessous répertorie les noms et les descriptions des attributs que vous pouvez utiliser dans un script LUA.

Remarque LUA est sensible à la casse.

Tableau 5 : Noms et descriptions des attributs

Nom de l'attribut	Description
cert.subject.c	Pays
cert.subject.cn	Nom usuel
cert.subject.dnq	DN qualifier (Qualificatif du DN)
cert.subject.ea	Adresse courriel
cert.subject.genq	Qualificateur de génération
cert.subject.gn	Prénom
cert.subject.i	Initiales
cert.subject.l	Localité
cert.subject.n	Nom
cert.subject.o	Organisation
cert.subject.ou	Unité d'organisation
cert.subject.ser	Numéro de série du sujet
cert.subject.sn	Nom
cert.subject.sp	État ou Province
cert.subject.t	Titre
cert.subject.uid	Identifiant utilisateur
cert.issuer.c	Pays
cert.issuer.cn	Nom usuel
cert.issuer.dnq	DN qualifier (Qualificatif du DN)
cert.issuer.ea	Adresse courriel
cert.issuer.genq	Qualificateur de génération
cert.issuer.gn	Prénom
cert.issuer.i	Initiales
cert.issuer.l	Localité

cert.issuer.n	Nom
cert.issuer.o	Organisation
cert.issuer.ou	Unité d'organisation
cert.issuer.ser	Numéro de série de l'émetteur
cert.issuer.sn	Nom
cert.issuer.sp	État ou Province
cert.issuer.t	Titre
cert.issuer.uid	Identifiant utilisateur
cert.serialnumber	Numéro de série du certificat
cert.subjectaltname.upn	Nom d'utilisateur principal

Si une erreur se produit lors de l'activation d'un script de groupe de tunnels et empêche le script de s'activer, la console de l'administrateur affiche un message d'erreur.

Profils de connexion, Comptabilité

Le volet Accounting (Comptabilité) dans Connection Profile > Advanced (Profil de connexion > Avancé) définit les options de comptabilité globalement dans l'ASA.

- Accounting Server Group (Groupe de serveurs de comptabilité) : choisissez le groupe de serveurs défini précédemment à utiliser pour la comptabilité.
- Manage (Gérer) : ouvre la boîte de dialogue Configure AAA Server Groups (Configurer les groupes de serveurs AAA), dans laquelle vous pouvez créer un groupe de serveurs AAA.

Profil de connexion, alias de groupe et URL de groupe

La boîte de dialogue GroupAlias/Group URL dans Connection Profile (Profil de connexion) > Advanced (Avancé) configure les attributs qui affectent ce que l'utilisateur distant voit lors de la connexion.

Le nom de l'onglet dans le profil de connexion est Group URL/Group Alias pour Secure Client.

- **Login and Logout (Portal) Page Customization (Clientless SSL VPN only) (Personnalisation de la page de connexion et de déconnexion [portail]** [VPN SSL sans client uniquement]) : configure l'apparence de la page de connexion utilisateur en précisant les attributs de personnalisation préconfigurés à appliquer. La valeur par défaut est DfltCustomization. Cliquez sur **Manage** (Gérer) pour créer un nouvel objet de personnalisation.
- **Enable the display of Radius Reject-Message on the login screen (Activer l'affichage de Radius Reject**-Message sur l'écran de connexion) : cochez cette case pour afficher le message de rejet RADIUS dans la boîte de dialogue de connexion lorsque l'authentification est rejetée.

- **Enable the display of SecurId message on the login screen** (Activer l'affichage du message SecurID sur l'écran de connexion) : cochez cette case pour afficher les messages SecurID dans la boîte de dialogue de connexion.
- **Connection Aliases** (Alias de connexion) : les alias de connexion et leur état. Un alias de connexion s'affiche sur la page de connexion de l'utilisateur si la connexion est configurée pour permettre aux utilisateurs de choisir une connexion particulière (groupe de tunnels) lors de la connexion. Cliquez sur les boutons **Add** (Ajouter) ou **Delete** (Supprimer) pour ajouter ou supprimer des alias. Pour modifier un alias, double-cliquez sur l'alias dans le tableau et modifiez l'entrée. Pour modifier l'état activé, cochez ou désélectionnez la case dans le tableau.
- **Group URLs** (URL de groupe) : les URL de groupe et leur état. Une URL de groupe s'affiche sur la page de connexion de l'utilisateur si la connexion est configurée pour permettre aux utilisateurs de choisir un groupe particulier lors de la connexion. Cliquez sur les boutons **Add** (Ajouter) ou **Delete** (Supprimer) pour ajouter ou supprimer des URL. Pour **Edit** (Modifier) une URL, double-cliquez sur l'URL dans le tableau et modifiez l'entrée. Pour modifier l'état activé, cochez ou décochez la case dans le tableau.

Profils de connexion IKEv1

Les profils de connexion IKEv1 définissent les politiques d'authentification pour les clients VPN natifs et tiers, y compris L2TP-IPsec. Les profils de connexion IKEv1 sont configurés dans le volet **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau (client)) > IPsec(IKEv1) Connection Profiles (Profils de connexion IPsec(IKEv1))**.

- **Access Interfaces** (Interfaces d'accès) : sélectionne les interfaces à activer pour l'accès IPsec. La valeur par défaut est aucun accès.
- **Connection Profiles** (Profils de connexion) : affiche sous forme tabulaire les paramètres configurés pour les connexions IPsec existantes. Le tableau Connections contient des enregistrements qui déterminent les politiques de connexion. Un enregistrement identifie une stratégie de groupe par défaut pour la connexion et contient des paramètres de connexion spécifiques au protocole. Le tableau contient les colonnes suivantes :
  - **Nom** : spécifie le nom ou l'adresse IP de la connexion IPsec IKEv1.
  - **IPsec Enabled** (IPsec activé) : indique si le protocole IPsec est activé. Vous activez ce protocole dans la boîte de dialogue Add (Ajouter) ou Edit (Modifier) IPsec Remote Access Connection (Connexion d'accès à distance IPsec) > Basic (Base).
  - **L2TP/IPsec Enabled** (L2TP/IPsec activé) : indique si le protocole L2TP/IPsec est activé. Vous activez ce protocole dans la boîte de dialogue Add (Ajouter) ou Edit (Modifier) IPsec Remote Access Connection (Connexion d'accès à distance IPsec) > Basic (Base).
  - **Authentication Server Group (Groupe de serveurs d'authentification)** : nom du groupe de serveurs qui peuvent fournir l'authentification.
  - **Group Policy (Stratégie de groupe)** : indique le nom de la stratégie de groupe pour cette connexion IPsec.

Remarque Delete (Supprimer) : supprime le groupe de serveurs sélectionné du tableau. Il n'y a ni confirmation ni annulation.

Profil de connexion d'accès à distance IPsec, onglet Basic (Base)

La boîte de dialogue Add or Edit IPsec Remote Access Connection Profile Basic (Ajouter ou modifier un profil de connexion d'accès à distance IPsec de base) sous **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > IPsec(IKEv1) Connection Profiles (Profils de connexion IPsec [IKEv1]) > Add/Edit (Ajouter/Modifier) > Basic (Base)** vous permet de configurer les attributs communs des connexions VPN IPsec IKEv1, y compris L2TP-IPsec.

- **Name** (Nom) : nom de ce profil de connexion.
- **IKE Peer Authentication** (Authentification d'homologue IKE) : configure les homologues IKE.
  - **Pre-shared key** (Clé prépartagée) : spécifie la valeur de la clé prépartagée pour la connexion. La longueur maximale de la clé partagée est de 128 caractères.
  - **Identity Certificate** (Certificat d'identité) : sélectionne le nom d'un certificat d'identité, si des certificats d'identité sont configurés et inscrits. **Manage** (Gérer) ouvre la boîte de dialogue **Manage Identity Certificates** (Gérer les certificats d'identité), dans laquelle vous pouvez ajouter, modifier, supprimer, exporter et afficher les détails d'un certificat sélectionné.
- **User Authentication** (Authentification de l'utilisateur) : spécifie les renseignements sur les serveurs utilisés pour l'authentification des utilisateurs. Vous pouvez configurer davantage de renseignements d'authentification dans la section Advanced (Avancé).
  - **Server Group** (Groupe de serveurs) : sélectionne le groupe de serveurs à utiliser pour l'authentification des utilisateurs. La valeur par défaut est LOCAL. Si vous sélectionnez une valeur autre que LOCAL, la case Fallback (Repli) devient disponible. Pour ajouter un groupe de serveurs, cliquez sur le bouton **Manage** (Gérer).
  - **Fallback** (Repli) : spécifie s'il faut utiliser LOCAL pour l'authentification des utilisateurs en cas d'échec du groupe de serveurs spécifié.
- **Client Address Assignment** (Affectation d'adresses client) : spécifie les attributs pertinents pour l'affectation d'attributs client.
  - **DHCP Servers** (Serveurs DHCP) : spécifie l'adresse IP d'un serveur DHCP à utiliser. Vous pouvez ajouter jusqu'à 10 serveurs, séparés par des espaces.
  - **Client Address Pools** (Ensembles d'adresses client) : spécifie jusqu'à 6 ensembles d'adresses prédéfinis. Pour définir un ensemble d'adresses, cliquez sur le bouton **Select** (Sélectionner).
- **Default Group Policy** (Stratégie de groupe par défaut) : spécifie les attributs pertinents de la stratégie de groupe par défaut.
  - **Group Policy** (Stratégie de groupe) : sélectionne la stratégie de groupe par défaut à utiliser pour cette connexion. La valeur par défaut est DfltGrpPolicy. Pour définir une nouvelle stratégie de groupe à associer à cette stratégie de groupe, cliquez sur **Manage**.

- **Enable IPsec protocol** (Activer le protocole IPsec) et **Enable L2TP over IPsec protocol** (Activer le protocole L2TP sur IPsec) : sélectionne le ou les protocoles à utiliser pour cette connexion.

Ajouter/modifier les connexions d'accès à distance, avancé, général

Utilisez cette boîte de dialogue pour préciser s'il faut supprimer le domaine et le groupe du nom d'utilisateur avant de les transmettre au serveur AAA, et pour préciser les paramètres de gestion des mots de passe.

- **Strip the realm from username before passing it on to the AAA server** (Supprimer le domaine du nom d'utilisateur avant de le transmettre au serveur AAA) : active ou désactive la suppression du domaine (domaine administratif) du nom d'utilisateur avant de transmettre ce nom au serveur AAA. Cochez la case Strip Realm (Supprimer le domaine) pour supprimer le qualificateur de domaine du nom d'utilisateur lors de l'authentification. Vous pouvez ajouter le nom de domaine au nom d'utilisateur pour AAA : autorisation, authentification et comptabilité. Le seul délimiteur valide pour un domaine est le caractère @. Le format est nom d'utilisateur@domaine, par exemple, JanDoe@exemple.com. Si vous cochez cette case Strip Realm (Supprimer le domaine), l'authentification est basée uniquement sur le nom d'utilisateur. Sinon, l'authentification est basée sur la chaîne complète de nom d'utilisateur@domaine. Vous devez cocher cette case si votre serveur ne peut pas analyser les délimiteurs.

Remarque Vous pouvez ajouter le domaine et le groupe à un nom d'utilisateur. Si c'est le cas, l'ASA utilise les paramètres configurés pour le groupe et le domaine pour les fonctions AAA. Le format de cette option est nom d'utilisateur[@realm]]<#or!>group], par exemple, JanDoe@example.com#VPNGroup. Si vous choisissez cette option, vous devez utiliser le caractère # ou ! pour le délimiteur de groupe, car l'ASA ne peut pas interpréter le @ comme un délimiteur de groupe s'il est également présent comme délimiteur de domaine.

L'ASA ne prend pas en charge l'utilisateur@groupolicy. Seul le client L2TP/IPsec prend en charge la commutation de tunnel par l'intermédiaire de user@tunnelgroup.

- **Strip the group from the username before passing it on to the AAA server** (Supprimer le groupe du nom d'utilisateur avant de le transmettre au serveur AAA) : active ou désactive la suppression du nom de groupe du nom d'utilisateur avant de transmettre ce nom au serveur AAA. Cochez la case Strip Group (Supprimer le groupe) pour supprimer le nom du groupe du nom d'utilisateur lors de l'authentification. Cette option n'est significative que lorsque vous avez également coché la case Enable Group Lookup (Activer la recherche de groupe). Lorsque vous ajoutez un nom de groupe à un nom d'utilisateur à l'aide d'un délimiteur et que vous activez la recherche de groupe, l'ASA interprète tous les caractères à gauche du délimiteur comme nom d'utilisateur et ceux à droite comme nom de groupe. Les délimiteurs de groupe valides sont le @, le # et le ! caractères, en utilisant le caractère @ comme caractère par défaut pour la recherche de groupe. Vous ajoutez le groupe au nom d'utilisateur dans le format nom d'utilisateur<delimiter>groupe, les possibilités étant, par exemple, JaneDoe@VPNGroup, JaneDoe#VPNGroup et JaneDoe!VPNGroup.

- **Password Management (Gestion des mots de passe)** : vous permet de configurer les paramètres pertinents pour remplacer une indication de compte désactivé provenant d'un serveur AAA et pour informer les utilisateurs de l'expiration du mot de passe.

- **Enable notification upon password expiration to allow user to change password** (Activer la notification à l'expiration du mot de passe pour permettre à l'utilisateur de modifier le mot de passe) : en cochant cette case, les deux paramètres suivants deviennent disponibles. Vous pouvez choisir soit d'aviser l'utilisateur lors de la connexion un nombre précis de jours avant l'expiration du mot de passe, soit de l'aviser uniquement le jour de l'expiration du mot de passe. La valeur par défaut est d'envoyer une notification à l'utilisateur 14 jours avant l'expiration du mot de passe et chaque jour par la suite jusqu'à ce que l'utilisateur modifie le mot de passe. La plage est comprise entre 1 et 180 jours.

Remarque Cela ne modifie pas le nombre de jours avant l'expiration du mot de passe, mais active la notification. Si vous choisissez cette option, vous devez également préciser le nombre de jours.

Dans les deux cas, et, si le mot de passe expire sans être modifié, l'ASA offre 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.

Ce paramètre est valide pour les serveurs AAA qui prennent en charge une telle notification; c'est-à-dire, RADIUS, RADIUS avec un serveur NT et des serveurs LDAP. L'ASA ignore cette commande si l'authentification RADIUS ou LDAP n'a pas été configurée.

Cette fonctionnalité nécessite l'utilisation de MS-CHAPv2.

Adressage de client IKEv1

La configuration de l'adressage client est commune pour les profils de connexion client. Consultez Profil de connexion, adressage du client, à la page 111 pour de plus amples renseignements.

Profil de connexion IKEv1, authentification

Cette boîte de dialogue est disponible pour IPsec sur les groupes de tunnels d'accès à distance et de site à site. Les paramètres de cette boîte de dialogue s'appliquent à ce profil de connexion (groupe de tunnels) globalement dans l'ASA. Pour définir les paramètres de groupe de serveurs d'authentification par interface, cliquez sur **Advanced** (Avancé). Cette boîte de dialogue vous permet de configurer les attributs suivants :

- **Authentication Server Group** (Groupe de serveurs d'authentification) : répertorie les groupes de serveurs d'authentification disponibles, y compris le groupe LOCAL (par défaut). Vous pouvez également choisir Aucun. La sélection d'un élément autre que Aucun ou Local rend disponible la case Use LOCAL if Server Group Fails (Utiliser LOCAL si le groupe de serveurs échoue).
- **Use LOCAL if Server Group Fails** (Utiliser LOCAL si le groupe de serveurs échoue) : active ou désactive le retour à la base de données LOCAL si le groupe spécifié par l'attribut Authentication Server Group (Groupe de serveurs d'authentification) échoue.

  Vous pouvez configurer l'authentification sur la base du nom d'utilisateur uniquement en décochant la case Enable Group Lookup (activer la recherche de groupe). Cocher la case Enable Group Lookup (activer la recherche de groupe) et supprimer le groupe vous permet de maintenir une base de données d'utilisateurs avec des noms de groupe ajoutés sur votre serveur AAA et d'authentifier en même temps les utilisateurs en fonction de leur nom d'utilisateur uniquement.

Profil de connexion IKEv1, autorisation

La configuration de l'autorisation est courante pour les profils de connexion client. Consultez Profil de connexion Secure Client, attributs d'authentification, à la page 113 pour de plus amples renseignements.

Profil de connexion IKEv1, comptabilité

La configuration de la comptabilité est courante pour les profils de connexion client. Consultez Profils de connexion, Comptabilité, à la page 122 pour de plus amples renseignements.

Profil de connexion IKEv1, IPsec

Configuration > Remote Access VPN (VPN d'accès distant) > Network (Client) Access (Accès réseau [client]) > IPsec(IKEv1) Connection Profiles (Profils de connexion IPsec [IKEv1]) > Add/Edit (Ajouter/Modifier) > Advanced (Avancé) > IPsec

- **Send Certificate Chain** (Envoyer la chaîne de certificats) : active ou désactive l'envoi de l'ensemble de la chaîne de certificats. Cette action inclut le certificat racine et tous les certificats d'autorité de certification subordonnés dans la transmission.
- **KE Peer ID Validation** (Validation de l'ID d'homologue IKE) : sélectionne si la validation de l'ID d'homologue IKE est ignorée, requise ou vérifiée uniquement si elle est prise en charge par un certificat.
- **IKE Keep Alive** (Maintien de l'activité IKE) : active et configure la surveillance Keepalive ISAKMP.
  - **Disable Keep Alives** (Désactiver les messages Keepalive) : active ou désactive les messages Keepalive ISAKMP.
  - **Monitor Keep Alives** (Surveiller les messages Keepalive) : active ou désactive la surveillance Keepalive ISAKMP. La sélection de cette option rend disponibles les champs Confidence Interval (Intervalle de confiance) et Retry Interval (Intervalle de nouvelle tentative).
  - **Confidence Interval** (Intervalle de confiance) : spécifie l'intervalle de confiance des messages Keepalive ISAKMP. Cet intervalle est le nombre de secondes permettant à un homologue de passer au mode inactif avant de commencer la surveillance Keepalive. L'intervalle minimal est de 10 secondes ; l'intervalle maximal est de 300 secondes. La valeur par défaut pour un groupe d'accès à distance est de 300 secondes.
  - **Retry Interval** (Intervalle de nouvelle tentative) : spécifie le nombre de secondes à attendre entre les nouvelles tentatives de messages Keepalive ISAKMP. La valeur par défaut est de 2 secondes.
  - **Head End Will Never Initiate Keepalive Monitoring** (La tête de réseau ne lancera jamais la surveillance Keepalive) : spécifie que l'ASA du site central ne lance jamais la surveillance Keepalive.

Profil de connexion IKEv1, IPsec, authentification IKE

Configuration > Remote Access VPN (VPN d'accès distant) > Network (Client) Access (Accès réseau [client]) > IPsec(IKEv1) Connection Profiles (Profils de connexion IPsec [IKEv1]) > Add/Edit (Ajouter/Modifier) > Advanced (Avancé) > IPsec > IKE Authentication (Authentification IKE)

- **Default Mode** (Mode par défaut) : vous permet de choisir le mode d'authentification par défaut : none, xauth ou hybrid.

- **Interface-Specific Mode** (Mode spécifique à l'interface) : spécifie le mode d'authentification pour chaque interface.
  - **Add/Edit/Delete** (Ajouter/Modifier/Supprimer) : permet d'ajouter, de modifier ou de supprimer une sélection de paire interface/mode d'authentification dans le tableau Interface/Authentication Modes (Interface/Modes d'authentification).
  - **Interface** : sélectionnez une interface nommée. Les interfaces par défaut sont interne et externe, mais si vous avez configuré un nom d'interface différent, ce nom s'affiche également dans la liste.
  - **Authentication Mode** (Mode d'authentification) : vous permet de choisir le mode d'authentification : none, xauth ou hybrid.

Profil de connexion IKEv1, IPsec, mise à jour du logiciel client

Configuration > Remote Access VPN (VPN d'accès distant) > Network (Client) Access (Accès réseau [client]) > IPsec(IKEv1) Connection Profiles (Profils de connexion IPsec [IKEv1]) > Add/Edit (Ajouter/Modifier) > Advanced (Avancé) > IPsec > Client Software Update (Mise à jour du logiciel client)

Client VPN Software Update Table (Tableau de mise à jour du logiciel VPN client) : répertorie le type de client, les révisions du client VPN et l'URL de l'image pour chaque progiciel logiciel VPN client installé. Pour chaque type de client, vous pouvez préciser les révisions de logiciel client acceptables et l'URL ou l'adresse IP à partir de laquelle télécharger les mises à niveau logicielles, le cas échéant. Le mécanisme de mise à jour des clients (déchiffré en détail dans la boîte de dialogue Mise à jour des clients) utilise ces informations pour déterminer si le logiciel utilisé par chaque client VPN est à un niveau de révision approprié et, le cas échéant, pour fournir un message de notification et un mécanisme de mise à jour aux clients qui exécutent un logiciel obsolète.

- **Client Type** (Type de client) : identifie le type de client VPN.
- **VPN Client Revisions** (Révisions du client VPN) : spécifie le niveau de révision acceptable du client VPN.
- **Location URL** (URL d'emplacement) : spécifie l'URL ou l'adresse IP à partir de laquelle l'image logicielle appropriée du client VPN peut être téléchargée. Pour les clients VPN basés sur des boîtes de dialogue, l'URL doit être de la forme http:// ou https://. Pour ASA 5505 en mode client, l'URL doit être de la forme tftp://.

Profil de connexion IKEv1, PPP

Pour configurer les protocoles d'authentification autorisés pour une connexion PPP à l'aide de ce profil de connexion IKEv1, ouvrez **Configuration > Remote Access VPN (VPN d'accès distant) > Network (Client) Access (Accès réseau [client]) > IPsec(IKEv1) Connection Profiles (Profils de connexion IPsec [IKEv1]) > Add/Edit (Ajouter/Modifier) > Advanced (Avancé) > PPP**.

Cette boîte de dialogue s'applique *uniquement* aux profils de connexion d'accès à distance IPsec IKEv1.

- **CHAP** : active l'utilisation du protocole CHAP pour une connexion PPP.
- **MS-CHAP-V1** : active l'utilisation du protocole MS-CHAP-V1 pour une connexion PPP.
- **MS-CHAP-V2** : active l'utilisation du protocole MS-CHAP-V2 pour une connexion PPP.

- **PAP** : active l'utilisation du protocole PAP pour une connexion PPP.
- **EAP-PROXY** : active l'utilisation du protocole EAP-PROXY pour une connexion PPP. EAP désigne le protocole d'authentification extensible.

Profils de connexion IKEv2

Les profils de connexion IKEv2 définissent l'authentification par protocole EAP, par certificat et par clé prépartagée pour le module VPN AnyConnect des clients Cisco Secure Client. Le panneau de configuration dans ASDM est **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > IPsec (IKEv2) Connection Profiles (Profils de connexion IPsec [IKEv2])**.

- Access Interfaces (Interfaces d'accès) : sélectionne les interfaces à activer pour l'accès IPsec. La valeur par défaut est qu'aucun accès n'est sélectionné.
- Bypass interface access lists for inbound VPN sessions (Contourner les listes d'accès d'interface pour les sessions VPN entrantes) : cochez cette case pour contourner les listes d'accès d'interface pour les sessions VPN entrantes. Les listes d'accès pour la stratégie de groupe et la politique d'utilisateur s'appliquent toujours à tout le trafic.
- Connection Profiles (Profils de connexion) : affiche sous forme tabulaire les paramètres configurés pour les connexions IPsec existantes. Le tableau Profils de connexion contient des enregistrements qui déterminent les politiques de connexion. Un enregistrement identifie une stratégie de groupe par défaut pour la connexion et contient des paramètres de connexion spécifiques au protocole. Le tableau contient les colonnes suivantes :
  - Nom : spécifie le nom ou l'adresse IP de la connexion IPsec.
  - IKEv2 activé : spécifie que le protocole IKEv2 est activé si cette option est cochée.
  - Groupe de serveurs d'authentification : spécifie le nom du groupe de serveurs utilisé pour l'authentification.
  - Stratégies de groupe : indique le nom de la stratégie de groupe pour cette connexion IPsec.

Remarque Supprimer : supprime le groupe de serveurs sélectionné du tableau. Il n'y a ni confirmation ni annulation.

Profil de connexion IPsec IKEv2, onglet Basic (Base)

La boîte de dialogue Add or Edit IPsec Remote Access Connection Profile Basic (Ajouter ou modifier un profil de connexion d'accès à distance IPsec de base) configure les attributs communs des connexions IPsec IKEv2.

- **Name** (Nom) : identifie le nom de la connexion.
- **IKE Peer Authentication** (Authentification d'homologue IKE) : configure les homologues IKE.
  - **Pre-shared key** (Clé prépartagée) : spécifie la valeur de la clé prépartagée pour la connexion. La longueur maximale d'une clé prépartagée est de 128 caractères.

- **Enable Certificate Authentication** (Activer l'authentification par certificat) : vous permet d'utiliser des certificats pour l'authentification si cette option est cochée.
- **Enable peer authentication using EAP** (Activer l'authentification d'homologue à l'aide d'EAP) : vous permet d'utiliser EAP pour l'authentification si cette option est cochée. Vous devez utiliser des certificats pour l'authentification locale si vous cochez cette case.
- **Send an EAP identity request to the client** (Envoyer une demande d'identité EAP au client) : vous permet d'envoyer une demande EAP d'authentification au client VPN d'accès à distance.

- Post Quantum Key (Clé post-quantique) : cochez cette case pour spécifier la clé prépartagée (PPK) post-quantique. PPK est une chaîne hexadécimale de 256 bits et 64 caractères qui protège la session contre les attaques d'ordinateurs quantiques.
  - Post Quantum Key Identity (Identité de la clé post-quantique) : spécifiez l'ID du PPK.

- **Mobike RRC** : active/désactive le RRC mobike.
  - **Enable Return Routability Check for mobike** (Activer la vérification de la routabilité de retour pour mobike) : active/désactive la vérification de la routabilité de retour pour les modifications d'adresses IP dynamiques dans les associations de sécurité IKE/IPsec sur lesquelles mobike est activé.

- **User Authentication** (Authentification de l'utilisateur) : spécifie les renseignements sur les serveurs utilisés pour l'authentification des utilisateurs. Vous pouvez configurer davantage de renseignements d'authentification dans la section Advanced (Avancé).
  - **Server Group** (Groupe de serveurs) : sélectionne le groupe de serveurs à utiliser pour l'authentification des utilisateurs. La valeur par défaut est LOCAL. Si vous choisissez une valeur autre que LOCAL, la case Fallback devient disponible.
  - **Manage** (Gérer) : ouvre la boîte de dialogue Configure AAA Server Groups (Configurer les groupes de serveurs AAA).
  - **Fallback** : spécifie s'il faut utiliser LOCAL pour l'authentification des utilisateurs en cas d'échec du groupe de serveurs spécifié.

- **Client Address Assignment** (Affectation d'adresses client) : spécifie les attributs pertinents pour l'affectation d'attributs client.
  - **DHCP Servers** (Serveurs DHCP) : spécifie l'adresse IP d'un serveur DHCP à utiliser. Vous pouvez ajouter jusqu'à 10 serveurs, séparés par des espaces.
  - **Ensembles d'adresses client** : spécifie jusqu'à 6 ensembles d'adresses prédéfinis. Cliquez sur Select (Sélectionner) pour ouvrir la boîte de dialogue Address Pools (Ensembles d'adresses).

- **Default Group Policy** (Stratégie de groupe par défaut) : spécifie les attributs pertinents de la stratégie de groupe par défaut.
  - **Group Policy** (Stratégie de groupe) : sélectionne la stratégie de groupe par défaut à utiliser pour cette connexion. La valeur par défaut est DfltGrpPolicy.
  - **Manage** (Gérer) : ouvre la boîte de dialogue Configure Group Policies (Configurer les stratégies de groupe), à partir de laquelle vous pouvez ajouter, modifier ou supprimer des stratégies de groupe.

- **Client Protocols** (Protocoles client) : sélectionne le protocole ou les protocoles à utiliser pour cette connexion. Par défaut, IPsec et L2TP sur IPsec sont sélectionnés.
- **Enable IKEv2 Protocol** (Activer le protocole IKEv2) : active le protocole IKEv2 à utiliser dans les profils de connexion d'accès à distance. Il s'agit d'un attribut de la stratégie de groupe que vous venez de sélectionner.

Profil de connexion d'accès à distance IPsec, avancé, onglet IPsec

La table IPsec sur les profils de connexion IPsec (IKEv2) comporte les champs suivants.

- Send certificate chain (Envoyer la chaîne de certificats) : cochez cette option pour activer ou désactiver l'envoi de l'ensemble de la chaîne de certificats. Cette action inclut le certificat racine et tous les certificats d'autorité de certification subordonnés dans la transmission.
- IKE Peer ID Validation (Validation d'ID d'homologue IKE) : choisissez dans la liste déroulante si la validation de l'ID d'homologue IKE n'est pas vérifiée, est requise ou est vérifiée si elle est prise en charge par un certificat.

Mappage des certificats aux profils de connexion IPsec ou SSL VPN

Lorsque l'appareil de sécurité adaptable Cisco reçoit une demande de connexion IPsec avec authentification par certificat client, il attribue un profil de connexion à la connexion en fonction des politiques que vous configurez. Cette politique peut consister à utiliser des règles que vous configurez, le champ OU du certificat, l'identité IKE (c'est-à-dire le nom d'hôte, l'adresse IP, l'ID de clé), l'adresse IP homologue ou un profil de connexion par défaut. Pour les connexions SSL, l'ASA utilise uniquement les règles que vous configurez.

Pour les connexions IPsec ou SSL utilisant des règles, l'ASA évalue les attributs du certificat par rapport aux règles jusqu'à ce qu'il trouve une correspondance. Lorsqu'il trouve une correspondance, il affecte le profil de connexion associé à la règle correspondante à la connexion. S'il ne parvient pas à trouver de correspondance, il attribue le profil de connexion par défaut (DefaultRAGroup pour IPsec et DefaultWebVPNGroup pour SSL VPN) à la connexion et permet à l'utilisateur de choisir le profil de connexion dans une liste déroulante affichée sur la page du portail (s'il est activé). Le résultat de la tentative de connexion une fois dans ce profil de connexion dépend de la validité du certificat et des paramètres d'authentification du profil de connexion.

Une politique de correspondance de groupe de certificats définit la méthode à utiliser pour identifier les groupes d'autorisations des utilisateurs de certificats.

Configurez la politique de correspondance dans le volet Policy (Politique). Si vous choisissez d'utiliser des règles pour la mise en correspondance, accédez au volet Rules (Règles) pour préciser les règles.

Certificat de mappage de profil de connexion, Politique

Pour les connexions IPsec, une politique de mappage de groupe de certificats définit la méthode à utiliser pour identifier les groupes d'autorisations des utilisateurs de certificats. Les paramètres de ces politiques sont configurés dans **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau client) > Advanced (Avancé) > IPsec > Certificate to Connection Profile Maps (Mappages de certificat à profil de connexion) > Policy (Politique)**

- **Use the configured rules to match a certificate to a group** (Utiliser les règles configurées pour faire correspondre un certificat à un groupe) : vous permet d'utiliser les règles que vous avez définies sous Rules (Règles).
- **Use the certificate OU field to determine the group** (Utiliser le champ OU du certificat pour déterminer le groupe) : vous permet d'utiliser le champ d'unité organisationnelle pour déterminer le groupe auquel faire correspondre le certificat. Cette option est sélectionnée par défaut.
- **Use the IKE identity to determine the group** (Utiliser l'identité IKE pour déterminer le groupe) : vous permet d'utiliser l'identité que vous avez précédemment définie sous **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau client) > Advanced (Avancé) > IPsec > IKE Parameters (Paramètres IKE)**. L'identité IKE peut être un nom d'hôte, une adresse IP, un ID de clé ou automatique.
- **Utiliser l'adresse IP homologue pour déterminer le groupe** : vous permet d'utiliser l'adresse IP de l'homologue. Cette option est sélectionnée par défaut.
- **Default to Connection Profile** (Profil de connexion par défaut) : vous permet de choisir un groupe par défaut pour les utilisateurs de certificats qui est utilisé lorsqu'aucune des méthodes précédentes n'a donné de correspondance. Cette option est sélectionnée par défaut. Cliquez sur le groupe par défaut dans la liste Default to group (Par défaut pour le groupe). Le groupe doit déjà exister dans la configuration. Si le groupe ne s'affiche pas dans la liste, vous devez le définir à l'aide de Configuration (**Configuration) > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau client) > Group Policies** (Stratégies de groupe).

Règles de mappage des certificats vers les profils de connexion

Pour les connexions IPsec, une politique de mappage de groupe de certificats définit la méthode à utiliser pour identifier les groupes d'autorisations des utilisateurs de certificats. Les mappages de profils de connexion sont créés dans **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Advanced (Avancé) > IPsec > Certificate to Connection Profile Maps (Mappages des certificats vers les profils de connexion) > Rules (Règles)**.

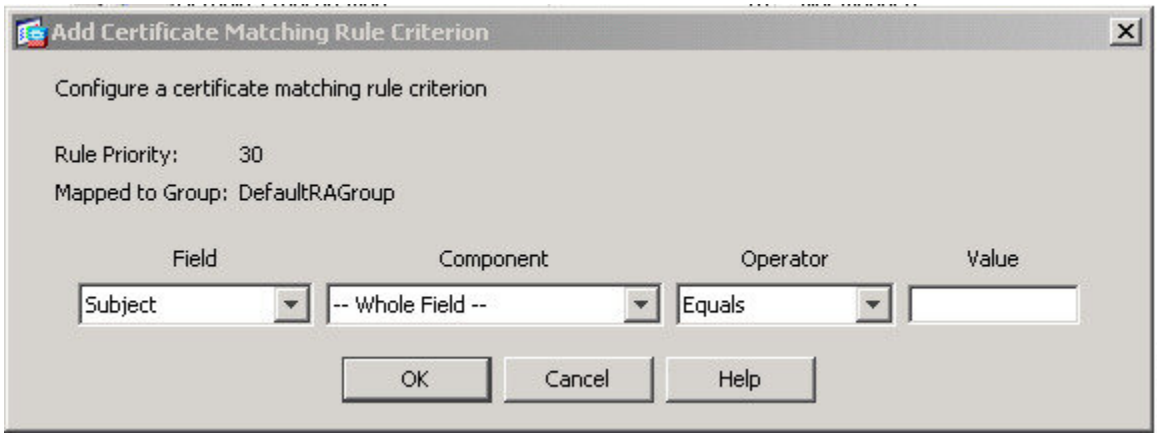
Ce volet comporte une liste des mappages de certificats pour les profils de connexion et des critères de mappage.

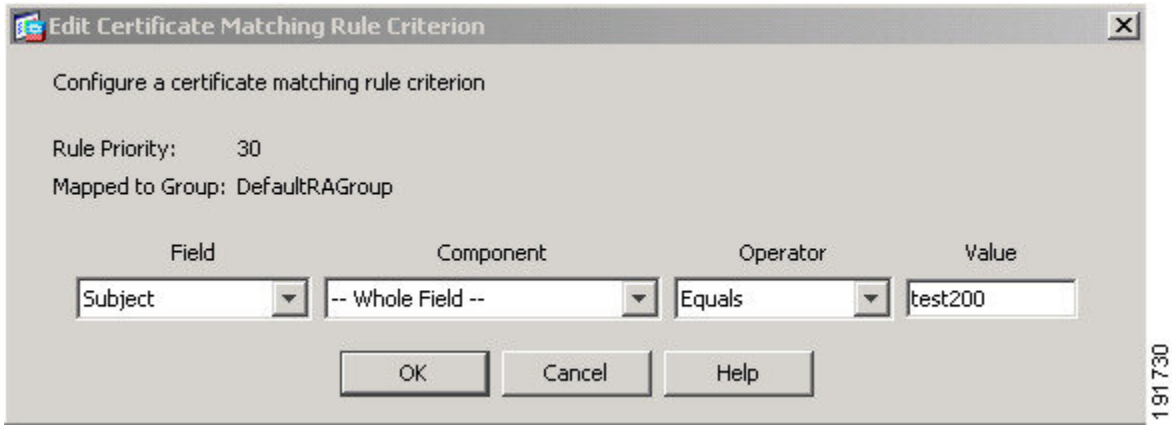
Cartes de profil de connexion et de certificat, ajouter des critères de règle de correspondance de certificat

Créez des profils de mappage pour mapper les profils de connexion aux règles de mappage.

- Mappage : choisissez l'une des options suivantes :
  - Existing (Existant) : sélectionnez le nom de la carte pour inclure la règle.
  - New (Nouveau) : saisissez un nouveau nom de carte pour une règle.
- Priority (Priorité) : saisissez un nombre décimal pour préciser la séquence dans laquelle l'ASA évalue la carte lorsqu'il reçoit une demande de connexion. Pour la première règle définie, la priorité par défaut est 10. L'ASA évalue chaque connexion par rapport à la carte ayant le numéro de priorité le plus bas en premier.
- Mapped to Connection Profile (Mappé au profil de connexion) : sélectionnez le profil de connexion, anciennement appelé « groupe de tunnels », à mapper à cette règle.

Si vous n'affectez pas de critère de règle à la carte, comme décrit dans la section suivante, l'ASA ignore l'entrée de carte.





Ajouter/Modifier les critères de la règle de correspondance de certificat

Utilisez cette boîte de dialogue pour configurer un critère de règle de correspondance de certificat que vous pouvez mapper à un profil de connexion.

- Rule Priority (Priorité de règle) : (affichage uniquement). Séquence avec laquelle l'ASA évalue la carte lorsqu'il reçoit une demande de connexion. L'ASA évalue chaque connexion par rapport à la carte en utilisant le numéro de priorité le plus bas en premier.
- Mapped to Group (Mappé à un groupe) : (affichage uniquement). Profil de connexion auquel la règle est affectée.
- Field (Champ) : sélectionnez la partie du certificat à évaluer dans la liste déroulante.
  - Subject (Sujet : la personne ou le système qui utilise le certificat. Pour un certificat racine d'autorité de certification, le sujet et l'émetteur sont identiques.
  - Alternative Subject (Sujet alternatif) : l'extension des noms alternatifs du sujet permet de lier des identités supplémentaires au sujet du certificat.
  - Issuer (Émetteur) : l'autorité de certification ou une autre entité (instance) qui a émis le certificat.

- Extended Key Usage (Utilisation étendue de la clé) : une extension du certificat client qui fournit d'autres critères que vous pouvez choisir de mettre en correspondance.

- Component (Composant) : (s'applique uniquement si Subject (Sujet) ou Issuer (Émetteur) est sélectionné.) Sélectionnez le composant de nom distinctif utilisé dans la règle :

Champ DN	Définition
Champ entier	Le nom distinctif complet.
Pays (C)	L'abréviation du pays à deux lettres. Ces codes sont conformes aux abréviations de pays ISO 3166.
Nom usuel	Le nom d'une personne, d'un système ou d'une autre entité. Il s'agit du niveau le plus bas (le plus spécifique) dans la hiérarchie d'identification.
DNQ (Qualificatif du DN)	Un attribut de DN spécifique.
Adresses de courriel (EA)	L'adresse courriel de la personne, du système ou de l'entité qui possède le certificat.
Qualificatif générationnel (GENQ)	Un attribut générationnel tel que Jr., Sr. ou III.
Prénom (GN)	Le prénom du propriétaire du certificat.
Initiales (I)	Les premières lettres de chaque partie du nom du propriétaire du certificat.
Localité	La ville ou le gouvernement où se trouve l'organisation.
Nom (N)	Le nom du propriétaire du certificat.
Organisation	Le nom de l'entreprise, de l'établissement, de l'agence, de l'association ou de toute autre entité.
Unité organisationnelle	Le sous-groupe dans l'organisation.
Numéro de série (SER)	Le numéro de série du certificat.
Nom de famille (SN)	Le nom de famille ou le nom de famille du propriétaire du certificat.
État/Province (S/P)	L'état ou la province où se trouve l'organisation.
Titre (T)	Le titre du propriétaire du certificat, par exemple, Dr.
UID (Identifiant de l'utilisateur)	Le numéro d'identification du propriétaire du certificat.
UNAME (Nom non structuré)	Le type d'attribut unstructuredName spécifie le nom ou les noms d'un sujet sous forme d'une chaîne ASCII non structurée.
IP (Adresse IP)	Champ de l'adresse IP.

- Opérateur : sélectionnez l'opérateur utilisé dans la règle :

- Égal à : le champ du nom distinctif doit correspondre exactement à la valeur.
- Contient : le champ du nom distinctif doit inclure la valeur qu'il contient.
- N'est pas égal : le champ du nom distinctif ne doit pas correspondre à la valeur
- Ne contient pas : le champ du nom distinctif ne doit pas inclure la valeur qu'il contient.

- Valeur : saisissez jusqu'à 255 caractères pour préciser l'objet de l'opérateur. Pour Extended Key Usage (Utilisation de clé étendue), choisissez l'une des valeurs prédéfinies dans la liste déroulante, ou vous pouvez saisir des OID pour d'autres extensions. Les valeurs prédéfinies sont les suivantes :

Choix	Objectif d'utilisation de la clé	Chaîne d'OID
clientauth	**Authentification du client**	**1.3.6.1.5.5.7.3.2**
codesigning	Signature de code	1.3.6.1.5.5.7.3.3
emailprotection	Protection de courriel sécurisé	1.3.6.1.5.5.7.3.4
ocspsigning	Signature OCSP	1.3.6.1.5.5.7.3.9
serverauth	Serveur d'authentification	1.3.6.1.5.5.7.3.1
timestamping	Horodatage	1.3.6.1.5.5.7.3.8

Profils de connexion de site à site

La boîte de dialogue Connection Profiles (Profils de connexion) affiche les attributs des profils de connexion de site à site actuellement configurés (groupes de tunnels). Elle vous permet également de choisir le délimiteur à utiliser lors de l'analyse des noms de profils de connexion et d'ajouter, de modifier ou de supprimer des profils de connexion.

L'ASA prend en charge les connexions VPN IPsec de réseau local à réseau local pour IPv4 ou IPv6 en utilisant IKEv1 ou IKEv2 et prend en charge les réseaux internes et externes à l'aide des en-têtes IP internes et externes.

Champs du volet du profil de connexion de site à site

- Access Interfaces (Interfaces d'accès) : affiche un tableau des interfaces de périphérique où vous pouvez activer l'accès par un périphérique homologue distant sur l'interface :
  - Interface : interface du périphérique permettant d'activer ou de désactiver l'accès.
  - Allow IKEv1 Access (Autoriser l'accès IKEv1) : cochez cette option pour activer l'accès IPsec IKEv1 par un périphérique homologue.
  - Allow IKEv2 Access (Autoriser l'accès IKEv2) : cochez cette option pour activer l'accès IPsec IKEv2 par un périphérique homologue.

- Connection Profiles (Profils de connexion) : affiche un tableau des profils de connexion dans lequel vous pouvez ajouter, modifier ou supprimer des profils :
  - Add (Ajouter) : ouvre la boîte de dialogue Add IPsec Site-to-Site Connection Profile (Ajouter un profil de connexion IPsec de site à site).

- Edit (Modifier) : ouvre la boîte de dialogue Edit IPsec Site-to-Site Connection Profile (Modifier le profil de connexion IPsec de site à site).
- Delete (Supprimer) : supprime le profil de connexion sélectionné. Il n'y a ni confirmation ni annulation.
- Name (Nom) : nom du profil de connexion.
- Interface : interface sur laquelle le profil de connexion est activé.
- Local Network (Réseau local) : spécifie l'adresse IP du réseau local.
- Remote Network (Réseau distant) : spécifie l'adresse IP du réseau distant.
- IKEv1 Enabled (IKEv1 activé) : affiche IKEv1 activé pour le profil de connexion.
- IKEv2 Enabled (IKEv2 activé) : affiche IKEv2 activé pour le profil de connexion.
- Group Policy (Stratégies de groupe) : affiche la stratégie de groupe par défaut du profil de connexion.

Ajouter ou modifier un profil de connexion de site à site

La boîte de dialogue Add or Edit IPsec Site-to-Site Connection (Ajouter ou modifier une connexion IPsec de site à site) vous permet de créer ou de modifier une connexion IPsec de site à site. Ces boîtes de dialogue vous permettent de préciser l'adresse IP de l'homologue (IPv4 ou IPv6), de préciser un nom de connexion, de choisir une interface, de préciser les paramètres d'authentification d'homologue et d'utilisateur IKEv1 et IKEv2, de préciser les réseaux protégés et de préciser les algorithmes de chiffrement.

Remarque Lorsque vous créez un profil de connexion VPN de site à site, ouvrez le profil de connexion, puis annulez-le sans apporter de modifications à la configuration. Si vous voyez le bouton Apply (Appliquer) en surbrillance, ignorez les modifications.

L'ASA prend en charge les connexions VPN de réseau local (LAN) à Cisco ou à des homologues tiers lorsque les deux homologues ont des réseaux internes et externes IPv4 (adresses IPv4 sur les interfaces interne et externe).

Pour les connexions de réseau local à réseau local utilisant un adressage mixte IPv4 et IPv6, ou un adressage entièrement IPv6, l'appareil de sécurité prend en charge les tunnels VPN si les deux homologues sont des ASA et si les deux réseaux internes utilisent des schémas d'adressage correspondants (IPv4 ou IPv6).

Plus précisément, les topologies suivantes sont prises en charge lorsque les deux homologues sont des ASA :

- Les ASA ont des réseaux internes IPv4 et le réseau externe est IPv6 (adresses IPv4 sur les interfaces internes et adresses IPv6 sur les interfaces externes).
- Les ASA ont des réseaux internes IPv6 et le réseau externe est IPv4 (adresses IPv6 sur l'interface interne et adresses IPv4 sur les interfaces externes).
- Les ASA ont des réseaux internes IPv6 et le réseau externe est IPv6 (adresses IPv6 sur les interfaces interne et externe).

Champs du panneau de base

- Peer IP Address (Adresse IP homologue) : vous permet de spécifier une adresse IP (IPv4 ou IPv6) et si cette adresse est statique.
- onnection Name (Nom de connexion) :spécifie le nom affecté à ce profil de connexion. Pour la fonction d'édition, ce champ est d'affichage uniquement. Vous pouvez spécifier que le nom de la connexion est le même que l'adresse IP spécifiée dans le champ Adresse IP homologue.
- Interface : sélectionne l'interface à utiliser pour cette connexion.
- Protected Networks (Réseaux protégés) : sélectionne ou spécifie les réseaux locaux et distants protégés pour cette connexion.
  - IP Address Type (Type d'adresse IP) : spécifie que l'adresse est une adresse IPv4 ou IPv6.
  - Local Network (Réseau local) : spécifie l'adresse IP du réseau local.
  - ... : ouvre la boîte de dialogue Browse Local Network (Parcourir le réseau local), dans laquelle vous pouvez choisir un réseau local.
  - Remote Network (Réseau distant) : spécifie l'adresse IP du réseau distant.
- IPsec Enabling (Activation IPsec) : spécifie la stratégie de groupe pour ce profil de connexion et le protocole d'échange de clés spécifié dans cette stratégie :
  - Group Policy Name (Nom de la stratégie de groupe) : spécifie la stratégie de groupe associée à ce profil de connexion.
  - Manage (Gérer) : ouvre la boîte de dialogue Browse Remote Network (Parcourir le réseau distant), dans laquelle vous pouvez choisir un réseau distant.
  - Enable IKEv1 (Activer IKEv1) : active le protocole d'échange de clés IKEv1 dans la stratégie de groupe spécifiée.
  - Enable IKEv2 (Activer IKEv2) : active le protocole d'échange de clés IKEv2 dans la stratégie de groupe spécifiée.
- IKEv1 Settings tab (Onglet Paramètres IKEv1) : spécifie les paramètres d'authentification et de chiffrement pour IKEv1 :
  - Pre-shared Key (Clé prépartagée) : spécifiez la valeur de la clé prépartagée pour le groupe de tunnels. La longueur maximale de la clé prépartagée est de 128 caractères.
  - Device Certificate (Certificat de périphérique) : spécifie le nom du certificat d'identité, le cas échéant, à utiliser pour l'authentification.
  - Manage (Gérer) : ouvre la boîte de dialogue Manage Identity Certificates (Gérer les certificats d'identité), dans laquelle vous pouvez voir les certificats déjà configurés, ajouter de nouveaux certificats, afficher les détails d'un certificat et modifier ou supprimer un certificat.
  - IKE Policy (Politique IKE) : spécifie un ou plusieurs algorithmes de chiffrement à utiliser pour la proposition IKE.
  - Manage (Gérer) : ouvre la boîte de dialogue Configure IKEv1 Proposals (Configurer les propositions IKEv1).

- IPsec Proposal (Proposition IPsec) : spécifie un ou plusieurs algorithmes de chiffrement à utiliser pour la proposition IPsec IKEv1.

- IKEv2 Settings tab (Onglet Paramètres IKEv2) : spécifie les paramètres d'authentification et de chiffrement pour IKEv2 :
  - Local Pre-shared Key (Clé prépartagée locale) : spécifiez la valeur de la clé prépartagée pour le groupe de tunnels. La longueur maximale est de 128 caractères.
  - Local Device Certificate (Certificat de périphérique local) : spécifie le nom du certificat d'identité, le cas échéant, à utiliser pour l'authentification.
  - Manage (Gérer : ouvre la boîte de dialogue Manage Identity Certificates (Gérer les certificats d'identité), dans laquelle vous pouvez voir les certificats déjà configurés, ajouter de nouveaux certificats, afficher les détails d'un certificat et modifier ou supprimer un certificat.
  - Remote Peer Pre-shared Key (Clé prépartagée de l'homologue distant) : spécifiez la valeur de la clé prépartagée de l'homologue distant pour le groupe de tunnels. La longueur maximale est de 128 caractères.
  - Remote Peer Certificate Authentication (Authentification du certificat de l'homologue distant) : cochez Allowed (Autorisé) pour autoriser l'authentification par certificat pour les connexions IKEv2 de ce profil de connexion.
  - Manage (Gérer) : ouvre la boîte de dialogue Manage CA Certificates (Gérer les certificats d'autorité de certification), dans laquelle vous pouvez afficher les certificats et en ajouter de nouveaux.
  - Pour VTI dynamique :
    - IKEv2 Route Accept Any (Accepter tout l'itinéraire IKEv2) : cochez cette case pour que l'ASA accepte les adresses IP de l'interface de tunnel reçues pendant les échanges IKEv2. Par défaut, cette option est activée.
    - IKEv2 Route Set Interface (Définir l'interface d'itinéraire IKEv2) : cochez cette case pour envoyer l'adresse IP de l'interface de tunnel pendant les échanges IKEv2. Cette option configure la voie de routage dynamique vers l'interface du tunnel de l'homologue et exécute les protocoles de routage dynamique entre le concentrateur et les sites distants sur le tunnel.
  - Enable RSA Signature Hash (Activer le hachage de signature RSA) : cochez cette case pour activer le hachage de signature RSA. RSA est un type de chiffrement.
  - IKE Policy (Politique IKE) : spécifie un ou plusieurs algorithmes de chiffrement à utiliser pour la proposition IKE.
  - Manage (Gérer) : ouvre la boîte de dialogue Configure IKEv1 Proposals (Configurer les propositions IKEv1).
  - Proposition IPsec : spécifie un ou plusieurs algorithmes de chiffrement à utiliser pour la proposition IPsec IKEv1.
  - Sélectionner : ouvre la boîte de dialogue Sélectionner les propositions IPsec (ensembles Transform), où vous pouvez affecter une proposition au profil de connexion pour les connexions IKEv2.

Ce profil de connexion comporte également les paramètres suivants :

- Advanced (Avancé) > Crypto Map Entry (Entrée de carte de chiffrement). Pour en savoir plus, consultez Profil de connexion de site à site, entrée de carte de chiffrement, à la page 142.
- Advanced (Avancé) > Tunnel Group (Groupe de tunnels). Pour en savoir plus, consultez Groupe de tunnels de profil de connexion de site à site, à la page 143.

Groupes de tunnels de site à site

Le volet ASDM **Configuration > Site-to-Site VPN (VPN de site à site) > Advanced (Avancé) > Tunnel Groups (Groupes de tunnels)** spécifie les attributs des profils de connexion IPsec de site à site (groupes de tunnels). En outre, vous pouvez choisir les paramètres d'authentification des homologues et des utilisateurs IKE, configurer la surveillance Keepalive IKE et choisir une stratégie de groupe par défaut.

- Name (Nom) : spécifie le nom attribué à ce groupe de tunnels. Pour la fonction d'édition, ce champ est d'affichage uniquement.
- IKE Authentication (Authentification IKE) : spécifie la clé prépartagée et les paramètres de certificat d'identité à utiliser lors de l'authentification d'un homologue IKE.
  - Pre-shared Key (Clé prépartagée) : spécifiez la valeur de la clé prépartagée pour le groupe de tunnels. La longueur maximale est de 128 caractères.
  - Identity Certificate (Certificat d'identité) : spécifie le nom du certificat d'identité à utiliser pour l'authentification, le cas échéant.
  - Manage (Gérer) : ouvre la boîte de dialogue Manage Identity Certificates (Gérer les certificats d'identité), dans laquelle vous pouvez voir les certificats déjà configurés, ajouter de nouveaux certificats, afficher les détails d'un certificat et modifier ou supprimer un certificat.
  - IKE Peer ID Validation (Validation de l'ID d'homologue IKE) : spécifie s'il faut vérifier la validation de l'ID d'homologue IKE. La valeur par défaut est Required (Obligatoire).
- IPsec Enabling (Activation IPsec) : spécifie la stratégie de groupe pour ce profil de connexion et le protocole d'échange de clés spécifié dans cette politique :
  - Group Policy Name (Nom de la stratégie de groupe) : spécifie la stratégie de groupe associée à ce profil de connexion.
  - Manage (Gérer) : ouvre la boîte de dialogue Browse Remote Network (Parcourir le réseau distant), dans laquelle vous pouvez choisir un réseau distant.
  - Enable IKEv1 (Activer IKEv1) : active le protocole d'échange de clés IKEv1 dans la stratégie de groupe précisée.
  - Enable IKEv2 (Activer IKEv2) : active le protocole d'échange de clés IKEv2 dans la stratégie de groupe précisée.
- IKEv1 Settings (Paramètres IKEv1) : spécifie les paramètres d'authentification et de chiffrement pour IKEv1 :
  - Pre-shared Key (Clé prépartagée) : spécifiez la valeur de la clé prépartagée pour le groupe de tunnels. La longueur maximale est de 128 caractères.
  - Certificat de périphérique : spécifie le nom du certificat d'identité, le cas échéant, à utiliser pour l'authentification.

Remarque Certains profils peuvent ne pas être en mesure de déterminer s'il s'agit d'un accès à distance ou d'une connexion LAN à 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*).

- Manage (Gérer) : ouvre la boîte de dialogue Manage Identity Certificates (Gérer les certificats d'identité), dans laquelle vous pouvez voir les certificats déjà configurés, ajouter de nouveaux certificats, afficher les détails d'un certificat et modifier ou supprimer un certificat.
- IKE Policy (Politique IKE) : spécifie un ou plusieurs algorithmes de chiffrement à utiliser pour la proposition IKE.
- Manage (Gérer) : ouvre la boîte de dialogue Configure IKEv1 Proposals (Configurer les propositions IKEv1).
- IPsec Proposal (Proposition IPsec) : spécifie un ou plusieurs algorithmes de chiffrement à utiliser pour la proposition IPsec IKEv1.

- IKEv2 Settings (Paramètres IKEv2) : spécifie les paramètres d'authentification et de chiffrement pour IKEv2 :
  - Local Pre-shared Key (Clé prépartagée locale) : spécifiez la valeur de la clé prépartagée pour le groupe de tunnels. La longueur maximale est de 128 caractères.
  - Local Device Certificate (Certificat de périphérique local) : spécifie le nom du certificat d'identité, le cas échéant, à utiliser pour l'authentification.
  - Manage (Gérer) : ouvre la boîte de dialogue Manage Identity Certificates (Gérer les certificats d'identité), dans laquelle vous pouvez voir les certificats déjà configurés, ajouter de nouveaux certificats, afficher les détails d'un certificat et modifier ou supprimer un certificat.
  - Remote Peer Pre-shared Key (Clé prépartagée de l'homologue distant) : spécifiez la valeur de la clé prépartagée de l'homologue distant pour le groupe de tunnels. La longueur maximale est de 128 caractères.
  - Remote Peer Certificate Authentication (Authentification du certificat d'homologue distant) : cochez la case Allowed (Autorisé) pour autoriser l'authentification des certificats pour les connexions IKEv2 pour ce profil de connexion.
  - Manage (Gérer) : ouvre la boîte de dialogue Manage CA Certificates (Gérer les certificats d'autorité de certification), où vous pouvez afficher les certificats et en ajouter de nouveaux.
  - Politique IKE : spécifie un ou plusieurs algorithmes de chiffrement à utiliser pour la proposition IKE.
  - Manage (Gérer) : ouvre la boîte de dialogue Configure IKEv1 Proposals (Configurer les propositions IKEv1).
  - IPsec Proposal (Proposition IPsec) : spécifie un ou plusieurs algorithmes de chiffrement à utiliser pour la proposition IPsec IKEv1.

- Select (Sélectionner) : ouvre la boîte de dialogue Select IPsec Proposals (Transform Sets) (Sélectionner les propositions IPsec [ensembles Transform]), où vous pouvez affecter une proposition au profil de connexion pour les connexions IKEv2.
- Pour le VTI dynamique :
  - IKEv2 Route Accept Any (Accepter tout l'itinéraire IKEv2) : cochez cette case pour que l'ASA accepte les adresses IP de l'interface de tunnel reçues pendant les échanges IKEv2. Par défaut, cette option est activée.
  - IKEv2 Route Set Interface (Définir l'interface d'itinéraire IKEv2) : cochez cette case pour envoyer l'adresse IP de l'interface de tunnel pendant les échanges IKEv2. Cette option configure la voie de routage dynamique vers l'interface du tunnel de l'homologue et exécute les protocoles de routage dynamique entre le concentrateur et les sites distants sur le tunnel.

- IKE Keepalive : active et configure la surveillance Keepalive IKE. Vous ne pouvez choisir qu'un seul des attributs suivants.
  - Disable Keep Alives (Désactiver Keep Alives) : active ou désactive les messages keepalive IKE.
  - Monitor Keep Alives (Surveillance Keep Alives) : active ou désactive la surveillance Keepalive IKE. La sélection de cette option rend disponibles les champs Intervalle de confiance et Intervalle de nouvelle tentative.
  - Intervalle de confiance : spécifie l'intervalle de confiance de maintien d'activité IKE. Cet intervalle est le nombre de secondes permettant à un homologue de passer au mode inactif avant de commencer la surveillance Keepalive. L'intervalle minimal est de 10 secondes ; l'intervalle maximal est de 300 secondes. La valeur par défaut pour un groupe d'accès à distance est de 10 secondes.
  - Retry Interval (Intervalle de nouvelle tentative) : spécifie le nombre de secondes à attendre entre les nouvelles tentatives de messages Keepalive IKE. La valeur par défaut est de 2 secondes.
  - La tête de réseau ne lancera jamais la surveillance Keepalive : spécifie que l'ASA du site central ne lance jamais la surveillance Keepalive.

- Pour le VTI dynamique : associez un modèle virtuel au groupe de tunnels.
  - Virtual Template (Modèle virtuel) : choisissez un modèle virtuel dans la liste déroulante. 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.

    Pour terminer avec succès la configuration du modèle virtuel, vous devez configurer les paramètres d'interface DVTI suivants (**Configuration > Configuration du périphérique > Paramètres de l'interface > Interfaces > Ajouter > Ajouter l'interface DVTI**
    - Nom d'interface
    - Activer l'interface
    - Activer la superposition d'IP en mode de tunnel pour IPSec (IPv4 ou IPv6)
    - Protection du tunnel avec le profil IPsec

Profil de connexion de site à site, entrée de carte de chiffrement

Dans cette boîte de dialogue, précisez les paramètres cryptographiques pour le profil de connexion de site à site actuel.

- **Priority** (Priorité) : une priorité unique (de 1 à 65 543, 1 étant la priorité la plus élevée). Lorsque la négociation IKE commence, l'homologue qui commence la négociation envoie toutes ses politiques à l'homologue distant, et ce dernier recherche une correspondance avec ses propres politiques, par ordre de priorité.
- **Perfect Forward Secrecy** (Confidentialité persistante) : garantit que la clé d'une SA IPsec donnée n'est dérivée d'aucun autre secret (comme certaines autres clés). Si personne ne parvenait à casser une clé, le protocole PFS garantit que l'agresseur ne pourrait pas obtenir d'autres clés. Si vous activez PFS, la liste des groupes Diffie-Hellman devient active.
  - **Diffie-Hellman Group** (Groupe Diffie-Hellman) : groupe Diffie-Hellman utilisé pour dériver un secret partagé entre deux homologues IPsec sans transmission de ce secret. Les choix sont le groupe 1 (768 bits), le groupe 2 (1 024 bits) et le groupe 5 (1 536 bits).
- **nable NAT-T** (Activer NAT-T) : active la traversée NAT (NAT-T) pour cette politique, ce qui permet aux homologues IPsec d'établir des connexions d'accès à distance et de réseau local à réseau local via un périphérique NAT.
- **Enable Reverse Route Injection** (Activer l'injection de route inverse) : permet l'insertion automatique de routes statiques dans le processus de routage pour les réseaux et les hôtes protégés par un terminal de tunnel distant.
- **Security Association Lifetime** (Durée de vie de l'association de sécurité) : configure la durée de vie d'une association de sécurité (SA). Ce paramètre spécifie comment mesurer la durée de vie des clés de SA IPsec, qui correspond à la durée de vie de la SA IPsec jusqu'à son expiration et doit être renégociée avec de nouvelles clés.
  - **Time** (Temps) : spécifie la durée de vie de la SA en heures (hh), minutes (mm) et secondes (ss).
  - **Traffic Volume** (Volume du trafic) : définit la durée de vie de la SA en fonction du volume de trafic en kilo-octets. Saisissez le nombre de kilo-octets de données de charge utile après lequel la SA IPsec expire. Le minimum est de 100 Ko, la valeur par défaut est de 10 000 Ko, et le maximum est de 2 147 483 647 Ko.
- Static Crypto Map Entry Parameters (Paramètres d'entrée de carte de chiffrement statique) : configurez ces paramètres supplémentaires lorsque Peer IP Address (Adresse IP de l'homologue) est définie comme Static (Statique).
  - Connection Type (Type de connexion) : précisez si la négociation autorisée est bidirectionnelle, avec réponse seulement ou avec origine seulement.
  - Envoyer le certificat d'ID Chain (Chaîne) : permet la transmission de l'ensemble de la chaîne de certificats.
  - IKE Negotiation Mode (Mode de négociation IKE) : définit le mode d'échange des informations de clé pour l'établissement des SA, Main (Principal) ou Aggressive (Agressif). Il définit également le mode utilisé par l'initiateur de la négociation ; le répondeur négocie automatiquement. Le mode agressif est plus rapide, utilise moins de paquets et moins d'échanges, mais il ne protège pas l'identité des parties qui communiquent. Le mode principal est plus lent, utilisant plus de paquets et plus d'échanges, mais il protège les identités des parties qui communiquent. Ce mode est plus sécurisé

et il s'agit de la sélection par défaut. Si vous choisissez Aggressive (Mode agressif), la liste Diffie-Hellman Group (Groupe Diffie-Hellman) devient active.

- Diffie-Hellman Group (Groupe Diffie-Hellman) : groupe Diffie-Hellman utilisé pour dériver un secret partagé entre deux homologues IPsec sans transmission de ce secret. Les choix sont le groupe 1 (768 bits), le groupe 2 (1 024 bits) et le groupe 5 (1 536 bits).

Groupe de tunnels de profil de connexion de site à site

Dans cette boîte de dialogue, précisez les paramètres de groupe de tunnels pour le profil de connexion de site à site actuel.

- Envoyer la chaîne de certificat : active ou désactive l'envoi de l'ensemble de la chaîne de certificats. Cette action inclut le certificat racine et tous les certificats d'autorité de certification subordonnés dans la transmission.
- Validation de l'ID d'homologue IKE : sélectionne si la validation de l'ID d'homologue IKE est ignorée, requise ou vérifiée uniquement si elle est prise en charge par un certificat.
- IKE Keepalive : active et configure la surveillance IKE Keepalive. Vous ne pouvez choisir qu'un seul des attributs suivants.
  - Disable Keep Alives (Désactiver Keep Alives) : active ou désactive les messages keepalive IKE.
  - Monitor Keep Alives (Surveillance Keep Alives) : active ou désactive la surveillance Keepalive IKE. La sélection de cette option rend disponibles les champs Confidence Interval (Intervalle de confiance) et Retry Interval (Intervalle de nouvelle tentative).
  - Intervalle de confiance : spécifie l'intervalle de confiance de maintien d'activité IKE. Cet intervalle est le nombre de secondes permettant à un homologue de passer au mode inactif avant de commencer la surveillance Keepalive. L'intervalle minimal est de 10 secondes ; l'intervalle maximal est de 300 secondes. L'intervalle par défaut pour un groupe d'accès à distance est de 10 secondes.
  - Retry Interval (Intervalle de nouvelle tentative) : spécifie le nombre de secondes à attendre entre les nouvelles tentatives de messages Keepalive IKE. La valeur par défaut est de 2 secondes.
  - Head End Will Never Initiate Keepalive Monitoring (La tête de réseau ne lancera jamais la surveillance Keepalive) : spécifie que l'ASA du site central ne lance jamais la surveillance Keepalive.
- Pour le VTI dynamique : associez un modèle virtuel au groupe de tunnels.
  - Virtual Template : choisissez un modèle virtuel dans la liste déroulante. 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.

    Pour terminer avec succès la configuration du modèle virtuel, vous devez configurer les paramètres d'interface DVTI suivants **Configuration > Device Setup (Configuration du périphérique) > Interface Settings (Paramètres de l'interface) > Interfaces (Interfaces) > Add (Ajouter) > Add DVTI Interface (Ajouter l'interface DVTI**))
    - Nom de l'interface DVTI
    - Activer l'interface
    - Activer la superposition d'IP en mode de tunnel pour IPSec (IPv4 ou IPv6)

- Protection du tunnel avec le profil IPsec

•

Gestion des certificats d'autorité de certification

La gestion des certificats d'autorité de certification s'applique à l'accès à distance et au VPN de site à site :

- Sur Site-to-Site (Site à site), cliquez sur Manage (Gérer) sous IKE Peer Authentication (Authentification d'homologue IKE) pour ouvrir la boîte de dialogue Manage CA Certificates (Gérer les certificats d'autorité de certification).
- Sur Remote Access VPN (VPN d'accès à distance), cliquez sur **Certificate Management** > **(Gestion des certificats)** > **CA Certificates** (Certificats d'autorité de certification).

Utilisez cette boîte de dialogue pour afficher, ajouter, modifier et supprimer des entrées dans la liste des certificats d'autorité de certification disponibles pour l'authentification des homologues IKE. La boîte de dialogue Manage CA Certificates (Gérer les certificats d'autorité de certification) répertorie les renseignements sur les certificats actuellement configurés, y compris les renseignements sur l'entité à laquelle le certificat a été délivré, l'autorité qui a délivré le certificat, la date d'expiration du certificat et les données d'utilisation.

- Add or Edit (Ajouter ou modifier) : ouvre la boîte de dialogue Install Certificate (Installer le certificat) ou Edit Certificate (Modifier le certificat), qui vous permet de préciser des renseignements sur un certificat et de l'installer.
- Show Details (Afficher les détails) : affiche des renseignements détaillés sur un certificat sélectionné dans le tableau.
- Delete (Supprimer) : supprime le certificat sélectionné du tableau. Il n'y a ni confirmation ni annulation.

Profil de connexion de site à site, certificat d'installation

Utilisez cette boîte de dialogue pour installer un nouveau certificat d'autorité de certification. Vous pouvez remplacer le certificat de l'une des manières suivantes :

- Cliquez sur Install from a file (Installer à partir d'un fichier) et accédez au fichier de certificat.
- Collez le texte de certificat obtenu précédemment au format PEM dans la zone de cette boîte de dialogue.
- Use SCEP (Utiliser SCEP) : spécifie l'utilisation du module complémentaire SCEP (Simple Certificate Enrollment Protocol) pour les services de certificats exécutés sur la famille Windows Server 2003. Il prend en charge le protocole SCEP, qui permet aux routeurs Cisco et à d'autres périphériques réseau intermédiaires d'obtenir des certificats.
  - SCEP URL (URL SCEP) : http:// : spécifie l'URL à partir de laquelle télécharger les informations SCEP.
  - Retry Period (Période de nouvelle tentative) : spécifie le nombre de minutes qui doivent s'écouler entre les requêtes SCEP.
  - Retry Count (Nombre maximal de tentatives) : spécifie le nombre maximal de tentatives autorisées.

- More Options (Plus d'options) : ouvre la boîte de dialogue Configure Options for CA Certificate (Configurer les options du certificat d'autorité de certification).

Utilisez cette boîte de dialogue pour préciser les détails de la récupération des certificats d'autorité de certification pour cette connexion d'accès à distance IPsec. Les boîtes de dialogue de cette boîte de dialogue sont les suivantes : Revocation Check (Vérification de la révocation), CRL Retrieval Policy (Politique de récupération des CRL), CRL Retrieval Method (Méthode de récupération des CRL), OCSP Rules (Règles OCSP) et Advanced (Avancé).

Utilisez la boîte de dialogue Revocation Check (Vérification de la révocation) pour préciser les renseignements sur la vérification de la révocation du certificat d'autorité de certification.

- Les boutons radio précisent s'il faut vérifier les certificats pour la révocation. Choisissez **Do Not Check Certificates for Revocation** (Ne pas vérifier les certificats pour la révocation) ou Check Certificates for Revocation (Vérifier les certificats pour la révocation).
- Revocation Methods area (Zone de méthodes de révocation) : vous permet de préciser la méthode (CRL ou OCSP) à utiliser pour la vérification de la révocation et l'ordre dans lequel utiliser ces méthodes. Vous pouvez choisir l'une ou les deux méthodes.

Module AnyConnect VPN de Cisco Secure Client Image

Le volet **Configuration > Remote Access VPN (VPN d'accès distant) > Network (Client) Access (Accès réseau [client]) > Secure Client > Software (Logiciel)** répertorie les images Secure Client configurées dans ASDM.

Secure Client Images Table (Tableau des images) : affiche les fichiers de progiciels configurés dans ASDM et vous permet de définir l'ordre dans lequel l'ASA télécharge les images vers le PC distant.

- Add (Ajouter) : affiche la boîte de dialogue Add Image Secure Client (Ajouter une image), dans laquelle vous pouvez spécifier un fichier de la mémoire flash comme image client ou parcourir la mémoire flash pour sélectionner un fichier à utiliser comme image client. Vous pouvez également charger un fichier d'un ordinateur local vers la mémoire flash.
- Replace (Remplacer) : affiche la boîte de dialogue Replace Image Secure Client (Remplacer image), dans laquelle vous pouvez spécifier un fichier de la mémoire flash comme image client pour remplacer une image sélectionnée dans le tableau SSL VPN Client Images (Images des clients VPN SSL). Vous pouvez également charger un fichier d'un ordinateur local vers la mémoire flash.
- Delete (Supprimer) : supprime une image du tableau. Cela ne supprime pas le fichier de paquet de la mémoire flash.
- Move Up (Déplacer vers le haut) et Move Down (Déplacer vers le bas) : les flèches haut et bas modifient l'ordre dans lequel l'ASA télécharge les images client vers le PC distant. Il télécharge d'abord l'image en haut du tableau. Par conséquent, vous devez déplacer l'image utilisée par le système d'exploitation le plus souvent rencontré vers le haut.

Module VPN AnyConnect de Cisco Secure Client Image, ajouter/Remplacer

Dans ce volet, vous pouvez spécifier un nom de fichier pour un fichier sur la mémoire flash ASA que vous souhaitez ajouter en tant qu'image Secure Client ou pour remplacer une image déjà répertoriée dans le tableau. Vous pouvez également parcourir la mémoire flash pour trouver un fichier à identifier ou charger un fichier à partir d'un ordinateur local.

- Flash SVC Image (Image SVC flash) : spécifiez le fichier de la mémoire flash que vous souhaitez identifier comme image client VPN SSL.
- Browse Flash (Parcourir la mémoire flash) : affiche la boîte de dialogue Browse Flash (Parcourir la mémoire flash), dans laquelle vous pouvez afficher tous les fichiers présents dans la mémoire flash.
- Upload (Téléverser) : affiche la boîte de dialogue Upload Image (Téléverser une image), dans laquelle vous pouvez téléverser un fichier depuis un PC local que vous souhaitez utiliser comme image client.
- Regular Expression to Match User-Agent (Expression régulière pour correspondre à l'agent utilisateur) : spécifie une chaîne que l'ASA utilise pour la comparer à la chaîne User-Agent transmise par le navigateur. Pour les utilisateurs mobiles, vous pouvez réduire le temps de connexion de l'appareil mobile en utilisant la fonction. Lorsque le navigateur se connecte à l'ASA, il inclut la chaîne User-Agent dans l'en-tête HTTP. Lorsque l'ASA reçoit la chaîne, si la chaîne correspond à une expression configurée pour une image, il télécharge immédiatement cette image sans tester les autres images client.

Module AnyConnect VPN de Cisco Secure Client Image, Charger l'image

Dans ce volet, vous pouvez indiquer le chemin d'accès d'un fichier situé sur l'ordinateur local ou dans la mémoire flash de l'appareil de sécurité que vous souhaitez désigner comme image Secure Client. Vous pouvez également parcourir l'ordinateur local ou la mémoire flash de l'appareil de sécurité pour repérer un fichier.

- Chemin d'accès au fichier local : identifie le nom de fichier du fichier sur l'ordinateur local que vous souhaitez identifier comme une image de client VPN SSL.
- Browse Local Files (Parcourir les fichiers locaux) : affiche la boîte de dialogue Select File Path (Sélectionner le chemin d'accès au fichier) où vous pouvez afficher tous les fichiers sur l'ordinateur local et choisir un fichier à identifier comme image client.
- Flash File System Path (Chemin d'accès au système de fichiers flash) : identifie le nom de fichier dans la mémoire flash du périphérique de sécurité que vous souhaitez identifier comme image de client VPN SSL.
- Browse Flash (Parcourir la mémoire flash) : affiche la boîte de dialogue Browse Flash Dialog (Parcourir la mémoire flash) où vous pouvez afficher tous les fichiers dans la mémoire flash du périphérique de sécurité et choisir un fichier à identifier comme image client.
- Upload File (Charger le fichier) : lance le chargement du fichier.

Progiciel SAML Secure Client du navigateur externe

Le volet **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) >Secure Client External Browser (Navigateur externe Secure Client/AnyConnect)** répertorie les progiciels de navigateur externe Secure Client disponibles pour l'authentification par authentification unique SAML (SSO) Secure Client.

Secure Client Images du progiciel du navigateur externe : affiche les fichiers de progiciel de navigateur externe configurés dans ASDM.

- **Add** (Ajouter) : affiche la boîte de dialogue Add Secure ClientExternal Browser Image (Ajouter une image de navigateur externe), dans laquelle vous pouvez spécifier un fichier dans la mémoire Flash comme image de progiciel externe ou parcourir la mémoire Flash pour sélectionner un fichier de progiciel de navigateur externe.

- **Replace** (Remplacer) : affiche la boîte de dialogue Replace Secure Client External Browser Package (Remplacer le progiciel de navigateur externe), dans laquelle vous pouvez spécifier un fichier dans la mémoire Flash comme progiciel de navigateur externe pour remplacer un fichier de progiciel existant.
- **Delete** (Supprimer) : supprime un fichier de progiciel de navigateur externe du tableau. Cela ne supprime pas le fichier de progiciel de la mémoire flash.
- **Move Up (Déplacer vers le haut) et Move Down (Déplacer vers le bas)** : les flèches vers le haut et vers le bas modifient l'ordre dans lequel l'ASA télécharge le progiciel de navigateur externe sur le PC distant.

Images du progiciel SAML Secure Client de navigateur externe, ajouter/remplacer

Dans ce volet, vous pouvez indiquer le nom d'un fichier situé dans la mémoire flash de l'ASA que vous souhaitez ajouter comme image de progiciel de navigateur externe Secure Client ou pour remplacer une image déjà répertoriée dans la table. Vous pouvez également parcourir la mémoire flash pour repérer un fichier, ou charger un fichier à partir d'un ordinateur local.

- **Secure Client External Browser Package** (Progiciel de navigateur externe) : spécifiez le fichier dans la mémoire flash que vous souhaitez identifier comme image de progiciel de navigateur externe.
- **Browse Flash** (Parcourir la mémoire Flash) : affiche la boîte de dialogue Browse Flash (Parcourir la mémoire Flash) dans laquelle vous pouvez afficher tous les fichiers de la mémoire Flash.
- **Upload** (Charger) : affiche la boîte de dialogue Upload Image (Charger l'image) dans laquelle vous pouvez charger un fichier à partir d'un ordinateur local que vous souhaitez identifier comme image de progiciel de navigateur externe.

Images du progiciel SAML Secure Client de navigateur externe, charger l'image

Dans ce volet, vous pouvez indiquer le chemin d'accès d'un fichier situé sur l'ordinateur local ou dans la mémoire flash de l'appareil de sécurité que vous souhaitez désigner comme image Secure Client. Vous pouvez également parcourir l'ordinateur local ou la mémoire flash de l'appareil de sécurité pour repérer un fichier.

- **Local File Path** (Chemin d'accès au fichier local) : identifie le nom du fichier sur l'ordinateur local que vous souhaitez identifier comme image de progiciel de navigateur externe.
- **Browse Local Files** (Parcourir les fichiers locaux) : affiche la boîte de dialogue Select File Path (Sélectionner le chemin d'accès au fichier) dans laquelle vous pouvez afficher tous les fichiers de l'ordinateur local et choisir un fichier à identifier comme image de progiciel de navigateur externe.
- **Flash File System Path** (Chemin d'accès au système de fichiers Flash) : identifie le nom du fichier dans la mémoire Flash du périphérique de sécurité que vous souhaitez identifier comme image de progiciel de navigateur externe.
- **Browse Flash** (Parcourir la mémoire Flash) : affiche la boîte de dialogue Browse Flash (Parcourir la mémoire Flash) dans laquelle vous pouvez afficher tous les fichiers de la mémoire Flash du périphérique de sécurité et choisir un fichier à identifier comme image de progiciel de navigateur externe.
- **Upload File** (Charger le fichier) : lance le chargement du fichier.

Configurer les connexions VPN Secure Client

Lignes directrices et limites relatives aux connexions Secure Client

Recommandations pour les jetons de session

Lorsque l'ASA authentifie une demande de connexion VPN à partir de Secure Client, un jeton de session est renvoyé au client pour une sécurité renforcée. À partir d'AnyConnect 4.9 (MR1), l'ASA et Secure Client prennent en charge un mécanisme qui offre une sécurité renforcée pour le jeton de session. Vous pouvez configurer une règle DAP pour rejeter les tentatives de connexion à partir de versions Secure Client qui ne prennent pas en charge la sécurité par jeton. Consultez Utiliser DAP pour vérifier la sécurité des jetons de session, à la page 220.

Configurer les profils Secure Client

Vous pouvez configurer l'ASA pour déployer des profils Secure Client globalement pour tous les utilisateurs Secure Client ou pour les utilisateurs en fonction de leur stratégie de groupe. Généralement, un utilisateur a un seul profil client pour chaque moduSecure Client installé. Dans certains cas, vous pouvez fournir plusieurs profils pour un utilisateur. Une personne qui travaille à partir de plusieurs emplacements peut avoir besoin de plusieurs profils. Sachez que certains paramètres de profil (comme SBL) contrôlent l'expérience de connexion à un niveau global. Les autres paramètres sont uniques à un hôte particulier et dépendent de l'hôte sélectionné.

Pour en savoir plus sur la création et le déploiement de profils Secure Client et le contrôle des fonctionnalités client, consultez le module AnyConnect VPN du Guide de l'administrateur pour.

Les profils clients sont configurés dans **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau (client)) > Profile (Profil) Secure Client**.

Add/Import (Ajouter/Importer) : affiche la boîte de dialogue Add Profiles (Ajouter des profils) Secure Client, où vous pouvez spécifier un fichier dans la mémoire Flash comme profil ou parcourir la mémoire Flash à la recherche d'un fichier à spécifier comme profil. Vous pouvez également charger un fichier d'un ordinateur local vers la mémoire flash.

- Profile Name (Nom du profil) : spécifiez un profil Secure Client pour cette stratégie de groupe.
- Profile Usage (Utilisation du profil) : affiche l'utilisation affectée au profil lors de sa création initiale : VPN, Network Access Manager, Web Security, ISE Posture, aMP Enabler, Network Visibility Module, Umbrella Roaming Security ou management VPN tunnel. Si ASDM ne reconnaît pas l'utilisation spécifiée dans le fichier XML, la liste déroulante devient sélectionnable et vous pouvez choisir un type d'utilisation manuellement.
- Profile Location (Emplacement du profil) : spécifiez un chemin d'accès au fichier de profil dans la mémoire flash de l'ASA. Si le fichier n'existe pas, l'ASA en crée un en fonction du modèle de profil.
- Group Policy (Stratégie de groupe) : spécifiez une stratégie de groupe pour ce profil. Le profil est téléchargé vers les utilisateurs appartenant à la stratégie de groupe avec Secure Client.

Edit (Modifier) : affiche la fenêtre de modification du profil du client VPN SSL, où vous pouvez modifier les paramètres contenus dans le profil pour les fonctionnalités Secure Client.

Exportation

- Device Profile Path (Chemin d'accès au profil du périphérique) : affiche le chemin d'accès et le nom du fichier de profil.
- Local Path (Chemin local) : spécifiez le chemin d'accès et le nom de fichier pour exporter le fichier de profil.
- Browse Local (Parcourir les fichiers locaux) : cliquez pour lancer une fenêtre afin de parcourir le système de fichiers des périphériques locaux.

Delete (Supprimer) : supprime un profil du tableau. Cela ne supprime pas le fichier XML de la mémoire flash.

Profiles Table (Tableau des profils) Secure Client : affiche les fichiers XML spécifiés comme profils Secure Client :

Exempter le trafic Secure Client de la traduction d'adresses réseau

Si vous avez configuré votre ASA pour effectuer la traduction d'adresses réseau (NAT), vous devez exempter le trafic Secure Client d'accès à distance de la traduction afin que les Secure Client, les réseaux internes et les ressources d'entreprise sur une DMZ puissent établir des connexions réseau entre eux. Le fait de ne pas exempter le trafic Secure Client de la traduction empêche les Secure Client et les autres ressources d'entreprise de communiquer.

La « NAT d'identité » (également connue sous le nom de « Exemption NAT ») permet à une adresse d'être traduite en elle-même, ce qui contourne efficacement la NAT. La NAT d'identité peut être appliquée entre deux ensembles d'adresses, un ensemble d'adresses et un sous-réseau ou deux sous-réseaux.

Cette procédure illustre comment configurer la NAT d'identité entre ces objets réseau hypothétiques dans notre exemple de topologie réseau : ensemble d'adresses VPN Engineering, ensemble d'adresses VPN Sales, réseau interne, réseau DMZ et Internet. Chaque configuration NAT d'identité nécessite une règle NAT.

Tableau 6 : Adressage réseau pour la configuration de la NAT d'identité pour les clients VPN

Réseau ou ensemble d'adresses	Nom du réseau ou de l'ensemble d'adresses	Une plage d'adresses IP.
Réseau interne	inside-network	10.50.50.0 – 10.50.50.255
Ensemble d'adresses de VPN d'ingénierie	Engineering-VPN	10.60.60.1 – 10.60.60.254
Ensemble d'adresses VPN Sales	Sales-VPN	10.70.70.1 – 10.70.70.254
Réseau DMZ	Réseau DMZ	192.168.1.0 – 192.168.1.255

Procédure

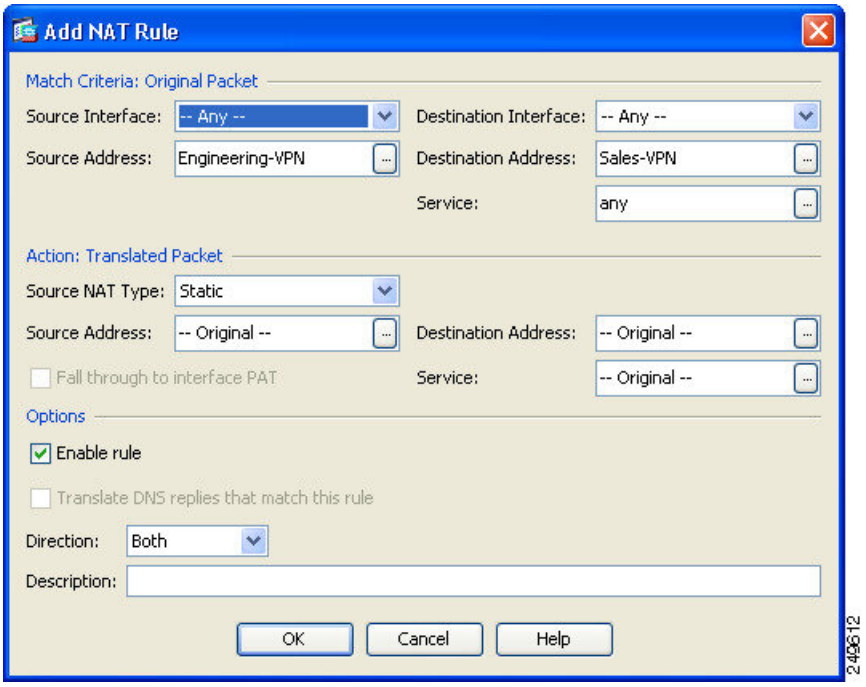
Étape 1 Connectez-vous à ASDM et accédez à **Configuration > Firewall (Pare-feu) > NAT Rules (Règles NAT)**.

Étape 2 Créez une règle NAT pour que les hôtes de l'ensemble d'adresses VPN Engineering puissent atteindre les hôtes de l'ensemble d'adresses VPN Sales. Dans le volet NAT Rules (Règles NAT), accédez à **Add (Ajouter)**

> **Add NAT Rule Before "Network Object" NAT rules** (Ajouter une règle NAT avant les règles NAT « Network Object ») afin que l'ASA évalue cette règle avant les autres règles de la table NAT unifiée.

Remarque
L'évaluation des règles NAT est appliquée de haut en bas, sur la base de la première correspondance. Une fois que l'ASA fait correspondre un paquet à une règle NAT particulière, il n'effectue aucune évaluation supplémentaire. Il est important que vous placiez les règles NAT les plus spécifiques en haut de la table NAT unifiée afin que l'ASA ne les fasse pas correspondre prématurément à des règles NAT plus générales.

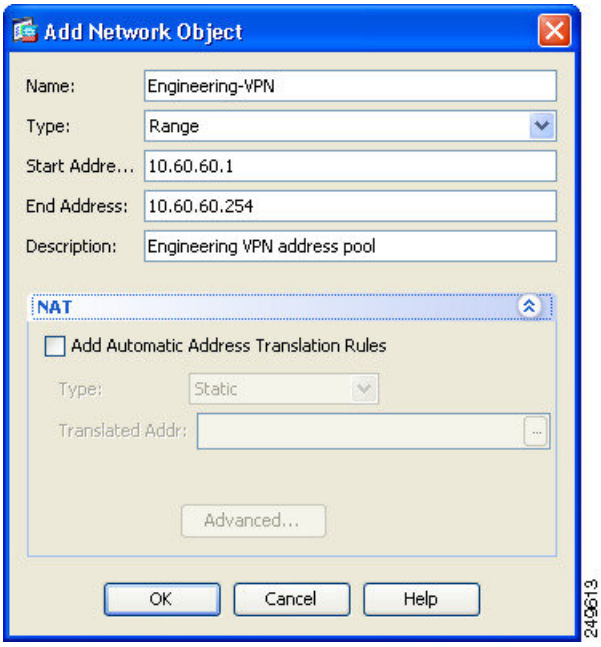
Illustration 2 : Boîte de dialogue Add NAT rule (Ajouter une règle NAT)



a) Dans la zone Match criteria: Original Packet (Critères de correspondance : Paquet d'origine), configurez ces champs :

- **Source Interface** (Interface source) : Any
- **Destination Interface** (Interface de destination) : Any
- **Source Address** (Adresse source) : cliquez sur le bouton de navigation Source Address (Adresse source) et créez l'objet réseau qui représente l'ensemble d'adresses VPN Engineering. Définissez le type d'objet comme une plage d'adresses. N'ajoutez pas de règle automatique de traduction d'adresses.
- **Destination Address** (Adresse de destination) : cliquez sur le bouton de navigation Destination Address (Adresse de destination) et créez l'objet réseau qui représente l'ensemble d'adresses VPN Sales. Définissez le type d'objet comme une plage d'adresses. N'ajoutez pas de règle automatique de traduction d'adresses.

Illustration 3 : Créer un objet réseau pour un ensemble d'adresses VPN



b) Dans la zone **ActionTranslated Packet** (Action traduite d'un paquet traduit), configurez ces champs :

- **Source NAT Type** (Type de NAT source) : Static
- **Source Address** (Adresse source) : Original
- **Destination Address (Adresse de destination)** : Original
- **Service** : Original

c) Dans la zone Options, configurez ces champs :

- Cochez la case **Enable rule** (Activer la règle).
- Décochez ou laissez vide la case **Translate DNS replies that match this rule** (Traduire les réponses DNS correspondant à cette règle).
- **Direction** : Both
- **Description** : ajoutez une description pour cette règle.

d) Cliquez sur **OK**.

e) Cliquez sur **Apply** (Appliquer).

Exemple de CLI

```
nat source static Engineering-VPN Engineering-VPN destination static Sales-VPN Sales-VPN
```

f) Cliquez sur Send (envoyer).

Étape 3 Lorsque l'ASA effectue la NAT, afin que deux hôtes du même ensemble VPN puissent se connecter l'un à l'autre ou pour que ces hôtes puissent accéder à Internet par le tunnel VPN, vous devez activer l'option Enable

traffic between two or more hosts connected to the same interface (Activer le trafic entre deux hôtes ou plus connectés à la même interface). Pour ce faire, dans ASDM, choisissez **Configuration > Device Setup (Configuration du périphérique) > Interface Settings (Paramètres de l'interface) > Interfaces**. Au bas du volet Interface, cochez la case Enable traffic between two or more hosts connected to the same interface (Activer le trafic entre deux hôtes ou plus connectés à la même interface) et cliquez sur Apply (Appliquer).

Exemple de CLI

```
same-security-traffic permit inter-interface
```

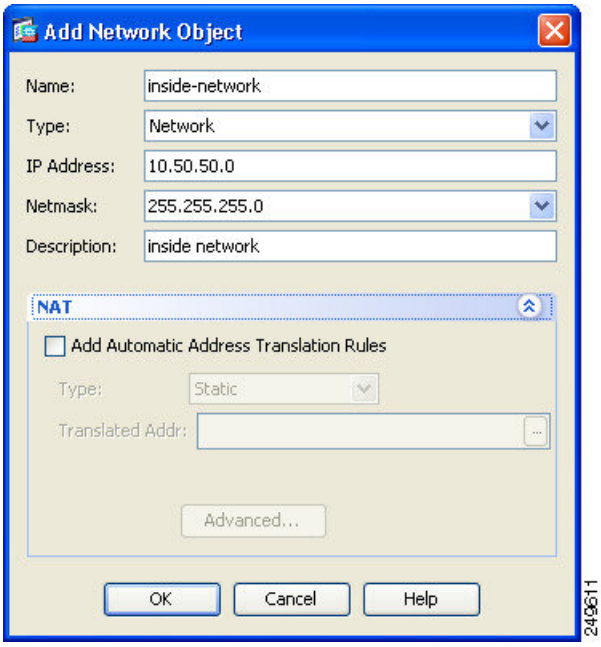
Étape 4 Créez une règle NAT pour que les hôtes de l'ensemble d'adresses VPN Engineering puissent atteindre les autres hôtes de l'ensemble d'adresses VPN Engineering. Créez cette règle exactement comme vous avez créé la règle précédente, sauf que vous spécifiez l'ensemble d'adresses VPN Engineering comme Source Address (Adresse source) et comme Destination Address (Adresse de destination) dans la zone Match criteria: Original Packet (Critères de correspondance : Paquet d'origine).

Étape 5 Créez une règle NAT pour que les clients d'accès à distance du VPN d'ingénierie puissent atteindre le réseau « interne ». Dans le volet NAT Rules (Règles NAT), choisissez Add (Ajouter) > Add NAT Rule Before "Network Object" NAT rules (Ajouter une règle NAT avant les règles NAT « Objet réseau ») afin que cette règle soit traitée avant les autres règles.

a) Dans la zone Match criteria: Original Packet (Critères de correspondance : Paquet d'origine), configurez ces champs :

- Source Interface (Interface source) : Any
- Destination Interface (Interface de destination) : Any
- Source Address (Adresse source) : cliquez sur le bouton de navigation Source Address (Adresse source) et créez un objet réseau qui représente le réseau interne. Définissez le type d'objet comme un réseau d'adresses. N'ajoutez pas de règle de traduction automatique d'adresses.
- Destination Address (Adresse de destination) : cliquez sur le bouton de navigation Destination Address (Adresse de destination) et choisissez l'objet réseau qui représente l'ensemble d'adresses VPN Engineering.

Illustration 4 : Add inside-network object (Ajouter un objet de réseau interne)



b) Dans la zone Action: Translated Packet (Action : Paquet traduit), configurez ces champs :

- Source NAT Type (Type de NAT source) : Static
- Source Address (Adresse source) : Original
- Destination Address (Adresse de destination) : Original
- Service : Original

c) Dans la zone **Options**, configurez ces champs :

- Cochez la case **Enable rule** (Activer la règle).
- Décochez ou laissez vide la case **Translate DNS replies that match this rule** (Traduire les réponses DNS correspondant à cette règle).
- Direction : Both
- Description : ajoutez une description pour cette règle.

d) Cliquez sur **OK**.

e) Cliquez sur **Apply** (Appliquer).

Exemple de CLI

```
nat source static inside-network inside-network destination static Engineering-VPN
Engineering-VPN
```

Étape 6 Créez une nouvelle règle, en suivant la méthode de **l'étape 5**, pour configurer la NAT d'identité pour la connexion entre l'ensemble d'adresses VPN Engineering et le réseau DMZ. Utilisez le réseau DMZ comme

Source Address (Adresse source) et l'ensemble d'adresses VPN Engineering comme Destination Address (Adresse de destination).

Étape 7 Créez une nouvelle règle NAT pour permettre à l'ensemble d'adresses VPN d'ingénierie d'accéder à Internet par le tunnel. Dans ce cas, vous ne souhaitez pas utiliser la NAT d'identité, car vous souhaitez modifier l'adresse source d'une adresse privée en une adresse routable Internet. Pour créer cette règle, suivez cette procédure :

a) Dans le volet NAT Rules (Règles NAT), choisissez Add (Ajouter) > Add NAT Rule Before "Network Object" NAT rules (Ajouter une règle NAT avant les règles NAT « Objet réseau ») afin que cette règle soit traitée avant les autres règles.

b) Dans la zone Match criteria: Original Packet (Critères de correspondance : Paquet d'origine), configurez ces champs :

- Source Interface (Interface source) : Any
- Destination Interface (Interface de destination) : Any Ce champ sera automatiquement rempli avec « outside » après que vous aurez choisi « outside » comme Source Address (Adresse source) dans la zone Action: Translated Packet (Action : Paquet traduit).
- Source Address (Adresse source) : cliquez sur le bouton de navigation Source Address (Adresse source) et choisissez l'objet réseau qui représente l'ensemble d'adresses VPN Engineering.
- Destination Address (Adresse de destination) : Any

c) Dans la zone Action: Translated Packet (Action : Paquet traduit), configurez ces champs :

- Source NAT Type (Type de NAT source) : Dynamic PAT (Hide)
- Source Address (Adresse source) : cliquez sur le bouton de navigation Source Address (Adresse source) et choisissez l'interface externe.
- Destination Address (Adresse de destination) : Original
- Service : Original

d) Dans la zone Options, configurez ces champs :

- Cochez la case Enable rule (Activer la règle).
- Décochez ou laissez vide la case Translate DNS replies that match this rule (Traduire les réponses DNS correspondant à cette règle).
- Direction : Both
- Description : ajoutez une description pour cette règle.

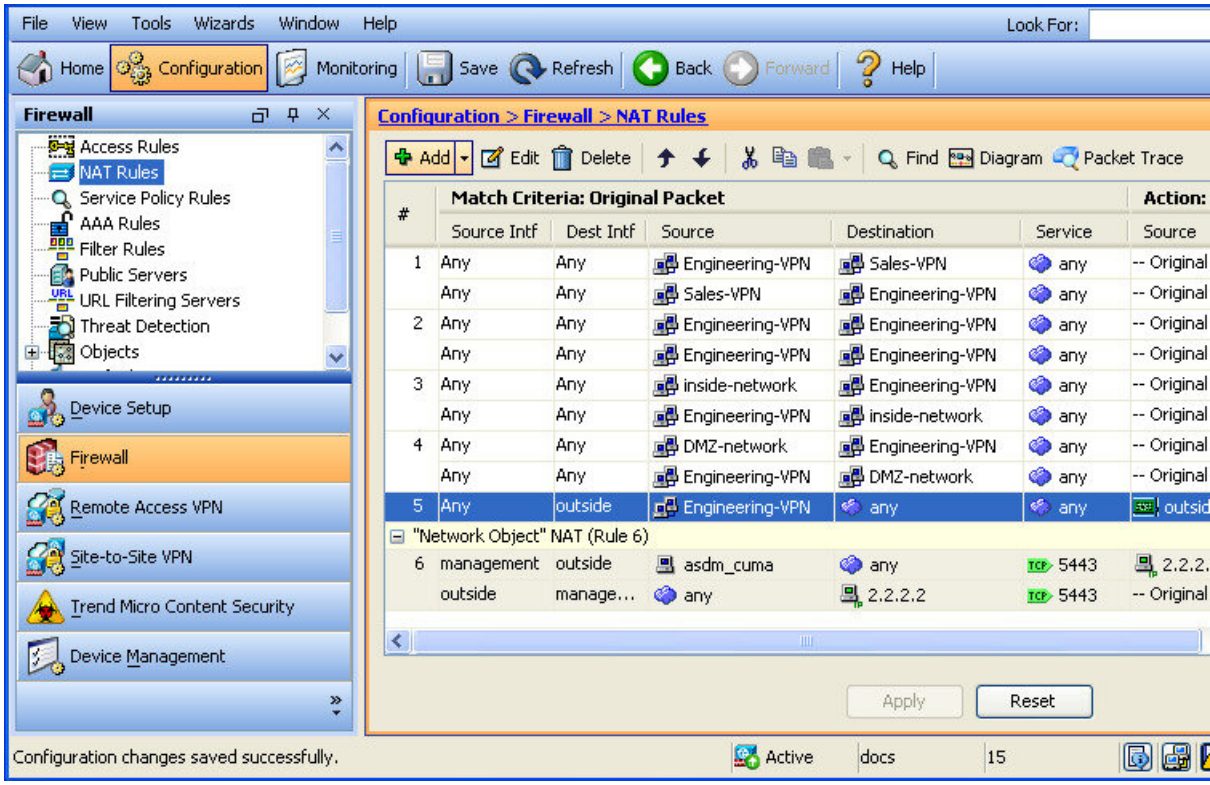
e) Cliquez sur **OK**.

f) Cliquez sur **Apply** (Appliquer).

Exemple de CLI

```
nat (any,outside) source dynamic Engineering-VPN interface
```

Illustration 5 : Table NAT unifiée



Étape 8 Après avoir configuré l'ensemble d'adresses VPN Engineering pour qu'il puisse atteindre lui-même, l'ensemble d'adresses VPN Sales, le réseau interne, le réseau DMZ et Internet, vous devez répéter ce processus pour l'ensemble d'adresses VPN Sales. Utilisez la NAT d'identité pour exempter le trafic de l'ensemble d'adresses VPN Sales de la traduction d'adresses réseau entre lui-même, le réseau interne, le réseau DMZ et Internet.

Étape 9 Dans le menu **File** (Fichier) de l'ASA, choisissez **Save Running Configuration to Flash** (Enregistrer la configuration en cours dans la mémoire Flash) pour mettre en œuvre vos règles de NAT d'identité.

HostScan Secure Client

Secure Client HostScan, maintenant appelé Secure Firewall Posture, permet au client de d'identifier le système d'exploitation l'antiprogramme malveillant et le logiciel de pare-feu installés sur l'hôte. L'application Secure Firewall Posture/HostScan recueille ces informations. L'évaluation de la posture nécessite l'installation de Secure Firewall Posture/HostScan sur l'hôte.

L'interface utilisateur ASDM est dynamique, de sorte que si HostScan est chargé, elle reflétera HostScan. Lorsque Secure Firewall Posture est chargé, l'interface reflète Secure Firewall Posture. Les différentes dénominations dépendent de la version que vous utilisez.

Préalables pour la posture HostScan/Secure Firewall

Secure Client avec le module Secure Firewall Posture/HostScan nécessite les composants ASA suivants au minimum :

- ASA 8.4
- ASDM 6.4

Vous devez installer Secure Firewall Posture/HostScan pour utiliser la fonction d'authentification SCEP.

Reportez-vous aux plateformes VPN prises en charge, série Cisco ASA pour connaître les systèmes d'exploitation pris en charge pour l'installation de la posture de pare-feu sécurisé/HostScan.

Licences pour Secure Client HostScan/Secure Firewall Posture

Voici les exigences de licence pour Secure Firewall Posture/HostScan :

- Secure Client Advantage (Apex) pour la posture de base HostScan/Secure Firewall.
- Une licence d'évaluation avancée de point terminal est requise pour la correction.

Progiciel HostScan

Vous pouvez charger le paquet HostScan sur l'appareil de sécurité adaptable Cisco en tant que paquet 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 progiciel HostScan/Secure Firewall Posture et l'activer à l'aide d'ASDM. L'interface utilisateur d'ASDM est dynamique : si HostScan est chargé, elle reflète HostScan. Lorsque Secure Firewall Posture est chargé, l'interface reflète Secure Firewall Posture. Les différentes dénominations dépendent de la version que vous utilisez.

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 Guide de migration HostScan Secure Client 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.

Procédure

Étape 1 Téléchargez le fichier secure-firewall-posture-*version*-k9.pkg sur votre ordinateur si vous utilisez la version 5. Pour la version 4.x, le fichier est hostscan_*version*-k9.pkg.

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 Cliquez sur **Upload** (Charger) pour préparer le transfert d'une copie du progiciel HostScan/Secure Firewall Posture depuis votre ordinateur vers un lecteur de l'ASA.

Étape 4 Dans la boîte de dialogue Upload Image (Charger l'image), cliquez sur **Browse Local Files** (Parcourir les fichiers locaux) pour rechercher le progiciel HostScan/Secure Firewall Posture sur votre ordinateur local.

Étape 5 Choisissez le fichier hostscan_*version*-k9.pkg ou secure-firewall-posture-*version*-k9.pkg que vous avez téléchargé ci-dessus et cliquez sur **Sélectionner**. Le chemin d'accès au fichier que vous avez sélectionné figure dans le champ Local File Path (Chemin d'accès au fichier local), et le champ Flash File System Path (Chemin d'accès au système de fichiers flash) reflète le chemin de destination du progiciel HostScan/Secure Firewall Posture. Si votre ASA comporte plus d'un lecteur flash, vous pouvez modifier le champ Flash File System Path (Chemin d'accès au système de fichiers flash) pour indiquer un autre lecteur flash.

Étape 6 Cliquez sur **Upload File** (Charger le fichier). ASDM transfère une copie du fichier sur la carte flash. Une boîte de dialogue d'information indique que le fichier a été chargé avec succès dans la mémoire flash.

Étape 7 Cliquez sur **OK**.

Étape 8 Dans la boîte de dialogue Use Uploaded Image (Utiliser l'image téléchargée), cliquez sur **OK** pour utiliser comme image actuelle le fichier de progiciel HostScan/Secure Firewall Posture que vous venez de charger.

Étape 9 Cochez **Enable HostScan** (Activer HostScan) ou **Enable Posture Image** (Activer l'image Posture) si ce n'est pas déjà fait.

Étape 10 Cliquez sur **Apply** (Appliquer).

Étape 11 Dans le menu File (Fichier), choisissez **Save Running Configuration To Flash** (Enregistrer la configuration en cours dans la mémoire flash).

Configurer les paramètres de posture

Pour chaque périphérique, vous pouvez configurer les paramètres de posture.

Avant de commencer

Assurez-vous d'avoir le paquet HostScan/Secure Firewall Posture.

Procédure

Étape 1 Choisissez **Configuration > Remote Access VPN (VPN d'accès distant) > Posture (for Secure Firewall) (Posture [pour Secure Firewall]) > Posture Settings (Paramètres de posture)**.

Étape 2 Sélectionnez un appareil dans la liste d'appareils du volet de gauche.

Pour chaque périphérique, vous pouvez afficher les attributs de la **Basic Posture (Posture de base)** et les **Posture Extensions** (Extensions de la posture).

Étape 3 Par défaut, le logiciel de sécurité Endpoint Détection et réponse (EDR) communique avec son serveur respectif pour récupérer les informations. Vous pouvez configurer les paramètres suivants pour les mises à jour EDR :

- Cochez la case **For EDR Update, Skip Internet Check After VPN Is Active** (Pour la mise à jour EDR, ignorer la vérification Internet après l'activation du VPN) si vous souhaitez qu'EDR ignore la vérification de la connexion Internet lorsque le tunnel VPN est actif.
- Cochez la case **For EDR Update, Skip Internet Check Before VPN Is Active** (Pour la mise à jour EDR, ignorer la vérification Internet avant l'activation du VPN) pour activer l'évaluation HostScan/Secure Firewall Posture sans vérifier si le logiciel de sécurité est à jour. Si vous décochez la case, l'évaluation de la posture peut échouer en raison d'un manque de connectivité, ce qui entraîne un refus d'accès réseau en fonction de la politique. Nous vous recommandons de vérifier la connectivité Internet avant l'évaluation de la posture.

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.

Procédure

Étape 1 Dans ASDM, accédez à **Configuration > Remote Access VPN (VPN d'accès à distance) > Posture (for Secure Firewall) (Posture [pour Secure Firewall]) > Posture Image (Image de posture)** pour désinstaller la posture de pare-feu sécurisé. Si vous utilisez AnyConnect version 4.x et désinstallez HostScan, accédez à **Configuration > Remote Access VPN (VPN d'accès à distance) > Secure Desktop Manager (Gestionnaire de bureau sécurisé) > Host Scan Image (Image Host Scan)**.

Étape 2 Cliquez sur **Uninstall** (Désinstaller), puis sur **Yes** (Oui) pour confirmer.

Étape 3 Cliquez sur **Uninstall** (désinstaller).

Affecter des modules de fonctionnalité Secure Client aux stratégies de groupe

Cette procédure associe les modules de fonctionnalité Secure Client 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 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 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

Chiffrement du disque

Pour Windows, macOS et Linux, cliquer sur la case **Identify Encrypted Disks on Endpoint** (Identifier les disques chiffrés sur le point terminal) dans la fenêtre Configuration (Configuration) > Remote Access VPN (VPN d'accès à distance) > Posture (for Secure Firewall) (Posture (pour Secure Firewall)) > Posture Settings (Paramètres de posture) > Configure (Configurer) > Advanced Endpoint Assessment (Évaluation avancée des points terminaux) permet de signaler les produits de chiffrement de disque installés sur le point terminal. Dans le journal csc_cscan, vous pouvez trouver les détails de version et l'état de chiffrement des disques.

Cette fonctionnalité est uniquement disponible avec Secure Client 5.0.02075 (ou version ultérieure) et ASDM 7.19.1 (ou version ultérieure).

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'administrateur deCiscoSecure (y compris AnyConnect) AnyConnect* pour obtenir plus d'informations sur le fonctionnement de HostScan/Secure Firewall Posture avec Secure Client.

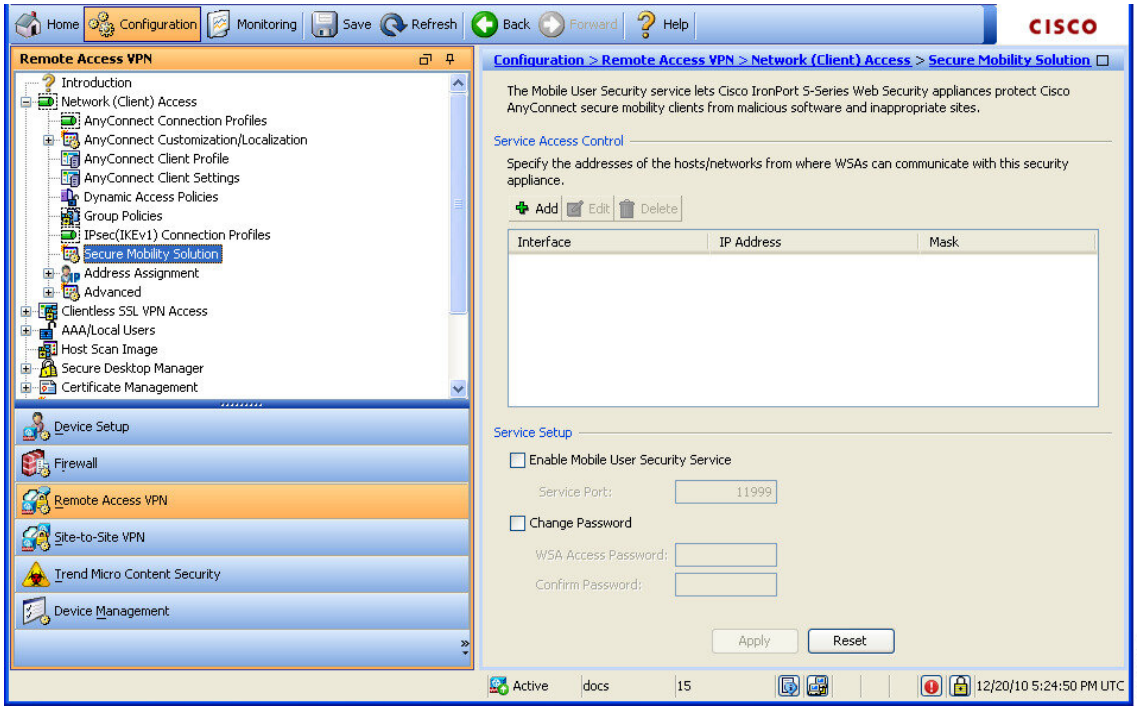
Solution Secure Client

Secure Client protège les intérêts et les actifs de l'entreprise contre les menaces Internet lorsque les employés sont mobiles. Secure Client permet aux appareils de sécurité Web Cisco IronPort de la série S d'analyser les clients Secure Client afin de s'assurer qu'ils sont protégés contre les logiciels malveillants et/ou les sites inappropriés. Le client vérifie périodiquement que la protection de l'appareil de sécurité Web Cisco IronPort de la série S est activée.

Remarque Cette fonctionnalité nécessite une version de l'appareil de sécurité Web Cisco IronPort qui fournit une prise en charge des licences Secure Client pour le Secure Client. Il nécessite également une version Secure Client qui prend en charge la fonctionnalité Secure Client. AnyConnect 3.1 et les versions ultérieures ne prennent pas en charge cette fonctionnalité.

Pour configurer des solutions de mobilité sécurisée, choisissez **Configuration > Remote Access VPN (VPN d'accès distant) > Network (Client) Access (Accès réseau [client]) > Secure Mobility Solution (Solution** de mobilité sécurisée).

Illustration 6 : Fenêtre de sécurité de l'utilisateur mobile



- Service Access Control (Contrôle d'accès de service) : spécifie l'hôte ou l'adresse réseau avec lequel les appareils de sécurité Web Cisco peuvent communiquer.
  - Add (Ajouter) : ouvre la boîte de dialogue Add MUS Access Control Configuration (Ajouter une configuration de contrôle d'accès MUS) pour la connexion sélectionnée.
  - Edit (Modifier) : ouvre la boîte de dialogue Edit MUS Access Control Configuration (Modifier la configuration de contrôle d'accès MUS) pour la connexion sélectionnée.
  - Delete (Supprimer) : supprime la connexion sélectionnée du tableau. Il n'y a ni confirmation ni annulation.
- Enable Mobile User Security Service (Activer le service de sécurité pour les utilisateurs mobiles) : démarre la connexion avec le client via le VPN. Si elle est activée, vous devez saisir un mot de passe, utilisé par le WSA lorsqu'il contacte l'ASA. Si aucun WSA n'est présent, l'état est désactivé.
- Service Port (Port de service) : si vous choisissez d'activer le service, spécifiez le numéro de port que le service doit utiliser. Le port doit être compris entre 1 et 65 535 et doit correspondre à la valeur

correspondante provisionnée dans l'appareil de sécurité adaptable Cisco avec le système de gestion. La valeur par défaut est 11 999.

- Change Password (Changer le mot de passe) : vous permet de modifier le mot de passe d'accès WSA.
- WSA Access Password (Mot de passe d'accès WSA) : spécifiez le mot de passe secret partagé requis pour l'authentification entre l'ASA et le WSA. Ce mot de passe doit correspondre au mot de passe correspondant configuré dans le WSA avec le système de gestion.
- Confirm Password (Confirmer le mot de passe) : saisissez de nouveau le mot de passe précisé.
- Show WSA Sessions (Afficher les sessions WSA) : vous permet d'afficher les informations de session des WSA connectés à l'ASA. L'adresse IP de l'hôte du WSA qui est connecté (ou a été connecté) et la durée de la connexion sont renvoyées dans une boîte de dialogue.

Ajouter ou modifier le contrôle d'accès MUS

La boîte de dialogue Add or Edit MUS Access Control (Ajouter ou modifier le contrôle d'accès MUS) sous Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau [client]) > Secure Mobility Solution (Solution de mobilité sécurisée) configure l'accès Mobile User Security (MUS) pour Secure Client.

- Nom de l'interface : utilisez la liste déroulante pour choisir le nom de l'interface que vous ajoutez ou modifiez.
- Adresse IP : entrez une adresse IPv4 ou IPv6.
- Masque : utilisez la liste déroulante pour choisir le masque approprié.

Personnalisation et localisation Secure Client

Vous pouvez personnaliser le module AnyConnect VPN du client Cisco Secure Client d'afficher votre propre image d'entreprise aux utilisateurs distants. Les champs suivants sous Customization/Localization (Personnalisation/Localisation) Secure Client vous permettent d'importer les types de fichiers personnalisés suivants :

- **Resources** : icônes de l'interface graphique modifiées pour Secure Client.
- **Binary** : fichiers exécutables pour remplacer le programme d'installation Secure Client. Cela inclut les fichiers d'interface graphique, ainsi que le profil de client VPN, les scripts et d'autres fichiers clients.
- **Script** : scripts qui seront exécutés avant ou après qu'Secure Client établisse une connexion VPN.
- **GUI Text and Messages** : titres et messages utilisés par Secure Client.
- **Customized Installer** : transformations qui modifient l'installation du client.
- **Localized Installer** : transformations qui modifient la langue utilisée par le client.

Chaque boîte de dialogue propose les actions suivantes :

- **Import** (Importer) lance la boîte de dialogue Import Customization Objects (Importer les objets de personnalisation) Secure Client, dans laquelle vous pouvez spécifier un fichier à importer en tant qu'objet.

- **Export** (Exporter) lance la boîte de dialogue Export Customization Objects (Exporter les objets de personnalisation) Secure Client, dans laquelle vous pouvez spécifier un fichier à exporter en tant qu'objet.
- **Delete** (Supprimer) supprime l'objet sélectionné.

Remarque Cette fonctionnalité n'est pas prise en charge en mode contexte multiple.

Personnalisation et localisation Secure Client, ressources

Les noms de fichier des composants personnalisés que vous importez doivent correspondre aux noms de fichier utilisés par l'interface graphique Secure Client, qui sont différents pour chaque système d'exploitation et sont sensibles à la casse pour Mac et Linux. Par exemple, si vous souhaitez remplacer le logo d'entreprise pour les clients Windows, vous devez importer votre logo d'entreprise en tant que logo_entreprise.png. Si vous l'importez sous un autre nom de fichier, le programme d'installation Secure Client ne modifie pas le composant. Toutefois, si vous déployez votre propre exécutable pour personnaliser l'interface graphique, l'exécutable peut appeler des fichiers de ressources en utilisant n'importe quel nom de fichier.

Si vous importez une image en tant que fichier de ressource (comme par exemple) : l'image que vous importez est personnalisée Secure Client jusqu'à ce que vous réimportez une autre image utilisant le même nom de fichier. Par exemple, si vous remplacez le fichier company_ logo.bmp par une image personnalisée, puis supprimez l'image, le client continue d'afficher votre image jusqu'à ce que vous importiez une nouvelle image (ou l'image du logo Cisco d'origine) utilisant le même nom de fichier.

Personnalisation et localisation Secure Client, binaire et script

Personnalisation et localisation Secure Client, binaire

Pour les ordinateurs Windows, Linux ou Mac (powerPC ou Intel), vous pouvez déployer votre propre client qui utilise l'API Secure Client. Vous remplacez l'interface graphique Secure Client et l'interface de ligne de commande Secure Client en remplaçant toutefois les fichiers binaires clients.

Champs de la boîte de dialogue **Import** :

- **Name** Saisissez le nom du fichier Secure Client que vous remplacez.
- **Platform** Sélectionnez la plateforme de système d'exploitation sur laquelle votre fichier est exécuté.
- **Select a file** Le nom de fichier n'a pas besoin d'être le même que le nom du fichier importé.

Personnalisation et localisation Secure Client, Script

Pour des informations complètes sur le déploiement de scripts, ainsi que sur leurs limites et restrictions, consultez le module AnyConnect VPN du Guide de l'administrateur Cisco Secure Client.

Champs de la boîte de dialogue **Import** :

- **Name** : saisissez un nom pour le script. Assurez-vous de préciser la bonne extension avec le nom. Par exemple, monscript.bat.
- **Script Type** : choisissez quand exécuter le script.

Secure Client Ajoute le préfixe scripts_ et le préfixe OnConnect ou OnDisconnect à votre nom de fichier pour identifier le fichier en tant que script sur l'ASA. Lorsque le client se connecte, l'ASA télécharge le script dans le répertoire cible approprié sur l'ordinateur distant, en supprimant le préfixe scripts_ et en conservant le préfixe OnConnect ou OnDisconnect restant. Par exemple, si vous importez le script monscript.bat, le script apparaît sur l'ASA sous le nom de scripts_OnConnect_myscript.bat. Sur l'ordinateur distant, le script s'affiche sous le nom OnConnect_myscript.bat.

Pour vous assurer que les scripts fonctionnent de manière fiable, configurez tous les ASA pour déployer les mêmes scripts. Si vous souhaitez modifier ou remplacer un script, utilisez le même nom que la version précédente et attribuez le script de remplacement à tous les ASA auxquels les utilisateurs peuvent se connecter. Lorsque l'utilisateur se connecte, le nouveau script remplace celui du même nom.

- **Platform** : sélectionnez la plateforme de système d'exploitation sur laquelle votre fichier est exécuté.
- **Select a file** : le nom de fichier n'a pas besoin d'être le même que le nom que vous avez fourni pour le script.

ASDM importe le fichier à partir de n'importe quel fichier source, créant le nouveau nom que vous spécifiez pour le nom.

Personnalisation et localisation Secure Client, texte et messages de l'interface graphique

Vous pouvez modifier la table de traduction par défaut ou en créer de nouvelles pour modifier le texte et les messages affichés sur l'interface graphique Secure Client. Ce volet partage également des fonctionnalités avec le volet Language Localization (Localisation de la langue). Pour une traduction linguistique plus approfondie, accédez à **Configuration > Remote Access VPN (VPN d'accès à distance) > Language Localization (Localisation de la langue)**.

En plus des boutons habituels dans la barre d'outils supérieure, ce volet comporte également un **Add**bouton , ainsi qu'une zone Template (Modèle) avec des boutons supplémentaires.

Add : le bouton Add (Ajouter) ouvre une copie de la table de traduction par défaut, que vous pouvez modifier directement ou enregistrer. Vous pouvez choisir la langue du fichier enregistré et modifier ultérieurement la langue du texte dans le fichier.

Lorsque vous personnalisez les messages dans la table de traduction, ne modifiez pas msgid. Modifiez le texte dans msgstr.

Précisez une langue pour le modèle. Le modèle devient un tableau de traduction dans la mémoire cache avec le nom que vous spécifiez. Utilisez une abréviation compatible avec les options linguistiques de votre navigateur. Par exemple, si vous créez un tableau pour la langue chinoise et que vous utilisez IE, utilisez l'abréviation *zh*, reconnue par IE.

Section Modèle

- Cliquez sur Template (Modèle) pour développer la zone des modèles, qui permet d'accéder à la table de traduction anglaise par défaut.
- Cliquez sur **View** pour afficher et éventuellement enregistrer la table de traduction anglaise par défaut.
- Cliquez sur **Export** pour enregistrer une copie de la table de traduction anglaise par défaut sans l'afficher.

Personnalisation et localisation Secure Client, transformations d'installation personnalisées

Vous pouvez effectuer une personnalisation plus approfondie de l'interface graphique Secure Client (Windows uniquement) en créant votre propre transformation qui se déploie avec le programme d'installation client. Vous importez la transformation dans l'ASA, qui la déploie avec le programme d'installation.

Windows est le seul choix valide pour l'application d'une transformation. Pour plus d'informations sur les transformations, consultez le *Guide de l'administrateur de Cisco* .

Personnalisation et localisation Secure Client, transformations localisées du programme d'installation

Vous pouvez traduire les messages affichés par le programme d'installation du client avec une transformation. La transformation modifie l'installation, mais laisse le MSI d'origine signé par la sécurité intact. Ces transformations ne font que traduire les écrans du programme d'installation et non les écrans de l'interface graphique utilisateur du client.

Attributs personnalisés Secure Client

Les attributs personnalisés sont envoyés à et utilisés par le Secure Client pour configurer des fonctionnalités telles que celles ci-dessous. Un attribut personnalisé a un type et une valeur nommée. Les attributs personnalisés prédéfinis sont utilisés par les politiques d'accès dynamique et les stratégies de groupe. Pour en savoir plus sur la configuration de ces attributs personnalisés, consultez la section Configurer les attributs personnalisés de Secure Client dans une stratégie de groupe interne. Créez et définissez des attributs personnalisés pour de nombreuses utilisations différentes :

- **DSCPPreservationAllowed** : pour activer la conservation DSCP, la définition de cet attribut personnalisé contrôle le point de code de services différentiels (DSCP) sur les plateformes de système d'exploitation Windows ou Mac pour la connexion DTLS. Il permet aux périphériques de hiérarchiser le trafic sensible à la latence et de marquer le trafic priorisé pour améliorer la qualité de la connexion sortante. Pour en savoir plus, consultez la section *Enable DSCP Preservation (activer la sauvegarde DSCP)* du Guide d'administration du client pour la mobilité sécurisée Cisco Secure Client.

  Valeurs : vrai/faux : par défaut Secure Client effectue la conservation DSCP (vrai). Pour le désactiver, définissez la valeur de l'attribut personnalisé sur faux sur la tête de réseau et relancez la connexion.

- **DeferredUpdateAllowed ou DeferredUpdateAllowed_ComplianceModule** : pour activer la mise à jour reportée sur un ASA : si ces attributs personnalisés sont configurés, lorsqu'une mise à jour client est disponible, Secure Client ouvre une boîte de dialogue demandant à l'utilisateur s'il souhaite procéder à une mise à jour ou à un report. Pour en savoir plus, consultez Activer la mise à niveau reportée Secure Client ou *Configurer la mise à jour reportée sur un ASA* dans le Guide d'administration du client pour la mobilité sécurisée Cisco Secure Client.

  Valeurs : vrai/faux : vrai active la mise à jour retardée. Si la mise à jour retardée est désactivée (faux), les paramètres suivants sont ignorés.

  - **DeferredUpdateMinimumVersion_ComplianceModule ou DeferredUpdateMinimumVersion** : version minimale de Secure Client qui doit être installée pour que les mises à jour soient reportables.

    Valeurs : x.x.x, avec 0.0.0 par défaut

- **DeferredUpdateDismissTimeout** : nombre de secondes pendant lesquelles l'invite de mise à niveau retardée s'affiche avant d'être rejetée automatiquement. S'applique uniquement lorsqu'une invite de mise à jour retardée s'affiche.

  Valeurs : de 0 à 300 secondes. Valeur par défaut : 150 secondes.

- **DeferredUpdateDismissResponse** : action à effectuer lorsque DeferredUpdateDismissTimeout se produit.

  Valeurs : différer ou mettre à jour. La valeur par défaut est mise à jour.

- **dynamic-split-exclude-domains <attribute name> <list of domains> ou dynamic-split-include-domains <attribute name> <list of domains>** : pour activer la tunnellisation fractionnée dynamique : en créant cet attribut personnalisé, vous pouvez fractionner dynamiquement la tunnellisation après l'établissement du tunnel en fonction du nom de domaine DNS de l'hôte. En ajoutant dynamic-split-exclude-domains, vous pouvez entrer des services en nuage ou Web auxquels le client doit accéder depuis l'extérieur du tunnel VPN. Pour en savoir plus, consultez la section *À propos de la tunnellisation fractionnée dynamique* dans le Guide d'administration du client pour la mobilité sécurisée Cisco Secure Client.

  Valeurs : le nom de l'attribut est le nom que vous choisissez. Par exemple, anyconnect-custom-data dynamic-split-exclude-domains excludedomains Webex.com, ciscospark.com.

- **managementTunnelAllAllowed** : le tunnel VPN de gestion nécessite, par défaut, une configuration de tunnellisation à inclusion fractionnée afin d'éviter d'affecter les communications réseau initiées par l'utilisateur (puisqu'il est conçu pour être transparent).

  Valeurs : vrai/faux. Pour remplacer ce comportement, définissez le nom et la valeur de l'attribut sur *true*. Secure Client puis procédez avec la connexion du tunnel de gestion si la configuration est de type tunnel-all, split-exclude, split-include ou bypass pour les deux protocoles IP.

- **UseLocalProfileAsAlternative** : si vous souhaitez distribuer un profil hors bande (à l'aide de SCCM, MDM, SecureX Cloud Management, ou similaire) sans configurer un profil client Cisco Secure (anciennement connu sous le nom de profil AnyConnect) sur le pare-feu Cisco Secure Firewall ASA, vous pouvez utiliser l'attribut personnalisé *UseLocalProfileAsAlternative*. Lorsque vous configurez cet attribut personnalisé, le client utilise le profil client Cisco Secure Client local (sur disque) pour ses paramètres et préférences (plutôt que les valeurs par défaut habituelles). Consultez la section sur le prédéploiement de Cisco Secure Client dans le guide d'administration pour obtenir des renseignements supplémentaires.

  L'établissement de la session à l'aide du profil local ne se produit que lorsque 1) *UseLocalProfileAsAlternative* est défini sur activé et 2) si un profil de stratégie de groupe ASA n'est pas configuré. Si vous configurez cet attribut personnalisé et n'annulez pas ou ne supprimez pas le profil client Cisco Secure de la configuration de la stratégie de groupe sur l'ASA, le profil client Cisco Secure configuré dans la stratégie de groupe sera conservé et utilisé pour chaque connexion, où le paramètre d'attribut personnalisé sera ignoré.

  Nom : désactivé/activé

  Valeurs : vrai/faux

- **no-dhcp-server-route** : pour définir la route du serveur DHCP public : cet attribut personnalisé permet au trafic DHCP local de circuler en clair lorsque Tunnel All Network est configuré. Secure Client ajoute une route spécifique au serveur DHCP local lorsque Secure Client se connecte et applique un filtre implicite sur l'adaptateur LAN de la machine hôte, bloquant tout le trafic pour cette route, à l'exception

du trafic DHCP. Pour en savoir plus, consultez la section *Définir la route du serveur DHCP public* du Guide d'administration du client pour la mobilité sécurisée Cisco Secure Client.

Valeurs : vrai/faux. L'attribut personnalisé no-dhcp-server-route doit être présent et défini sur true pour éviter de créer la route du serveur DHCP public lors de l'établissement du tunnel.

- **circumvent-host-filtering** : pour configurer Linux pour prendre en charge les sous-réseaux exclus : définit Linux pour prendre en charge l'exclusion des sous-réseaux lorsque la liste de réseau de tunnel ci-dessous est configurée pour la tunnellisation fractionnée. Pour de l'information supplémentaire, reportez-vous à la section Configurer Linux pour prendre en charge les sous-réseaux exclus, à la page 84.

  Valeurs : vrai/faux. Définissez-le sur true.

- **tunnel-from-any-source** : (Linux uniquement) Secure Client autorise les paquets avec n'importe quelle adresse source en mode split-include ou split-exclude. Il pourrait autoriser l'accès réseau à l'intérieur de l'instance de VM ou du conteneur Docker.

Remarque Les réseaux utilisés par les machines virtuelles ou les conteneurs Docker doivent être exclus du tunnel initialement.

- **par application** : la connexion VPN est utilisée pour un ensemble spécifique d'applications sur le périphérique portable (Android ou Apple iOS uniquement). Pour en savoir plus, consultez la section sur la création d'attributs personnalisés par application du *guide d'administrationCisco Secure Client AnyConnect*.

  Valeurs : ajoutez une ou plusieurs valeurs en copiant le format BASE64 de l'outil de politique et en le collez ici.

Pour terminer l'utilisation de ces fonctionnalités, la plupart des attributs personnalisés définis doivent être associés à une stratégie de groupe donnée dans le menu **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Group Policies (Stratégies de groupe)** > .

Logiciel client VPN IPsec

Remarque **Le client VPN est en fin de vie et n'est plus pris en charge.** Pour en savoir plus sur la configuration du client VPN, consultez la documentation d'ASDM pour l'ASA version 9.2. **Nous vous recommandons de passer au Secure Client.**

Serveur Zone Labs Integrity

Le volet **Configuration > Remote Access VPN (VPN d'accès distant) > Network (Client) Access (Accès réseau [client]) > Advanced (Avancé) > IPsec > Zone Labs Integrity Server** vous permet de configurer l'ASA pou Ce serveur fait partie du système Integrity, un système conçu pour appliquer les politiques de sécurité aux clients distants qui accèdent au réseau privé. En résumé, l'ASA agit comme un serveur proxy

pour le PC client vers le serveur pare-feu et relaye toutes les informations d'intégrité nécessaires entre le client d'intégrité et le serveur d'intégrité.

Remarque La version actuelle de l'appareil de sécurité prend en charge un serveur d'intégrité à la fois, même si les interfaces utilisateur prennent en charge la configuration jusqu'à cinq serveurs d'intégrité. En cas de défaillance du serveur actif, configurez un autre serveur d'intégrité sur l'ASA et puis rétablissez la session VPN cliente.

- **Server IP Address** (Adresse IP du serveur) : saisissez l'adresse IP du serveur d'intégrité. Utilisez la notation décimale à points.
- **Add** (Ajouter) : ajoute une nouvelle adresse IP de serveur à la liste des serveurs d'intégrité. Ce bouton est actif lorsqu'une adresse est saisie dans le champ Server IP Address (Adresse IP du serveur).
- **Delete** (Supprimer) : supprime le serveur sélectionné de la liste des serveurs d'intégrité.
- **Move Up** (Déplacer vers le haut) : déplace le serveur sélectionné vers le haut dans la liste des serveurs d'intégrité. Ce bouton est disponible uniquement lorsqu'il y a plusieurs serveurs dans la liste.
- **Move Down** (Déplacer vers le bas) : déplace le serveur sélectionné vers le bas dans la liste des serveurs d'intégrité. Ce bouton est disponible uniquement lorsqu'il y a plusieurs serveurs dans la liste.
- **Server Port** (Port du serveur) : saisissez le numéro de port de l'ASA sur lequel il est à l'écoute du serveur d'intégrité actif. Ce champ est disponible uniquement s'il y a au moins un serveur dans la liste des serveurs d'intégrité. Le numéro de port par défaut est 5054, et il peut être compris entre 10 et 10000. Ce champ est uniquement disponible lorsqu'il y a un serveur dans la liste des serveurs d'intégrité.
- **Interface** : choisissez l'interface ASA sur laquelle il communique avec le serveur d'intégrité actif. Ce menu de nom d'interface n'est disponible que lorsqu'il y a un serveur dans la liste des serveurs d'intégrité.
- **Fail Timeout** (Délai d'attente en cas d'échec) : saisissez le nombre de secondes pendant lesquelles l'ASA doit attendre avant de déclarer le serveur d'intégrité actif inaccessible. La valeur par défaut est 10 et la plage est comprise entre 5 et 20.
- **SSL Certificate Port** (Port de certificat SSL) : spécifiez le port ASA à utiliser pour l'autorisation SSL. La valeur par défaut est 80.
- **Enable SSL Authentication** (Activer l'authentification SSL) : cochez cette option pour activer l'authentification du certificat SSL du client distant par l'ASA. Par défaut, l'authentification SSL du client est désactivée.
- **Close Connection on Timeout** (Fermer la connexion à l'expiration) : cochez cette option pour fermer la connexion entre l'ASA et le serveur d'intégrité lorsqu'un délai d'expiration est atteint. Par défaut, la connexion reste ouverte.
- **Apply** (Appliquer) : cliquez pour appliquer le paramètre du serveur d'intégrité à la configuration ASA en cours d'exécution.
- **Reset** (Réinitialiser) : cliquez pour supprimer les modifications de configuration du serveur d'intégrité qui n'ont pas encore été appliquées.

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, les paquets CoA peuvent être envoyés directement à l'ASA à partir de 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
- L2TP/IPSec

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.

Configurer la modification d'autorisation dans ISE

La configuration du changement d'autorisation ISE implique la création d'un groupe de serveurs contenant les serveurs ISE RADIUS, puis l'utilisation de ce groupe de serveurs dans les profils de configuration VPN d'accès à distance (tunnels).

Procédure

Étape 1 Configurez le groupe de serveurs RADIUS AAA pour les serveurs ISE.

La procédure suivante explique la configuration minimale. Vous pouvez ajuster d'autres paramètres pour le groupe selon vos besoins. Les paramètres avancés comprennent des paramètres par défaut appropriés pour la plupart des réseaux. Consultez le guide de configuration général pour obtenir des renseignements complets sur la configuration des groupes de serveurs RADIUS AAA.

a) Choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **AAA/Local Users (AAA/Utilisateurs locaux)** > **AAA Server Groups (Groupes de serveurs AAA)**.

b) Cliquez sur **Add** (Ajouter) dans le champ **AAA Server Groups** (Groupes de serveurs AAA).

c) Saisissez un nom pour le groupe dans le champ **AAA Server Group** (Groupe de serveurs AAA).

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

e) Sélectionnez **Enable interim accounting update** (Activer la mise à jour provisoire de la comptabilité) et **Update Interval** (Intervalle de mise à jour) pour activer la génération périodique des messages de mise à jour provisoire de la comptabilité RADIUS.

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.

Vous pouvez modifier l'intervalle, en heures, pour l'envoi de ces mises à jour. La valeur par défaut est de 24 heures, la plage est comprise entre 1 et 120.

f) Sélectionnez **Enable dynamic authorization** (Activer l'autorisation dynamique).

Cette option active les services d'autorisation dynamique RADIUS (changement d'autorisation, CoA, d'ISE) pour le groupe de serveurs AAA. 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. Ne modifiez pas le port (1700), sauf si votre serveur ISE est configuré pour utiliser un port différent. La plage valide est de 1024 à 65535.

g) Si vous ne souhaitez pas utiliser ISE pour l'authentification, sélectionnez **Use authorization only mode** (Utiliser le mode d'autorisation uniquement).

Cela indique que lorsque ce groupe de serveurs est utilisé pour l'autorisation, le message de demande d'accès RADIUS sera généré en tant que demande « Autorize Only » (Autorisation uniquement), par opposition aux méthodes de mot de passe configurées pour le serveur AAA. Si vous configurez un mot de passe commun pour le serveur RADIUS, il sera ignoré.

Par exemple, vous utiliserez le mode d'autorisation seulement si vous souhaitez utiliser des certificats pour l'authentification plutôt que ce groupe de serveurs. Vous utiliserez toujours ce groupe de serveurs pour l'autorisation et la gestion de comptes dans le tunnel VPN.

h) Cliquez sur **OK** pour enregistrer le groupe de serveurs.

i) Une fois le groupe de serveurs sélectionné, cliquez sur **Add** (Ajouter) dans la liste **Servers in selected group** (Serveurs du groupe sélectionné) pour ajouter les serveurs ISE RADIUS au groupe.

Voici les attributs clés. Vous pouvez ajuster les valeurs par défaut pour d'autres paramètres selon vos besoins.

- **Interface Name** (Nom de l'interface) : l'interface par laquelle vous pouvez accéder au serveur ISE.
- **Server Name or IP Address** (Nom ou adresse IP du serveur) : nom d'hôte ou adresse IP du serveur ISE.
- (Facultatif) **Server Secret Key** (Clé secrète du serveur) : la clé permettant de chiffrer la connexion. Si vous ne configurez pas de clé, la connexion ne sera 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.

j) Cliquez sur **OK** pour ajouter le serveur au groupe.

Ajoutez des serveurs ISE supplémentaires au groupe de serveurs.

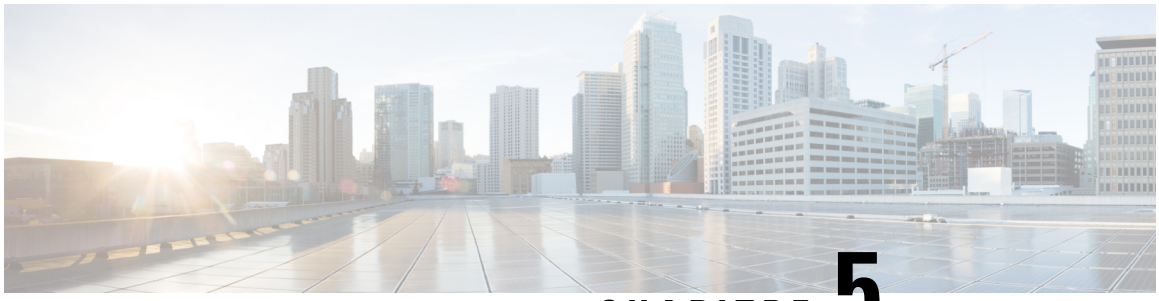
Étape 2 Mettez à jour les profils de configuration pour le VPN d'accès à distance afin d'utiliser le groupe de serveurs ISE.

Les étapes suivantes couvrent uniquement les options de configuration liées à ISE. Il existe d'autres options que vous devez configurer pour créer un VPN d'accès à distance fonctionnel. Suivez les instructions ailleurs dans ce guide pour mettre en œuvre le VPN d'accès à distance.

a) Choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Network (Client) Access (Accès au réseau (client))**Secure Client**Connection Profiles (Profils de connexion)**.
b) Dans le tableau **Connection Profiles** (Profils de connexion), ajoutez ou modifiez un profil.
c) Sur la page **Basic** (Base), configurez la méthode d'authentification.

- Si vous utilisez les serveurs ISE pour l'authentification, sélectionnez **AAA** pour **Authentication** > **Method** (Méthode d'authentification), puis sélectionnez le groupe de serveurs AAA ISE.
- Si vous avez configuré le groupe de serveurs ISE pour l'autorisation uniquement, sélectionnez une méthode d'authentification différente, par exemple **Certificate** (Certificat).

d) Sur la page **Advanced** > **(Avancé)** > **Authorization (Autorisation)**, sélectionnez le groupe de serveurs ISE pour **Authorization Server Group** (Groupe de serveurs d'autorisation).
e) Sur la page **Advanced (Avancé)** > **Accounting (Comptabilité)**, sélectionnez le groupe de serveurs ISE.
f) Cliquez sur **OK** pour enregistrer les modifications.



CHAPITRE 5

Adresses IP pour les VPN

Configurer une politique d'attribution d'adresses IP.

L'ASA peut utiliser une ou plusieurs des méthodes suivantes pour affecter des adresses IP aux clients d'accès à distance. Si vous configurez plusieurs méthodes d'attribution d'adresse, l'ASA essaie chacune des options jusqu'à ce qu'il trouve une adresse IP. Par défaut, toutes les méthodes sont activées.

- Use authentication server (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. Vous pouvez configurer des serveurs AAA dans le volet Configuration) > AAA Setup (Configuration AAA).Cette méthode est disponible pour les politiques d'attribution IPv4 et IPv6.

- Use 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. Si vous utilisez DHCP, configurez le serveur dans le volet Configuration > Remote Access VPN (VPN d'accès à distance) > DHCP Server (Serveur DHCP). Cette méthode est disponible pour les politiques d'attribution IPv4.

- **Use an internal address pool (Utiliser un ensemble d'adresses interne) :** les ensembles d'adresses configurés en interne constituent la méthode d'affectation la plus simple à configurer. Si vous utilisez cette méthode, configurez les ensembles d'adresses IP dans le volet Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools pane (Configuration > VPN d'accès à distance > Accès au réseau (client) > Affectation d'adresses > Ensembles d'adresses). Cette méthode est disponible pour les politiques d'attribution IPv4 et IPv6.

    - 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, cette option n'est pas cochée, ce qui signifie que l'ASA n'applique pas de délai. Si vous souhaitez appliquer un délai, cochez la case correspondante et saisissez un nombre de minutes compris entre 1 et 480 pour retarder la réaffectation de l'adresse IP.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 options d'affectation d'adresses IP

Procédure

Étape 1 Sélectionnez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Network (Client) Access (Accès réseau [client])** > **Address Assignment (Affectation d'adresses)** > **Assignment Policy (Politique d'affectation)**.

Étape 2 Dans la zone IPv4 Policy (politique IPv4), cochez la méthode d'affectation d'adresse pour l'activer ou décochez-la pour la désactiver. Ces méthodes sont activées par défaut :

- Utiliser le serveur d'authentification. Active l'utilisation d'un serveur d'authentification, d'autorisation et de comptabilité (AAA) que vous avez configuré pour fournir les adresses IP.
- Utiliser DHCP. Active l'utilisation d'un serveur DHCP (Dynamic Host Configuration Protocol) que vous avez configuré pour fournir des adresses IP.
- Use internal address pools (Utiliser des ensembles d'adresses internes) : active l'utilisation d'un ensemble d'adresses locales configuré sur l'ASA.

Si vous activez **Use internal address pools** (Utiliser des ensembles d'adresses internes), vous pouvez également activer la réutilisation d'une adresse IPv4 après sa libération. Vous pouvez spécifier une plage de minutes de 0 à 480 après laquelle l'adresse IPv4 peut être réutilisée.

Étape 3 Dans la zone IPv6 Policy (politique IPv6), cochez la méthode d'affectation d'adresse pour l'activer ou décochez-la pour la désactiver. Ces méthodes sont activées par défaut :

- Utiliser le serveur d'authentification. Active l'utilisation d'un serveur d'authentification, d'autorisation et de comptabilité (AAA) que vous avez configuré pour fournir les adresses IP.
- Utiliser des ensembles d'adresses internes : active l'utilisation d'un ensemble d'adresses locales configuré sur l'ASA.

Étape 4 Cliquez sur **Apply** (Appliquer).

Étape 5 Cliquez sur **OK**.

Afficher les méthodes d'attribution d'adresses

Procédure

Sélectionnez **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau [client]) > Address Assignment (Affectation d'adresses) > Assignment Policy (Stratégie d'affectation).**

Configurer les ensembles d'adresses IP locales

Pour configurer des ensembles d'adresses IPv4 ou IPv6 pour les tunnels VPN d'accès à distance, ouvrez ASDM et choisissez **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Address Management (Gestion des adresses) > Address Pools (Ensembles d'adresses) > Add/Edit IP Pool (Ajouter/Modifier un ensemble d'adresses IP)**. Pour supprimer un ensemble d'adresses, ouvrez ASDM et choisissez **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Address Management (Gestion des adresses) > Address Pools (Ensembles d'adresses)**. Sélectionnez l'ensemble d'adresses que vous souhaitez supprimer, et cliquez sur **Delete** (Supprimer).

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.

Configurer les ensembles d'adresses IPv4 locales

La zone IP Pool (Ensemble d'adresses IP) affiche les ensembles d'adresses configurés par nom avec leur plage d'adresses IP, par exemple : de 10.10.147.100 à 10.10.147.177. S'il n'existe aucun ensemble, la zone est vide. L'ASA utilise ces ensembles dans l'ordre indiqué : si toutes les adresses du premier ensemble ont été affectées, elle utilise l'ensemble suivant, et ainsi de suite.

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.

Procédure

Étape 1 **Sélectionnez Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Address Assignment (Attribution d'adresses) > Address Pools (Ensembles d'adresses).**

Étape 2 Pour ajouter une adresse IPv4, cliquez sur **Add (Ajouter) > IPv4 Address Pool (Ensemble d'adresses IPv4)**. Pour modifier un ensemble d'adresses existant, choisissez l'ensemble d'adresses dans la table d'ensemble d'adresses et cliquez sur **Edit** (Modifier).

Étape 3 Dans la boîte de dialogue Add/Edit IP Pool (Ajouter/Modifier un ensemble d'adresses IP), saisissez les renseignements suivants :

- Nom : saisissez le nom de l'ensemble d'adresses IP. Il peut comporter jusqu'à 64 caractères
- Adresse de départ : saisissez la première adresse IP disponible dans chaque ensemble configuré. Utilisez la notation décimale à points, par exemple : 10.10.147.100.
- Adresse de fin : saisissez la dernière adresse IP disponible dans chaque ensemble configuré. Notation décimale à points de l'utilisateur, par exemple : 10.10.147.177.
- Masque de sous-réseau : identifie le sous-réseau sur lequel cet ensemble d'adresses IP se trouve.

Étape 4 Cliquez sur **Apply** (Appliquer).

Étape 5 Cliquez sur **OK**.

Configurer les ensembles d'adresses IPv6 locales

La zone IP Pool (Ensemble IP) affiche les ensembles d'adresses configurées par nom avec une plage d'adresses IP de départ, le préfixe d'adresse et le nombre d'adresses configurables dans l'ensemble. S'il n'y a aucun ensemble, la zone est vide. L'ASA utilise ces ensembles dans l'ordre indiqué : si toutes les adresses du premier ensemble ont été affectées, elle utilise l'ensemble suivant, et ainsi de suite.

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.

Procédure

Étape 1 **Sélectionnez Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Network (Client) Access (Accès réseau [client])** > **Address Assignment (Affectation d'adresses)** > **Address Pools (Ensembles d'adresses).**

Étape 2 Pour ajouter une adresse IPv6, cliquez sur **Add** > **(Ajouter)** > **IPv6 Address Pool (Ensemble d'adresses IPv6)**. Pour modifier une ensemble d'adresses existant, choisissez l'ensemble d'adresses dans le tableau des ensembles d'adresses et cliquez sur **Edit** (Modifier).

Étape 3 Dans la boîte de dialogue Add/Edit IP Pool (Ajouter/Modifier un ensemble d'adresses IP), saisissez les informations suivantes :

- Nom : affiche le nom de chaque ensemble d'adresses configurée.

  Adresse IP de départ : saisissez la première adresse IP disponible dans l'ensemble d'adresses configuré. Par exemple : 2001:DB8::1.

- Longueur du préfixe : saisissez la longueur du préfixe d'adresse IP en bits. Par exemple, 32 représente /32 en notation CIDR. La longueur du préfixe définit le sous-réseau sur lequel réside l'ensemble d'adresses IP.

- Number of Addresses(nombre d'adresses) : Détermine le nombre d'adresses IPv6, en commençant par l'adresse IP de départ, qui se trouvent dans l'ensemble.

Étape 4 Cliquez sur **Apply** (Appliquer).

Étape 5 Cliquez sur **OK**.

Affecter des ensembles d'adresses internes aux stratégies de groupe

La boîte de dialogue Add or Edit Group Policy (Ajouter ou modifier une stratégie de groupe) vous permet de préciser les ensembles d'adresses, les protocoles de tunnellisation, les filtres, les paramètres de connexion et les serveurs pour la stratégie de groupe interne Network (Client) Access (Accès réseau [client]) en cours d'ajout ou de modification. Pour chacun des champs de cette boîte de dialogue, le fait de cocher la case Inherit

(Hériter) permet au paramètre correspondant de prendre sa valeur à partir de la stratégie de groupe par défaut. Inherit (Hériter) est la valeur par défaut de tous les attributs de cette boîte de dialogue.

Remarque : vous pouvez configurer des ensembles d'adresses IPv4 et IPv6 pour la même stratégie de groupe. Si les deux versions des adresses IP sont configurées dans la même politique de groupe, les clients configurés pour IPv4 obtiendront une adresse IPv4, les clients configurés pour IPv6 obtiendront une adresse IPv6 et les clients configurés pour à la fois les adresses IPv4 et IPv6 obtiendront à la fois une adresse IPv4 et une adresse IPv6.

Procédure

Étape 1 Connectez-vous à l'ASA à l'aide d'ASDM et sélectionnez **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Group Policies (Stratégies de groupe)**.

Étape 2 Créez une nouvelle stratégie de groupe ou sélectionnez la stratégie de groupe que vous souhaitez configurer avec un ensemble d'adresses internes, puis cliquez sur Edit (Modifier).

Le volet General attributes (Attributs généraux) est sélectionné par défaut dans la boîte de dialogue de stratégie de groupe.

Étape 3 Utilisez le champ Address Pools (Ensembles d'adresses) pour préciser un ensemble d'adresses IPv4 pour cette stratégie de groupe. Cliquez sur Select (Sélectionner) pour ajouter ou modifier un ensemble d'adresses IPv4.

Étape 4 Utilisez le champ IPv6 Address Pools (Ensembles d'adresses IPv6) pour préciser un ensemble d'adresses IPv6 à utiliser pour cette stratégie de groupe. Cliquez sur Select (Sélectionner) pour ajouter ou modifier un ensemble d'adresses IPv6.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Apply** (Appliquer).

Configurer l'adressage DHCP

Pour utiliser 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 de réseau DHCP dans la stratégie de groupe associée à un profil de connexion ou 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 de réseau DHCP de 10.100.10.1 pour la stratégie de groupe appelée **remotegroup**. (La stratégie de groupe appelée remotegroup est associée au profil de connexion appelé 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 vos serveurs DHCP.

Vous ne pouvez pas attribuer d'adresses IPv6 à Secure Clientà l'aide d'un serveur DHCP.

a) Vérifiez que DHCP est activé dans **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Network (Client) Access (Accès réseau [client])** > > **Address Assignment (Attribution d'adresses)** > **Assignment Policy (Politique d'attribution)**.
b) Configurez vos serveurs DHCP en sélectionnant **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **DHCP Server (Serveur DHCP)**.

Étape 2 Définissez le serveur DHCP dans le profil de connexion.

a) Sélectionnez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Network (Client) Access (Accès réseau [client]) > Secure ClientConnection Profiles (Profils de connexion Secure Client/AnyConnect)**.
b) Dans la zone Connection Profiles (Profils de connexion), cliquez sur **Add (Ajouter)** ou **Edit (Modifier)**.
c) Cliquez sur **Basic** (De base) dans l'arborescence de configuration du profil de connexion.
d) Dans la zone Client Address Assignment (affectation d'adresses client), saisissez l'adresse IPv4 du serveur DHCP que vous souhaitez utiliser pour attribuer les adresses IP aux clients. Par exemple, **172.33.44.19**.

Étape 3 Modifiez la stratégie de groupe associée au profil de connexion pour définir la portée de DHCP.

a) Sélectionnez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Network (Client) Access (Accès réseau [client])** > **Group Policies (Stratégies de groupe)**.
b) Cliquez deux fois sur la stratégie de groupe que vous souhaitez modifier.
c) Cliquez sur **Server (Serveur)** dans l'arborescence de configuration.
d) Développez la zone **More Options** (Plus d'options) en cliquant sur la flèche vers le bas.
e) Décochez **DHCP Scope Inherit** (Hériter de la portée DHCP) et définissez la portée DHCP.

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.

f) Cliquez sur **OK**.
g) Cliquez sur **Apply** (Appliquer).

Attribuer des adresses IP aux utilisateurs locaux

Les comptes d'utilisateurs locaux peuvent être configurés pour utiliser une stratégie de groupe, et certains attributs Secure Client peuvent également être configurés. Ces comptes d'utilisateurs fournissent un repli si les autres sources d'adresses IP échouent, de sorte que les administrateurs auront toujours un accès.

Avant de commencer

Pour ajouter ou modifier un utilisateur, choisissez **Configuration> Remote Access VPN (VPN d'accès à distance) > AAA/Local Users (AAA/Utilisateurs locaux) > Local Users (Utilisateurs locaux)**, puis cliquez sur **Add (Ajouter)** ou **Edit (Modifier)**.

Par défaut, la case **Inherit** (Hériter) est cochée pour chaque paramètre sur l'écran Edit User Account (Modifier le compte d'utilisateur), ce qui signifie que le compte d'utilisateur hérite de la valeur de ce paramètre de la stratégie de groupe par défaut, DfltGrpPolicy.

Pour remplacer chaque paramètre, décochez la case **Inherit** (Hériter) et saisissez une nouvelle valeur. Les étapes détaillées qui suivent décrivent les paramètres d'adresse IP. Consultez Configurer les attributs de politique VPN pour un utilisateur local, à la page 101 pour les détails complets de configuration.

Procédure

Étape 1 Démarrez ASDM et choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **AAA/Local Users (AAA/Utilisateurs locaux)** > **Local Users** > **(Utilisateurs locaux)**.

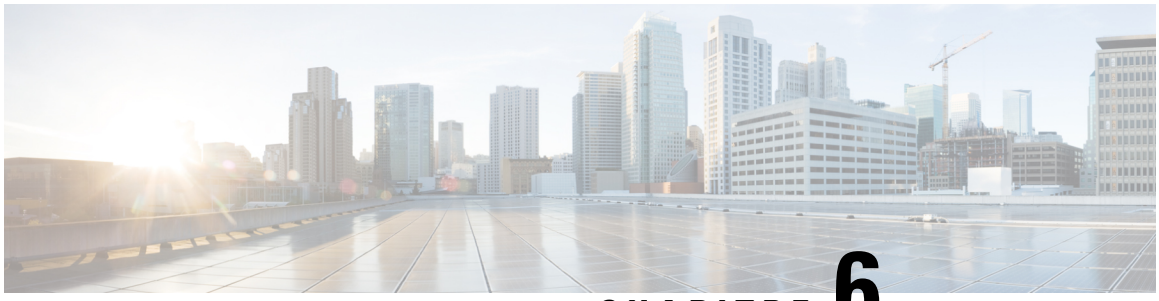
Étape 2 Sélectionnez l'utilisateur que vous souhaitez configurer et cliquez sur **Edit** (Modifier).

Étape 3 Dans le volet de gauche, cliquez sur **VPN Policy** (Politique VPN).

Étape 4 Pour définir une adresse IPv4 dédiée à cet utilisateur, saisissez une adresse IPv4 et un masque de sous-réseau dans la zone **Adresse IPv4 dédiée (facultatif)**.

Étape 5 Pour définir une adresse IPv6 dédiée à cet utilisateur, saisissez une adresse IPv6 avec un préfixe IPv6 dans la zone **Adresse IPv6 dédiée (facultatif)**. Le préfixe IPv6 indique le sous-réseau sur lequel se trouve l'adresse IPv6.

Étape 6 Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution.



CHAPITRE 6

Politiques d'accès dynamique

Ce chapitre décrit comment configurer les politiques d'accès dynamique.

À propos des politiques d'accès dynamique

Les passerelles VPN fonctionnent dans des environnements dynamiques. Plusieurs variables peuvent affecter chaque connexion VPN, par exemple, les configurations intranet qui changent fréquemment, les différents rôles de chaque utilisateur au sein d'une organisation, et les connexions à partir de sites d'accès à distance avec des configurations et des niveaux de sécurité différents. La tâche d'autoriser les utilisateurs est beaucoup plus complexe dans un environnement VPN que dans un réseau avec une configuration statique.

Les politiques d'accès dynamiques (DAP) sur l'ASA vous permettent de configurer l'autorisation qui traite ces nombreuses variables. Vous créez une politique d'accès dynamique en définissant un ensemble d'attributs de contrôle d'accès que vous associez à un tunnel d'utilisateur ou à une session spécifique. Ces attributs traitent des problèmes d'appartenance à plusieurs groupes et de sécurité des points terminaux. L'ASA accorde l'accès à un utilisateur particulier pour une session particulière en fonction des politiques que vous définissez. L'ASA génère une DAP au moment où l'utilisateur se connecte en sélectionnant ou en agrégeant les attributs d'un ou de plusieurs enregistrements DAP. Il sélectionne ensuite ces enregistrements DAP en fonction des informations de sécurité au point terminal du périphérique distant et des informations d'autorisation AAA pour l'utilisateur authentifié. Ensuite, l'ASA applique l'enregistrement DAP au tunnel ou à la session d'utilisateur.

Le système DAP comprend les composants suivants qui nécessitent votre attention :

- Fichier de configuration de sélection DAP : fichier texte contenant les critères utilisés par l'ASA pour sélectionner et appliquer les enregistrements DAP lors de l'établissement de la session. Stocké sur l'ASA. Vous pouvez utiliser ASDM pour le modifier et le charger dans l'ASA au format de données XML. Les

fichiers de configuration de sélection DAP comprennent tous les attributs que vous configurez. Il peut s'agir d'attributs AAA, d'attributs de terminal et de politiques d'accès, comme configuré dans les listes de filtre d'ACL de type réseau et Web, de transfert de port et d'URL.

- DfltAccess Policy (politique d'accès) : toujours la dernière entrée dans la table récapitulative DAP, toujours avec une priorité de 0. Vous pouvez configurer les attributs de politique d'accès pour la politique d'accès par défaut, mais celle-ci ne contient pas (et vous ne pouvez pas configurer) les attributs d'AAA ou de point terminal. Vous ne pouvez pas supprimer DfltAccessPolicy, et il doit s'agir de la dernière entrée du tableau récapitulatif.

Reportez-vous au *guide de déploiement de Dynamic Access* (https://supportforums.cisco.com/docs/DOC-1369) pour obtenir des renseignements supplémentaires.

Prise en charge par DAP des protocoles d'accès à distance et des outils d'évaluation de la posture

L'ASA obtient les attributs de sécurité de point terminal en utilisant des outils d'évaluation de la posture que vous configurez. Ces outils d'évaluation de la posture comprennent le module de posture AnyConnect , le paquet indépendant HostScan/Secure Firewall Posture et NAC.

Le tableau suivant identifie chacun des protocoles d'accès à distance pris en charge par DAP, les outils d'évaluation de la posture disponibles pour cette méthode et les informations que cet outil fournit.

Protocole d'accès à distance pris en charge	**Module de posture de pare-feu sécurisé** **Progiciel HostScan** **Cisco Secure Firewall Posture**	**Module de posture de pare-feu sécurisé** **Progiciel HostScan** **Cisco Secure Firewall Posture**	**NAC**	**Cisco NAC Appliance**
	Renvoie les renseignements sur les fichiers, les valeurs de clé de registre, les processus en cours d'exécution et le système d'exploitation	Renvoie les informations sur les logiciels de protection contre les programmes malveillants et de pare-feu personnel.	Renvoie l'état de la NAC	Renvoie le type de VLAN et les ID de VLAN
VPN IPsec	Non	Non	Oui	Oui
VPN AnyConnect de Cisco	Oui	Oui	Oui	Oui
VPN SSL sans client (basé sur un navigateur)	Oui	Oui	Non	Non

Protocole d'accès à distance pris en charge	Module de posture de pare-feu sécurisé Progiciel HostScan Cisco Secure Firewall Posture	Module de posture de pare-feu sécurisé Progiciel HostScan Cisco Secure Firewall Posture	NAC	Cisco NAC Appliance
proxy PIX (évaluation de la posture non disponible)	Non	Non	Non	Non

Séquence de connexion d'accès à distance avec les DAP

La séquence suivante décrit un établissement typique d'accès à distance.

1. Un client distant tente d'établir une connexion VPN.
2. L'ASA effectue une évaluation de la posture à l'aide des valeurs de posture du NAC et de HostScan/Secure Firewall configurées.
3. L'ASA authentifie l'utilisateur par le biais du protocole AAA. Le serveur AAA renvoie également les attributs d'autorisation pour l'utilisateur.
4. L'ASA applique les attributs d'autorisation AAA à la session et établit le tunnel VPN.
5. L'ASA sélectionne les enregistrements DAP en fonction des informations d'autorisation AAA pour l'utilisateur et des informations d'évaluation de la posture pour la session.
6. L'ASA regroupe les attributs DAP des enregistrements DAP sélectionnés et ils deviennent la politique DAP.
7. L'ASA applique la politique DAP à la session.

Licences des politiques d'accès dynamique

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

Les politiques d'accès dynamiques (DAP) nécessitent l'une des licences suivantes :

- Secure Client Premier : pour utiliser toutes les fonctionnalités DAP.
- Secure Client Advantage : pour la vérification de version du système d'exploitation et du système d'exploitation/Secure Client uniquement.

Sujets connexes

Ajouter les attributs de point terminal Secure Client à une DAP, à la page 194

Configurer des politiques d'accès dynamique

Avant de commencer

- Sauf indication contraire, vous devez installer HostScan/Secure Firewall Posture avant de configurer les attributs des points terminaux DAP.
- Si vous effectuez une mise à niveau d'HostScan 4.3.x vers HostScan 4.6.x ou une version ultérieure, vous devez migrer tous les attributs de point terminal AV/AS/FW existants vers les attributs de point terminal AM/FW de remplacement correspondants avant d'effectuer la mise à niveau. Consultez le guide de migration AnyConnect HostScan de la version 4.3.x à la version 4.6.x pour obtenir une procédure de mise à niveau et de migration complète.
- En raison de problèmes de sécurité dans Java Web Start, vous risquez de ne pas pouvoir remplir l'attribut de terminal avancé avec des valeurs configurées si vous utilisez une configuration basée sur Webvpn sur le périphérique. Pour résoudre ce problème, utilisez l'application de bureau ASDM ou ajoutez la ou les URL liées à l'AEA en tant qu'exceptions dans la sécurité Java.
- Avant de configurer les attributs de fichier, de processus et de registre, configurez les attributs de base de fichier, de processus et de registre HostScan/Secure Firewall Posture. Pour obtenir des instructions, accédez dans ASDM à l'écran de l'interface utilisateur approprié et cliquez sur **Help** (Aide).
- DAP ne prend en charge que les caractères ASCII.

Procédure

Étape 1 Démarrez ASDM et choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Network (Client) Access (Accès au réseau (client))**> **Dynamic Access Policies (Politiques d'accès dynamiques)**.

Remarque
Si un bouton d'action **Incompatible** s'affiche sous les actions Add (Ajouter), Edit (Modifier) et Delete (Supprimer), il y a eu une tentative de mise à niveau de HostScan vers une version (4.6.x ou ultérieure) qui a eu des mises à jour de bibliothèque internes qui le rendent incompatible avec vos politiques DAP existantes (créées lors de l'utilisation de HostScan 4.3.x ou d'une version antérieure). Vous devez effectuer une procédure de migration unique pour adapter votre configuration.

L'apparition de l'action **Incompatible** indique que la mise à niveau de HostScan a été lancée et que vous devez maintenant migrer votre configuration. Reportez-vous au Guide de migration AnyConnect Hostscan de la version 4.3.x à la version 4.6.x pour obtenir des instructions détaillées.

Étape 2 Pour inclure certains attributs de point terminal de pare-feu personnel ou de protection contre les programmes malveillants, cliquez sur le lien de **configuration** près du haut du volet. Ce lien ne s'affiche pas si vous avez déjà activé ces deux fonctionnalités.

Étape 3 Affichez la liste des DAP précédemment configurées.

Les champs suivants sont affichés dans le tableau :

- ACL Prior (priorité d'ACL) : affiche la priorité de l'enregistrement DAP.

  L'ASA utilise cette valeur pour séquencer logiquement les listes de contrôle d'accès lors de l'agrégation des listes de contrôle d'accès réseau et de type Web à partir de plusieurs enregistrements DAP. L'ASA

classe les enregistrements du numéro de priorité le plus élevé au plus bas, le plus bas au bas du tableau. Les numéros plus élevés ont une priorité plus élevée, c'est-à-dire qu'un enregistrement DAP avec une valeur de 4 a une priorité plus élevée qu'un enregistrement avec une valeur de 2. Vous ne pouvez pas les trier manuellement.

- Name (nom) : affiche le nom de l'enregistrement DAP.
- Network ACL List (Liste d'ACL de réseau) : affiche le nom de l'ACL de pare-feu qui s'applique à la session.
- Web-Type ACL List (Liste d'ACL de type Web) : affiche le nom de l'ACL VPN SSL qui s'applique à la session.
- Description : décrit l'objectif de l'enregistrement DAP.

Étape 4 Cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) pour Ajouter ou modifier une politique d'accès dynamique, à la page 185.

Étape 5 Cliquez sur **Apply** (Appliquer) pour enregistrer votre configuration DAP.

Étape 6 Recherchez une politique d'accès dynamique (DAP) en utilisant le champ **Find** (Rechercher).

Commencez à taper dans le champ et l'outil recherchera les caractères de début de chaque champ du tableau DAP pour une correspondance. Vous pouvez utiliser des caractères génériques pour élargir votre recherche.

Par exemple, taper **`sal`** dans le champ **Find** (Rechercher) correspond à une DAP nommée `Sales`, mais pas à une DAP nommée `Wholesalers`. Si vous tapez **`*sal`** dans le champ **Find** (Rechercher), la recherche trouve la première instance de **`Sales`** ou **`Wholesalers`** dans le tableau.

Étape 7 Tester les politiques d'accès dynamique, à la page 187 pour vérifier votre configuration.

Ajouter ou modifier une politique d'accès dynamique

Procédure

Étape 1 Démarrez ASDM et choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Network (Client) Access (Accès réseau [client])** ou **Clientless SSL VPN Access (Accès VPN SSL sans client)** > **Dynamic Access Policies (Politiques d'accès dynamique)** > **Add** or **Edit (Ajouter ou Modifier).**

Étape 2 Indiquez un nom (obligatoire) et une description (facultatif) de cette politique d'accès dynamique.

- Le **Policy Name** (Nom de la politique) est une chaîne de 4 à 32 caractères ; aucun espace n'est autorisé.
- Vous pouvez utiliser un maximum de 80 caractères dans le champ DAP **Description**.

Étape 3 Dans le champ **ACL Priority** (Priorité ACL), définissez une priorité pour la politique d'accès dynamique.

L'appareil de sécurité applique les politiques d'accès dans l'ordre que vous définissez ici, le numéro le plus élevé ayant la priorité la plus élevée. Les valeurs de 0 à 2 147 483 647 sont valides. La valeur par défaut est 0.

Étape 4 Précisez vos critères de sélection pour cette DAP :

a) Dans le volet Selection Criteria (Critères de sélection), utilisez la liste déroulante ANY/ALL/NONE (sans étiquette) pour choisir si un utilisateur doit avoir une, toutes ou aucune des valeurs d'attribut AAA que vous configurez pour utiliser cette politique d'accès dynamique, ainsi que satisfaire à chaque attribut de point terminal.

   Les entrées en double ne sont pas autorisées. Si vous configurez un enregistrement DAP sans attribut AAA ou de point terminal, l'ASA le sélectionne toujours, puisque tous les critères de sélection sont satisfaits.

b) Cliquez sur **Add** or **Edit** (Ajouter ou Modifier) dans le champ AAA Attributes (Attributs AAA) pour Configurer les critères de sélection des attributs AAA dans une DAP, à la page 188.

c) Cliquez sur **Add** or **Edit** (Ajouter ou Modifier) dans la zone Endpoint Attributes (Attributs de point terminal) pour Configurer les critères de sélection des attributs de point terminal dans une DAP, à la page 191.

d) Cliquez sur le champ **Advanced** (Avancé) pour #unique_179. Cette fonctionnalité nécessite une connaissance du langage de programmation Lua.

   - AND/OR (ET/OU) : cliquez pour définir la relation entre les règles de sélection de base et les expressions logiques que vous saisissez ici, c'est-à-dire si les nouveaux attributs ajoutent ou remplacent les attributs AAA et de point terminal déjà définis. La valeur par défaut est ET.
   - Logical Expressions (Expressions logiques) : vous pouvez créer plusieurs instances de chaque type d'attribut de point terminal. Saisissez du texte LUA de forme libre qui définit les nouveaux attributs de sélection AAA et/ou de point terminal. ASDM ne valide pas le texte que vous saisissez ici; il copie simplement ce texte dans le fichier XML DAP et l'ASA le traite, en rejetant les expressions qu'il ne peut pas analyser.

     Pour en savoir plus sur l'importation ou l'exportation d'un fichier *dap.xml*, consultez Importer et exporter le fichier XML DAP entre deux ASA, à la page 186.

Étape 5 Précisez les **Access/Authorization Policy Attributes** (Attributs de politique d'accès/d'autorisation pour cette DAP).

Les valeurs d'attribut que vous configurez ici remplacent les valeurs d'autorisation du système AAA, y compris celles des utilisateurs existants, des groupes, des groupes de tunnels et des enregistrements de groupe par défaut. Consultez Configurer les attributs de la politique d'accès DAP et d'autorisation, à la page 211.

Étape 6 Cliquez sur **OK**.

Importer et exporter le fichier XML DAP entre deux ASA

La configuration des politiques d'accès dynamique (DAP) de l'ASA est stockée dans un fichier appelé *dap.xml* dans la mémoire flash de l'ASA. Le fichier contient les attributs de sélection des politiques DAP.

Remarque Bien que vous puissiez exporter le fichier *dap.xml*, le modifier (si vous connaissez la syntaxe xml) et le réimporter, soyez très prudent, car vous pouvez forcer ASDM à cesser de traiter les enregistrements DAP si vous avez mal configuré quelque chose. Il n'y a pas d'interface de ligne de commande pour manipuler cette partie de la configuration.

Utilisez ces étapes pour importer et exporter le fichier *dap.xml* entre deux ASA.

La procédure utilise l'exemple d'exportation d'un fichier *dap.xml* à partir d'ASA#1 et d'importation sur ASA#2.

Pour en savoir plus sur le traitement des fichiers sur ASA à l'aide d'ASDM, consultez la section sur la *gestion des fichiers* du *Guide de configuration d'ASDM pour les opérations générales Cisco ASA*.

Procédure

Étape 1 Effacez le fichier *dap.xml* sur l'ASA#2.

a) Enregistrez la configuration ASA#2 et *dap.xml* en externe sur un serveur tftp ou ftp.

b) Quittez ASDM pour ASA#2.

Remarque
Vous pouvez également utiliser l'option ASDM (**ASDM)** > **Tools (Outils)** > **Back Up Configurations (Sauvegarder les configurations)** > **DAP Configurations (Configurations DAP)**pour enregistrer le fichier *dap.xml*.

Vous pouvez également renommer ou supprimer le fichier *dap.xml* dans la mémoire flash ASA #2.

Étape 2 Sur l'invite de commande ASA#2, saisissez la commande **clear configure dynamic-access-policy-record** pour supprimer les configurations d'enregistrement DAP.

Étape 3 Exportez le fichier *dap.xml* à partir de la mémoire flash ASA#1 et importez-le sur la mémoire flash ASA#2.

Étape 4 Utilisez la commande **dynamic-access-policy-record** pour configurer les entrées d'enregistrement DAP d'ASA#1 sur ASA#2.

Étape 5 Sur l'ASA#2, activez le DAP à l'aide de la commande **dynamic-access-policy-config activate**.

Remarque
Vous pouvez également relancer ASDM pour ASA#2 afin d'activer la configuration DAP.

Étape 6 Relancez l'ASDM sur l'ASA#2.
Les nouvelles politiques DAP sont configurées dans l'ASA n° 2.

Tester les politiques d'accès dynamique

Ce volet vous permet de tester la récupération de l'ensemble des enregistrements DAP configurés sur le périphérique en spécifiant des paires de valeurs d'attribut d'autorisation.

Procédure

Étape 1 Utilisez les boutons Add/Edit (Ajouter/Modifier) associés aux tableaux d'attributs AAA et d'attributs de point terminal pour spécifier des paires de valeurs d'attribut.

Les boîtes de dialogue qui s'affichent lorsque vous cliquez sur ces boutons Add/Edit (Ajouter/Modifier) sont similaires à celles des boîtes de dialogue Add/Edit AAA Attributes (Ajouter/Modifier des attributs AAA) et Add/Edit Endpoint Attributes (Ajouter/Modifier des attributs de point terminal).

Étape 2 Cliquez sur le bouton **Test** (Tester).

Le sous-système DAP sur le périphérique fait référence à ces valeurs lors de l'évaluation des attributs de sélection AAA et de point terminal pour chaque enregistrement. Les résultats s'affichent dans la zone **Test Results** (Résultats du test).

Configurer les critères de sélection des attributs AAA dans une DAP

DAP complète les services AAA en fournissant un ensemble limité d'attributs d'autorisation qui peuvent remplacer les attributs fournis par AAA. Vous pouvez spécifier les attributs AAA à partir de la hiérarchie des attributs Cisco AAA ou à partir de l'ensemble complet d'attributs de réponse que l'ASA reçoit d'un serveur RADIUS ou LDAP. L'ASA sélectionne les enregistrements DAP en fonction des informations d'autorisation AAA pour l'utilisateur et des informations d'évaluation de la posture pour la session. L'ASA peut choisir plusieurs enregistrements DAP en fonction de ces informations, qu'il regroupe ensuite pour créer des attributs d'autorisation DAP.

Procédure

Pour configurer les attributs AAA comme critères de sélection des enregistrements DAP, dans la boîte de dialogue Add/Edit AAA Attributes (Ajouter/Modifier les attributs AAA), définissez les attributs Cisco, LDAP ou RADIUS que vous souhaitez utiliser. Vous pouvez définir ces attributs à la valeur = ou != de la valeur que vous saisissez. Il n'y a aucune limite au nombre d'attributs AAA pour chaque enregistrement DAP. Pour de plus amples renseignements, voir Définitions des attributs AAA, à la page 191.

AAA Attributes Type (Type d'attributs AAA) : utilisez la liste déroulante pour choisir les attributs Cisco, LDAP ou RADIUS.

- Cisco : fait référence aux attributs d'autorisation des utilisateurs stockés dans le modèle hiérarchique AAA. Vous pouvez spécifier un petit sous-ensemble de ces attributs pour les attributs de sélection AAA dans l'enregistrement DAP. Il s'agit notamment de :
  - Group Policy (Stratégie de groupe) : nom de la stratégie de groupe associée à la session utilisateur VPN. Peut être défini localement sur l'appareil de sécurité ou envoyé par un serveur RADIUS/LDAP en tant qu'attribut IETF-Class (25). Maximum de 64 caractères.
  - Assigned IP Address (Adresse IP affectée) : saisissez l'adresse IPv4 que vous souhaitez affecter à la politique.
  - Assigned IPv6 Address (Adresse IPv6 affectée) : saisissez l'adresse IPv6 que vous souhaitez affecter à la politique.
  - Connection Profile (Profil de connexion) : nom du groupe de tunnels. Maximum de 64 caractères.
  - Username (Nom d'utilisateur) : nom d'utilisateur de l'utilisateur authentifié. Maximum de 64 caractères. S'applique si vous utilisez l'authentification/autorisation locale, RADIUS, LDAP ou tout autre type d'authentification (par exemple, RSA/SDI), domaine NT, etc.).
  - =/!= : égal à/non égal à.

- LDAP : le client LDAP (appareil de sécurité) stocke toutes les paires de valeurs d'attributs de réponse LDAP natives dans une base de données associée à la session AAA pour l'utilisateur. Le client LDAP écrit les attributs de réponse dans la base de données dans l'ordre dans lequel il les reçoit. Il supprime tous les attributs suivants avec ce nom. Ce scénario peut se produire lorsqu'un enregistrement d'utilisateur et un enregistrement de groupe sont tous deux lus à partir du serveur LDAP. Les attributs d'enregistrement d'utilisateur sont lus en premier et ont toujours la priorité sur les attributs d'enregistrement de groupe.

  Pour prendre en charge l'appartenance au groupe Active Directory, le client LDAP AAA fournit un traitement spécial de l'attribut de réponse LDAP memberOf. L'attribut AD memberOf spécifie la chaîne DN d'un enregistrement de groupe dans AD. Le nom du groupe est la première valeur CN dans la chaîne DN. Le client LDAP extrait le nom de groupe à partir de la chaîne de nom distinctif et le stocke en tant qu'attribut AAA memberOf et dans la base de données d'attributs de réponse en tant qu'attribut LDAP memberOf. S'il y a des attributs de memberOf supplémentaires dans le message de réponse LDAP, le nom de groupe est extrait de ces attributs et est combiné avec l'attribut AAA memberOf précédent pour former une chaîne de noms de groupe séparés par des virgules, également mise à jour dans la base de données des attributs de réponse.

  Dans le cas où la session d'accès à distance VPN à un serveur d'authentification/autorisation LDAP renvoie les trois groupes Active Directory suivants (énumérations de memberOf) :

  cn=Engineering,ou=People,dc=company,dc=com

  cn=Employees,ou=People,dc=company,dc=com

  cn=EastCoast,ou=People,dc=company,dc=com

  L'ASA traite trois groupes Active Directory : Engineering, Employees et EastCoast qui peuvent être utilisés dans n'importe quelle combinaison comme critères de sélection aaa.ldap.

  Les attributs LDAP comprennent un nom d'attribut et une paire de valeur d'attribut dans l'enregistrement DAP. Le nom de l'attribut LDAP est sensible à la syntaxe et à la casse. Si, par exemple, vous spécifiez l'attribut LDAP Department au lieu de ce que le serveur AD renvoie comme department, l'enregistrement DAP ne correspondra pas en fonction de ce paramètre d'attribut.

  Remarque
  Pour saisir plusieurs valeurs dans le champ Value (Valeur), utilisez le point-virgule (;) comme délimiteur. Par exemple :

  eng;sale; cn=Audgen VPN,ou=USERS,o=OAG

- RADIUS : le client RADIUS stocke toutes les paires de valeurs d'attribut de réponse RADIUS natives dans une base de données associée à la session AAA pour l'utilisateur. Le client RADIUS écrit les attributs de réponse dans la base de données dans l'ordre dans lequel il les reçoit. Il supprime tous les attributs suivants avec ce nom. Ce scénario peut se produire lorsqu'un enregistrement d'utilisateur et un enregistrement de groupe sont tous deux lus à partir du serveur RADIUS. Les attributs d'enregistrement d'utilisateur sont lus en premier et ont toujours la priorité sur les attributs d'enregistrement de groupe.

  Les attributs RADIUS comprennent un numéro d'attribut et une paire de valeurs d'attribut dans l'enregistrement DAP.

  Remarque
  Pour les attributs RADIUS, DAP définit l'ID d'attribut = 4096 + ID RADIUS.

  Par exemple :

  L'attribut RADIUS « Access Hours » a un ID Radius = 1, donc la valeur de l'attribut DAP = 4096 + 1 = 4097.

L'attribut RADIUS « Member Of » a un ID Radius = 146, donc la valeur de l'attribut DAP = 4096 + 146 = 4242.

- Les attributs LDAP et RADIUS comprennent :
  - Attribute ID (ID d'attribut) : nomme et numérote l'attribut. Maximum de 64 caractères.
  - Value (Valeur) : nom (LDAP) ou numéro (RADIUS) de l'attribut.

    Pour saisir plusieurs valeurs dans le champ Value (Valeur), utilisez le point-virgule (;) comme délimiteur. Par exemple : `eng;sale; cn=Audgen VPN,ou=USERS,o=OAG`
  - =/!= : égal à/non égal à.
- LDAP comprend le bouton Get AD Groups (Obtenir les groupes AD). Consultez Récupérer des groupes Active Directory, à la page 190.

Récupérer des groupes Active Directory

Vous pouvez interroger un serveur Active Directory pour connaître les groupes AD disponibles dans ce volet. Cette fonctionnalité s'applique uniquement aux serveurs Active Directory utilisant LDAP. Ce bouton interroge le serveur LDAP Active Directory pour obtenir la liste des groupes auxquels l'utilisateur appartient (énumérations de MemberOf). Utilisez les informations de groupe pour préciser les critères de sélection AAA de la politique d'accès dynamique.

Les groupes AD sont récupérés à partir du serveur LDAP à l'aide de la commande CLI **how-ad-groups** en arrière-plan. Le délai par défaut pendant lequel l'ASA attend une réponse du serveur est de 10 secondes. Vous pouvez ajuster cette heure à l'aide de la commande **group-search-timeout** en mode de configuration d'hôte aaa-server.

Vous pouvez modifier le niveau dans la hiérarchie Active Directory où la recherche commence en modifiant Group Base DN (DN de base de groupe) dans le volet Edit AAA Server (Modifier le serveur AAA). Vous pouvez également modifier le délai pendant lequel l'ASA attend une réponse du serveur dans la fenêtre. Pour configurer ces fonctionnalités, choisissez **Configuration > Remote Access VPN (VPN d'accès à distance) > AAA/Local Users (Utilisateurs AAA/locaux) > AAA Server Groups (Groupes de serveurs AAA) > Edit AAA Server (Modifier le serveur AAA)**.

Remarque Si le serveur Active Directory comporte un grand nombre de groupes, la liste des groupes AD récupérés (ou la sortie de la commande **show ad-groups**) peut être tronquée en fonction des limites de la quantité de données que le serveur peut contenir dans un paquet de réponse. Pour éviter ce problème, utilisez la fonction de filtre pour réduire le nombre de groupes signalés par le serveur.

AD Server Group (groupe de serveurs AD) : nom du groupe de serveurs AAA pour récupérer les groupes AD.

Filter By (Filtrer par) : spécifiez un groupe ou le nom partiel d'un groupe pour réduire les groupes affichés.

Group Name (Nom du groupe) : liste des groupes AD récupérés du serveur.

Définitions des attributs AAA

Le tableau suivant définit les noms d'attributs de sélection AAA qui sont disponibles pour une utilisation DAP. Le champ Attribute Name (nom d'attribut) vous montre comment saisir chaque nom d'attribut dans une expression logique LUA, ce que vous pouvez faire dans la section Advanced (Avancé) du volet Ajouter/Modifier une Politique d'accès dynamique.

Type d'attribut	Nom de l'attribut	Source	Valeur	Longueur maximale de la chaîne	Description
Cisco	aaa.cisco.grouppolicy	AAA	chaîne	64	Nom de la stratégie de groupe sur l'ASA ou envoyé par un serveur Radius/LDAP en tant qu'attribut IETF-Class (25)
	aaa.cisco.ipaddress	AAA	number	-	Adresse IP affectée pour les clients VPN de tunnel complet (IPsec, L2TP/IPsec, module SSL VPN Anyconnect)
	aaa.cisco.tunnelgroup	AAA	chaîne	64	Nom du profil de connexion ou nom du groupe de tunnels
	aaa.cisco.username	AAA	chaîne	64	Nom de l'utilisateur authentifié (s'applique si vous utilisez l'authentification/l'autorisation locale)
LDAP	aaa.ldap.<*label*>	LDAP	chaîne	128	Valeur d'attribut LDAP
RADIUS	aaa.radius.<number>	RADIUS	chaîne	128	Paire de valeurs d'attribut RADIUS

Configurer les critères de sélection des attributs de point terminal dans une DAP

Les attributs de point terminal contiennent des informations sur l'environnement système du point terminal, les résultats de l'évaluation de la posture et les applications. L'ASA génère dynamiquement un ensemble d'attributs de point terminal lors de l'établissement de la session et stocke ces attributs dans une base de données associée à la session. Chaque enregistrement DAP spécifie les attributs de sélection de point terminal qui doivent être satisfaits pour que l'ASA le choisisse pour une session. L'ASA sélectionne uniquement les enregistrements DAP qui satisfont toutes les conditions configurées.

Avant de commencer

- La configuration des attributs de point terminal en tant que critères de sélection pour les enregistrements DAP fait partie d'un processus plus vaste vers Configurer des politiques d'accès dynamique, à la page 184. Passez en revue cette procédure avant de configurer les attributs de point terminal comme critères de sélection pour les DAP.

- Pour des informations détaillées sur les attributs de point terminal, consultez Définitions des attributs de point terminal, à la page 201.
-
- Pour des informations détaillées sur la façon dont HostScan/Secure Firewall Posture vérifie les programmes de protection contre les programmes malveillants et de pare-feu personnel qui résident en mémoire, consultez DAP et programmes de protection contre les programmes malveillants et pare-feu personnel, à la page 200.

Procédure

Étape 1 Cliquez sur **Add** or **Edit** (Ajouter ou modifier) et ajoutez l'un des attributs de point terminal suivants comme critères de sélection.

Vous pouvez créer plusieurs instances de chaque type d'attribut de point terminal. Il n'y a aucune limite au nombre d'attributs de point terminal pour chaque enregistrement DAP.

- Ajouter un attribut de point terminal Anti-Malware/ à une DAP, à la page 193
- Ajouter un attribut d'application à une DAP, à la page 193
- Ajouter les attributs de point terminal Secure Client à une DAP, à la page 194
- Ajouter un attribut de point terminal de fichier à une DAP, à la page 195
- Ajouter un attribut de point terminal de périphérique à une DAP, à la page 196
- Ajouter un attribut de point terminal NAC à une DAP, à la page 197
- Ajouter un attribut de point terminal de système d'exploitation à une DAP, à la page 197
- Ajouter un attribut de point terminal Personal Firewall à une DAP, à la page 197
- Ajouter un attribut de point terminal à une DAP, à la page 198
- Ajouter un attribut de point terminal de processus à une DAP, à la page 198
- Ajouter un attribut de point terminal de registre à une DAP, à la page 199
- Ajouter plusieurs attributs d'authentification de certificat à DAP, à la page 200

Étape 2 Précisez les critères de correspondance de la politique DAP.

Pour chacun de ces types d'attribut de point terminal, décidez si la politique DAP doit exiger que l'utilisateur dispose de toutes les instances d'un type (Match All = AND, par défaut) ou d'une seule d'entre elles (Match Any = OR).

a) Cliquez sur **Logical Op** (Opération logique).
b) Choisissez **Match Any** (Correspondance avec n'importe lequel) (par défaut) ou **Match All** (Correspondance avec tous) pour chaque type d'attribut de point terminal.
c) Cliquez sur **OK**.

Étape 3 Retour à Ajouter ou modifier une politique d'accès dynamique, à la page 185.

Ajouter un attribut de point terminal Anti-Malware/ à une DAP

Avant de commencer

Si vous effectuez une mise à niveau d'HostScan 4.3.x vers HostScan 4.6.x ou une version ultérieure, vous devez migrer tous les attributs de point terminal AV/AS/FW existants vers les attributs de point terminal AM/FW de remplacement correspondants avant d'effectuer la mise à niveau. Consultez le guide de migration AnyConnect HostScan de la version 4.3.x à la version 4.6.x pour obtenir une procédure de mise à niveau et de migration complète.

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (Type d'attribut de point terminal), choisissez **Anti-Malware**.

Étape 2 Cliquez sur le bouton approprié **Installed (Installé) ou Not Installed (Non installé)** pour indiquer si l'attribut de point terminal sélectionné et les qualificateurs qui l'accompagnent (champs sous la colonne Name/Operation/Value [Nom/Opération/Valeur]) sont installés ou non installés.

Étape 3 Déterminez si vous souhaitez activer ou désactiver l'analyse en temps réel.

Étape 4 Dans la zone de liste **Vendor** (Fournisseur), choisissez le nom du fournisseur d'anti-programmes malveillants pour lequel vous effectuez le test.

Étape 5 Cochez la case **Product Description** (Description du produit) et choisissez dans la zone de liste le nom du produit du fournisseur pour lequel vous effectuez le test.

Étape 6 Cochez la case **Version** et définissez le champ d'opération sur Equal to (=) (Égal à [=]), not equal (!=) (différent de [!=]), less than (<) (inférieur à [<]), greater than (>) (supérieur à [>]), less than or equal to (<=) (inférieur ou égal à [<=]) ou greater than or equal to (>=) (supérieur ou égal à [>=]) le numéro de version du produit que vous choisissez dans la zone de liste **Version**.

Si le choix dans la zone de liste de versions comporte un x, comme par exemple 3.x, remplacez le x par un numéro de version spécifique, par exemple, 3.5.

Étape 7 Cochez la case **Last Update** (Dernière mise à jour). Indiquez le nombre de jours depuis la dernière mise à jour. Vous pouvez indiquer qu'une mise à jour doit se produire dans un délai inférieur à (<) ou supérieur (>) au nombre de jours que vous spécifiez.

Étape 8 Cliquez sur **OK**.

Ajouter un attribut d'application à une DAP

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (type d'attribut de terminal), choisissez **Application**.

Étape 2 Dans le champ d'opération du type de client, choisissez égal (=) ou non égal (!=).

Étape 3 Dans la zone de liste Client type (type de client), indiquez le type de connexion d'accès à distance pour lequel vous testez.

Étape 4 Cliquez sur **OK**.

Ajouter les attributs de point terminal Secure Client à une DAP

Les attributs de point terminal Secure Client, également connus sous le nom de posture mobile ou d'extensions d'identité AnyConnect (ACIDex), sont utilisés par le module VPN du client Cisco Secure Client pour communiquer les informations de posture à l'ASA. Les politiques d'accès dynamiques utilisent ces attributs de point terminal pour autoriser les utilisateurs.

Ces attributs de posture mobile peuvent être inclus dans une politique d'accès dynamique et appliqués sans installer HostScan/Secure Firewall Posture sur le point terminal.

Certains attributs de posture mobile ne sont pertinents que pour Secure Client exécuté sur les périphériques portables. Certains attributs de posture mobile sont pertinents à la fois pour les Secure Client exécuté sur les périphériques portables et les clients de poste de travail Secure Client.

Avant de commencer

La posture mobile nécessite une licence mobiSecure Client et une licence Premium Secure Client installées sur l'ASA. Les entreprises qui installent ces licences pourront appliquer les politiques DAP aux périphériques mobiles pris en charge en fonction des attributs DAP et d'autres attributs de point terminal existants. Cela inclut l'autorisation ou le refus de l'accès à distance à partir d'un appareil portable.

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (type d'attribut de terminal), choisissez Secure Client.

Étape 2 Cochez la case **Client Version** (Version du client) et définissez le champ d'opération pour qu'il soit égal à (=), non égal à (!=), inférieur à (<), supérieur à (>), inférieur ou égal à (<=) ou supérieur ou égal à (>=) au numéro de version Secure Client que vous spécifiez ensuite dans le champ **Client Version** (Version du client).

Vous pouvez utiliser ce champ pour évaluer la version du client sur les périphériques portables, tels que les téléphones portables et les tablettes, ou les appareils de bureau et d'ordinateur portable.

Étape 3 Cochez la case **Platform** (Plateforme) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) au système d'exploitation que vous choisissez ensuite dans la zone de liste **Platform** (Plateforme).

Vous pouvez utiliser ce champ pour évaluer le système d'exploitation sur les périphériques portables, tels que les téléphones portables et les tablettes, ainsi que le système d'exploitation sur les appareils de bureau et d'ordinateur portable. La sélection d'une plateforme active les champs d'attribut supplémentaires Device Type (Type de périphérique) et Device Unique ID (ID unique du périphérique).

Étape 4 Cochez la case **Platform Version** (Version de la plateforme) et définissez le champ d'opération pour qu'il soit égal à (=), non égal à (!=), inférieur à (<), supérieur à (>), inférieur ou égal à (<=) ou supérieur ou égal à (>=) au numéro de version du système d'exploitation que vous spécifiez ensuite dans le champ **Platform Version** (Version de la plateforme).

Si vous souhaitez créer un enregistrement DAP qui contient cet attribut, veillez à également spécifier une plateforme à l'étape précédente.

Étape 5 Si vous avez coché la case Platform (Plateforme), vous pouvez cocher la case **Device Type** (Type de périphérique). Définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) au périphérique que vous choisissez ensuite ou saisissez dans le champ **Device Type** (Type de périphérique).

Si vous avez un périphérique pris en charge qui ne figure pas dans le champ Device Type (Type de périphérique), vous pouvez le saisir dans le champ Device Type (Type de périphérique). Le moyen le plus fiable pour obtenir les informations sur le type de périphérique est d'installer Secure Client sur le point terminal, de vous connecter à l'ASA et d'effectuer un suivi DAP. Dans les résultats du suivi DAP, recherchez la valeur de **endpoint.anyconnect.devicetype**. Il s'agit de la valeur que vous devez saisir dans le champ Device Type (Type de périphérique).

Étape 6 Si vous avez coché la case Platform (Plateforme), vous pouvez cocher la case **Device Unique ID** (ID unique du périphérique). Définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) à l'ID unique du périphérique que vous spécifiez ensuite dans le champ **Device Unique ID** (ID unique du périphérique).

L'ID unique du périphérique distingue les périphériques individuels, ce qui vous permet de définir des politiques pour un périphérique portable particulier. Pour obtenir l'ID unique d'un périphérique, le périphérique doit se connecter à l'ASA et effectuer un suivi DAP. Recherchez la valeur **endpoint.anyconnect.deviceuniqueid**. Il s'agit de la valeur que vous devez saisir dans le champ Device Unique ID (ID unique du périphérique).

Étape 7 Si vous avez sélectionné une plateforme, vous pouvez ajouter des adresses MAC dans le champ **MAC Addresses Pool** (Ensemble d'adresses MAC). Définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) aux adresses MAC précisées. Chaque adresse MAC doit être au format xx-xx-xx-xx-xx-xx, où chaque 'x' est un caractère hexadécimal valide (0-9, A-F ou a-f). Les adresses MAC doivent être séparées par au moins un espace.

L'adresse MAC distingue les systèmes individuels, ce qui vous permet de définir des politiques pour un périphérique particulier. Pour obtenir l'adresse MAC d'un système, le périphérique doit se connecter à l'ASA et effectuer un suivi DAP. Recherchez la valeur **endpoint.anyconnect.macaddress**. Il s'agit de la valeur que vous devez saisir dans le champ MAC Addresses Pool (Ensemble d'adresses MAC).

Étape 8 Cliquez sur **OK**.

Ajouter un attribut de point terminal de fichier à une DAP

Avant de commencer

Avant de configurer un attribut de point terminal de fichier, définissez le fichier pour lequel vous souhaitez effectuer une analyse dans la fenêtre HostScan/Secure Firewall Posture.

Pour HostScan version 4.x, choisissez **Configuration > Remote Access VPN (VPN d'accès à distance) > Secure Desktop Manager (Gestionnaire Secure Desktop) > HostScan** dans ASDM. Pour Secure Firewall Posture version 5.x, choisissez **Configuration > Remote Access VPN (VPN d'accès à distance) > Posture (for Secure Firewall) (Posture (pour Secure Firewall)) > Posture Settings (Paramètres de posture)** dans ASDM.

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (Type d'attribut de point terminal), choisissez **File** (Fichier).

Étape 2 Sélectionnez le bouton radio approprié **Exists** (Existe) ou **Does not exist** N'existe pas) pour indiquer si l'attribut de point terminal sélectionné et les qualificateurs qui l'associent (champs sous les boutons Exists/Does not exist) doivent être présents ou non.

Étape 3 Dans la zone de liste **Endpoint ID** (ID de point terminal), choisissez dans la liste déroulante l'ID de terminal qui correspond à l'entrée de fichier pour laquelle vous souhaitez effectuer une analyse.

Les renseignements sur le fichier sont affichés sous la zone de liste des ID de terminal.

Étape 4 Cochez la case **Last Update** (Dernière mise à jour) et définissez le champ d'opération à inférieur à (<) ou supérieur à (>) un certain nombre de jours. Saisissez le nombre de jours anciens dans le champ **days** (jours) .

Étape 5 Cochez la case de **Checksum** (Somme de contrôle) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) la valeur de la somme de contrôle du fichier pour lequel vous testez.

Étape 6 Cliquez sur **Compute CRC32 Checksum** (Calculer la somme de contrôle CRC32) pour déterminer la valeur de la somme de contrôle du fichier pour lequel vous testez.

Étape 7 Cliquez sur **OK**.

Ajouter un attribut de point terminal de périphérique à une DAP

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (Type d'attribut de point terminal), choisissez **Device** (Périphérique).

Étape 2 Cochez la case **Host Name** (Nom d'hôte) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) au nom d'hôte du périphérique pour lequel vous effectuez le test. Utilisez uniquement le nom d'hôte de l'ordinateur, pas le nom de domaine complet (FQDN).

Étape 3 Cochez la case **MAC Address** (Adresse MAC) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) à l'adresse MAC de la carte d'interface réseau pour laquelle vous effectuez le test. Une seule adresse MAC par entrée. L'adresse MAC doit être au format XX-XX-XX-XX-XX-XX, où chaque X est un caractère hexadécimal.

Étape 4 Cochez la case **BIOS Serial Number** (Numéro de série du BIOS) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) à la valeur du numéro de série BIOS du périphérique pour lequel vous effectuez le test. Le format des numéros dépend du fabricant. Il n'y a aucune exigence de format.

Étape 5 Cochez la case **TCP/UDP Port Number** (Numéro de port TCP/UDP) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) au port TCP ou UDP dans l'état d'écoute pour lequel vous effectuez le test.

Dans la zone de liste déroulante TCP/UDP, choisissez le type de port pour lequel vous effectuez le test : TCP (IPv4), UDP (IPv4), TCP (IPv6) ou UDP (IPv6). Si vous testez pour plus d'un port, créez plusieurs règles d'attributs de point terminal individuelles dans le DAP et spécifiez un port dans chacune.

Étape 6 Cochez la case **Version of Secure Desktop** (CSD) (Version de Secure Desktop [CSD]) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) à la version de l'image HostScan/Secure Firewall Posture exécutée sur le terminal.

Étape 7 Cochez la case **Version of Endpoint Assessment** (Version de l'évaluation des points terminaux) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) à la version de l'évaluation des points terminaux (OPSWAT) pour laquelle vous effectuez le test.

Étape 8 Cliquez sur **OK**.

Ajouter un attribut de point terminal NAC à une DAP

Procédure

Étape 1 Dans la zone de liste **Attribute Type (type d'attribut)**, choisissez **NAC**.

Étape 2 Cochez la case **Posture Status** (état de la posture) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) la chaîne de jeton de posture reçue par l'ACS. Saisissez la chaîne du jeton de posture dans la zone Posture Status (État de la posture).

Étape 3 Cliquez sur **OK**.

Ajouter un attribut de point terminal de système d'exploitation à une DAP

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (Type d'attribut de terminal), choisissez **Operating System** (Système d'exploitation).

Étape 2 Cochez la case **OS Version** (Version du SE) et définissez le champ d'opération pour qu'il soit égal à (=) ou différent de (!=) du système d'exploitation Windows, Mac ou Linux que vous définissez dans la zone de liste **OS Version** (Version du SE).

Étape 3 Cochez la case **OS Update** (Mise à jour du SE) et définissez le champ d'opération pour qu'il soit égal à (=) ou différent de (!=) de la version de service Windows, Mac ou Linux pour le système d'exploitation que vous saisissez dans la zone de texte **OS Update** (Mise à jour du SE).

Étape 4 Cliquez sur **OK**.

Ajouter un attribut de point terminal Personal Firewall à une DAP

Avant de commencer

Si vous effectuez une mise à niveau d'HostScan 4.3.x vers HostScan 4.6.x ou une version ultérieure, vous devez migrer tous les attributs de point terminal AV/AS/FW existants vers les attributs de point terminal AM/FW de remplacement correspondants avant d'effectuer la mise à niveau. Consultez le guide de migration AnyConnect HostScan de la version 4.3.x à la version 4.6.x pour obtenir une procédure de mise à niveau et de migration complète.

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (Type d'attribut de terminal), choisissez **Operating System** (Système d'exploitation).

Étape 2 Cliquez sur le bouton **Installed (Installé) ou Not Installed (Non installé)** approprié pour indiquer si l'attribut de terminal sélectionné et les qualificateurs qui l'accompagnent (champs sous la colonne Name (Nom)/Operation (Opération)/Value (Valeur)) sont installés ou non installés.

Étape 3 Dans la zone de liste **Vendor** (Fournisseur), cliquez sur le nom du fournisseur de pare-feu personnel pour lequel vous effectuez le test.

Étape 4 Cochez la case **Product Description** (Description du produit) et choisissez dans la zone de liste le nom du produit du fournisseur pour lequel vous effectuez le test.

Étape 5 Cochez la case **Version** et définissez le champ d'opération sur Equal to (=) (Égal à), Not equal (!=) (Non égal à), Less than (<) (Inférieur à), Greater than (>) (Supérieur à), Less than or equal to (<=) (Inférieur ou égal à) ou Greater than or equal to (>=) (Supérieur ou égal à) le numéro de version du produit que vous choisissez dans la zone de liste **Version**.

Si le choix dans la zone de liste **Version** comporte un x, comme par exemple 3.x, remplacez le x par un numéro de version spécifique, par exemple, 3.5.

Étape 6 Cochez la case **Last Update** (Dernière mise à jour). Indiquez le nombre de jours depuis la dernière mise à jour. Vous pouvez indiquer qu'une mise à jour doit se produire dans un délai inférieur à (<) ou supérieur (>) au nombre de jours que vous spécifiez.

Étape 7 Cliquez sur **OK.**

Ajouter un attribut de point terminal à une DAP

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (Type d'attribut de point terminal), choisissez **Policy** (Politique).

Étape 2 Cochez la case **Location** (Emplacement) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) au profil d'emplacement Microsoft Windows Cisco Secure Desktop. Saisissez la chaîne de profil d'emplacement Microsoft Windows Cisco Secure Desktop dans la zone de texte **Location** (Emplacement).

Étape 3 Cliquez sur **OK**.

Ajouter un attribut de point terminal de processus à une DAP

Avant de commencer

Avant de configurer un attribut de point terminal de processus, définissez le processus que vous souhaitez analyser dans la fenêtre HostScan/Secure Firewall Posture pour Cisco Secure Desktop.

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (Type d'attribut de terminal), choisissez **Process** (Processus).

Étape 2 Cliquez sur le bouton **Exists (Existe) ou Does not exist (N'existe pas)** approprié pour indiquer si l'attribut de terminal sélectionné et les qualificateurs qui l'accompagnent (champs sous les boutons Exists (Existe) et Does not exist (N'existe pas)) doivent être présents ou non.

Étape 3 Dans la zone de liste **Endpoint ID** (ID de terminal), choisissez dans la liste déroulante l'ID du terminal pour lequel vous souhaitez effectuer l'analyse.

Les informations sur le processus d'ID de terminal sont affichées sous la zone de liste.

Étape 4 Cliquez sur **OK**.

Ajouter un attribut de point terminal de registre à une DAP

L'analyse des attributs de point terminal du registre s'applique aux systèmes d'exploitation Windows uniquement.

Avant de commencer

Avant de configurer un attribut de terminal de registre, définissez la clé de registre que vous souhaitez analyser dans la fenêtre HostScan/Secure Firewall Posture.

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (Type d'attribut de terminal), choisissez **Registry** (Registre).

Étape 2 Cliquez sur le bouton approprié **Exists (Existe) ou Does not exist (N'existe pas)** pour indiquer si l'attribut de terminal de **Registry** (Registre) et les qualificateurs qui l'accompagnent (champs sous les boutons Exists [Existe] et Does not exist [N'existe pas]) doivent être présents ou non.

Étape 3 Dans la zone de liste **Endpoint ID** (ID de terminal), choisissez dans la liste déroulante l'ID de terminal qui correspond à l'entrée de registre pour laquelle vous souhaitez effectuer une analyse.

Les informations du registre sont affichées sous la zone de liste Endpoint ID (ID de terminal).

Étape 4 Cochez la case **Value** (Valeur) et définissez le champ d'opération sur égal à (=) ou non égal à (!=).

Étape 5 Dans la première zone de liste **Value** (Valeur), identifiez la clé de registre comme un dword ou une chaîne.

Étape 6 Dans la deuxième zone de liste Value operation (Opération de valeur), saisissez la valeur de la clé de registre que vous analysez.

Étape 7 Si vous souhaitez ne pas tenir compte de la casse de l'entrée de registre lors de l'analyse, cochez la case. Si vous souhaitez que la recherche soit sensible à la casse, ne cochez pas la case.

Étape 8 Cliquez sur **OK**.

Ajouter plusieurs attributs d'authentification de certificat à DAP

Vous pouvez indexer chaque certificat pour permettre le référencement à l'un des certificats reçus, selon les règles configurées. En fonction de ces champs de certificat, vous pouvez configurer des règles DAP pour autoriser ou interdire les tentatives de connexion.

Procédure

Étape 1 Accédez à **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau (client)) > Dynamic Access Policies (Politiques d'accès dynamiques) > Add Endpoint Attribute (Ajouter un attribut de terminal)**.

Étape 2 Choisissez **Multiple Certificate Authentication** (Authentification de certificat multiple) comme type d'attribut de terminal dans le menu déroulant.

Étape 3 Configurez l'un des éléments suivants ou tous, selon vos préférences :

- Nom du sujet
- Nom de l'émetteur
- Autre nom de l'objet
- Numéro de série

Étape 4 Laissez le magasin de certificats à la valeur par défaut de Aucun pour autoriser les certificats de l'un ou l'autre du magasin ou choisissez lequel autoriser, uniquement l'utilisateur ou uniquement la machine. Si vous choisissez Utilisateur ou Machine, vous devez saisir le magasin d'origine du certificat. Ces informations sont envoyées par le client dans le protocole.

DAP et programmes de protection contre les programmes malveillants et pare-feu personnel

L'appareil de sécurité utilise une politique DAP lorsque les attributs de l'utilisateur correspondent aux attributs de AAA et de point terminal configurés. L'évaluation de préconnexion et HostScan/la posture de pare-feu sécurisé renvoient des informations au périphérique de sécurité sur les attributs de point terminal configurés, et le sous-système DAP utilise ces informations pour choisir un enregistrement DAP qui correspond aux valeurs de ces attributs.

La plupart des programmes de protection contre les programmes malveillants et de pare-feu personnel, mais pas tous, prennent en charge l'analyse active, ce qui signifie que les programmes sont résident en mémoire et donc toujours en cours d'exécution. HostScan/Secure Firewall Posture vérifie si un terminal est installé et s'il réside en mémoire, comme suit :

- Si le programme installé ne prend pas en charge l'analyse active, HostScan/Secure Firewall Posture signale la présence du logiciel. Le système DAP sélectionne les enregistrements DAP qui précisent le programme.
- Si le programme installé prend en charge l'analyse active et que l'analyse active est activée pour le programme, HostScan/Secure Firewall Posture signale la présence du logiciel. L'appareil de sécurité sélectionne à nouveau les enregistrements DAP qui précisent le programme.

- Si le programme installé prend en charge l'analyse active et que l'analyse active est désactivée pour le programme, HostScan/Secure Firewall Posture ignore la présence du logiciel. L'appareil de sécurité ne choisit pas les enregistrements DAP qui précisent le programme. De plus, la sortie de la commande **debug trace**, qui comprend de nombreuses informations sur DAP, n'indique pas la présence du programme, même s'il est installé.

Remarque Si vous effectuez une mise à niveau d'HostScan 4.3.x vers HostScan 4.6.x ou une version ultérieure, vous devez migrer tous les attributs de point terminal AV/AS/FW existants vers les attributs de point terminal AM/FW de remplacement correspondants avant d'effectuer la mise à niveau. Consultez le guide de migration AnyConnect HostScan de la version 4.3.x à la version 4.6.x pour obtenir une procédure de mise à niveau et de migration complète.

Définitions des attributs de point terminal

Les attributs de sélection de point terminal suivants sont disponibles pour une utilisation DAP. Le champ Attribute Name (Nom d'attribut) vous montre comment saisir chaque nom d'attribut dans une expression logique LUA utilisée dans la zone Advanced (Avancé) du volet Dynamic Access Policy Selection Criteria (Critères de sélection de la politique d'accès dynamique). La variable *label* identifie l'application, le nom de fichier, le processus ou l'entrée de registre.

Type d'attribut	Nom de l'attribut	Source	Valeur	Longueur maximale de la chaîne	Description
Antimalware	endpoint.am["*label*"].exists	Host ScanSecure Firewall Posture	vrai	—	Un programme de protection contre les programmes malveillants existe
	endpoint.am["*label*"].version		chaîne	32	Version
	endpoint.am["*label*"].description		chaîne	128	Description de l'antiprogramme malveillant
	endpoint.am["*label*"].lastupdate		nombre entier	—	Secondes depuis la mise à jour des définitions de programmes malveillants

Type d'attribut	Nom de l'attribut	Source	Valeur	Longueur maximale de la chaîne	Description
Pare-feu personnel	endpoint.pfw["*label*"].exists	Host Scan Secure Firewall Posture	vrai	—	Le pare-feu personnel existe
	endpoint.pfw["*label*"].version		chaîne	chaîne	Version
	endpoint.pfw["*label*"].description		chaîne	128	Description du pare-feu personnel
AnyConnect (Ne nécessite pas Host Scan Secure Firewall Posture)	Point terminaux.anyconnect. version du client	Point d'accès	version	—	version Secure Client
	Point terminaux.anyconnect. plateforme		chaîne	—	Système d'exploitation sur lequel Secure Client est installé
	Point terminaux.anyconnect. version de plateforme		version	64	Version du système d'exploitation sur lequel Secure Client est installé
	Point terminaux.anyconnect. type d'appareil		chaîne	64	Type de périphérique portable sur lequel Secure Client est installé
	endpoint.anyconnect. deviceuniqueid			64	ID unique du périphérique portable sur lequel Secure Client est installé
	endpoint.anyconnect. macaddress		chaîne	—	Adresse MAC du périphérique sur lequel Secure Client est installé L'adresse MAC doit être au format xx-xx-xx-xx-xx-xx, où chaque 'x' est un caractère hexadécimal
Application	endpoint.application. clienttype	Application	chaîne	—	Type de client : CLIENTLESS ANYCONNECT IPSEC L2TP

Type d'attribut	Nom de l'attribut	Source	Valeur	Longueur maximale de la chaîne	Description
Périphérique	endpoint.device. hostname	Point d'accès	chaîne	64	Nom d'hôte uniquement. Non FQDN
	endpoint.device.MAC		chaîne	—	Adresse MAC d'une carte d'interface réseau. Une seule adresse MAC par entrée L'adresse MAC doit être au format xxxx.xxxx.xxxx, où chaque x est un caractère hexadécimal.
	endpoint.device.id		chaîne	64	Numéro de série du BIOS Le format des numéros dépend du fabricant. Il n'y a aucune exigence de format
	endpoint.device.port		chaîne	—	État d'écoute du port TCP Vous pouvez définir un seul port par ligne Saisissez un entier entre 1 et 65 535.
	endpoint.device.protection_version		chaîne	64	Version de l'image HostScan/Secure Firewall Posture qu'ils utilisent
	endpoint.device. protection_extension		chaîne	64	Version de l'évaluation des points terminaux (OPSWAT)
Fichier	endpoint.file["*label*"].exists		vrai	—	Le fichier existe
	endpoint.file["label"]. endpointid				
	endpoint.file["*label*"]. lastmodified		nombre entier	—	Secondes écoulées depuis la dernière modification du fichier
	endpoint.file["*label*"]. crc.32		nombre entier	—	Hachage CRC32 du fichier

Type d'attribut	Nom de l'attribut	Source	Valeur	Longueur maximale de la chaîne	Description
NAC	endpoint.nac.status	NAC	chaîne	—	Chaîne d'état définie par l'utilisateur
Système d'exploitation	endpoint.os.version		chaîne	32	Système d'exploitation
	endpoint.os.servicepack		nombre entier	—	Service Pack pour Windows
Politique	endpoint.policy.location		chaîne	64	
Processus	endpoint. process["*label*"].exists		vrai	—	Le processus existe
	endpoint. process["*label*"].path		chaîne	255	Chemin complet du processus
Registre	endpoint. registry["*label*"].type		*dword string*	—	dword
	endpoint. registry["*label*"].value		chaîne	255	Valeur de l'entrée du registre
VLAN	endoint.vlan.type	CNA	chaîne	—	Type de VLAN : ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

Créer des critères de sélection DAP supplémentaires dans DAP à l'aide de LUA

Cette section fournit des informations sur la création d'expressions logiques pour les attributs AAA ou de point terminal. Sachez que cela nécessite une connaissance approfondie de LUA. Vous pouvez trouver des renseignements détaillés sur la programmation LUA à l'adresse suivante : http://www.lua.org/manual/5.1/manual.html.

Dans le champ Advanced (Avancé), vous saisissez du texte LUA de forme libre qui représente les opérations logiques AAA et/ou de sélection de point terminal. ASDM ne valide pas le texte que vous saisissez ici; il copie simplement ce texte dans le fichier de politique DAP, et l'ASA le traite en rejetant toute expression qu'il ne peut pas analyser.

Cette option est utile pour ajouter des critères de sélection autres que ceux possibles dans les zones des attributs AAA et de point terminal ci-dessus. Par exemple, bien que vous puissiez configurer l'ASA pour utiliser des attributs AAA qui satisfont un, tous ou aucun des critères spécifiés, les attributs de point terminal sont cumulatifs

et doivent tous être satisfaits. Pour permettre au périphérique de sécurité d'utiliser un attribut de point terminal ou un autre, vous devez créer les expressions logiques appropriées dans LUA et les saisir ici.

Les sections suivantes fournissent des instructions détaillées sur la création d'expressions LUA EVAL, ainsi que des exemples.

- Syntaxe pour la création d'expressions EVAL LUA, à la page 205
- Exemples d'expressions DAP EVAL, à la page 209
- Fonctions LUA supplémentaires, à la page 206

Syntaxe pour la création d'expressions EVAL LUA

Remarque Si vous devez utiliser le mode avancé, nous vous recommandons d'utiliser des expressions EVAL chaque fois que cela est possible pour des raisons de clarté, ce qui facilite la vérification du programme.

EVAL(<*attribute*> , <comparison>, {<*value*> | <*attribute*>}, [<type>])

<attribute>	Attribut AAA ou un attribut renvoyé par Cisco Secure Desktop, consultez Définitions des attributs de point terminal, à la page 201 pour les définitions d'attribut	
<comparison>	L'une des chaînes suivantes (guillemets requis)	
	« EQ »	égal à
	« NE »	n'est pas égal à
	« LT »	inférieur à
	« GT »	supérieur à
	« LE »	inférieur ou égal à
	« GE »	supérieur ou égal à
<value>	Une chaîne entre guillemets qui contient la valeur à laquelle comparer l'attribut	
<type>	L'une des chaînes suivantes (guillemets requis)	
	« string »	comparaison de chaînes sensibles à la casse
	""	comparaison de chaînes insensibles à la casse
	« integer »	comparaison de nombres, convertit les valeurs de chaîne en nombres
	« hex »	comparaison de nombres à l'aide de valeurs hexadécimales, convertit la chaîne hexadécimale en nombres hexadécimaux
	« version »	compare les versions du formulaire XHz où X, Y et Z sont des nombres

Procédures LUA pour HostScan 4.6 (et version ultérieure) et Secure Firewall Posture version 5

Script LUA pour « ANY » antiprogramme malveillant (endpoint.am) avec la dernière mise à jour

Utilisez le script LUA suivant pour vérifier s'il y a un produit ou un fournisseur de programmes malveillants « ANY » (endpoint.am). Des modifications peuvent s'appliquer pour s'adapter à un intervalle de dernière mise à jour différent. L'exemple suivant montre comment une dernière mise à jour doit avoir été effectuée en moins de 30 jours (2 592 000 secondes).

```
assert(function()
  for k,v in pairs(endpoint.am) do
    if(EVAL(v.activescan, "EQ", "ok", "string")and EVAL (v.lastupdate, "LT", "2592000",
"integer"))
     then
              return true
         end
  end
  return false
end)()
```

Script LUA pour pare-feu personnel « ANY » (tout)

Utilisez le script LUA suivant pour vérifier le produit ou le fournisseur de pare-feu « ANY » (endpoint.pfw) :

```
assert(function()
    for k,v in pairs(endpoint.pfw) do
         if (EVAL(v.enabled, "EQ", "ok", "string")) then
              return true
         end
    end
    return false
end)()
```

Fonctions LUA supplémentaires

Lorsque vous utilisez des politiques d'accès dynamiques, vous aurez peut-être besoin d'une plus grande flexibilité pour les critères de correspondance. Par exemple, vous pourriez vouloir appliquer une DAP différente en fonction des éléments suivants :

- CheckAndMsg est une fonction LUA que vous pouvez configurer DAP pour appeler. Il génère un message utilisateur en fonction d'une condition.
- Unité organisationnelle (OU) ou autre niveau de la hiérarchie pour l'objet utilisateur.
- Les noms de groupe qui suivent une convention de dénomination avec de nombreuses correspondances possibles peuvent nécessiter la possibilité d'utiliser un caractère générique.

Vous pouvez obtenir cette flexibilité en créant une expression logique LUA dans la section Avancé du volet DAP dans ASDM.

La fonction DAP CheckAndMsg

L'ASA affiche le message à l'utilisateur uniquement lorsque l'enregistrement DAP contenant la fonction LUA CheckAndMsg est sélectionné et entraîne la fin de la connexion.

La syntaxe de la fonction CheckAndMsg est la suivante :

```
CheckAndMsg(value, "<message string if value is true>", "<message string if value if false>")
```

Gardez à l'esprit les éléments suivants lors de la création des fonctions CheckAndMsg :

- CheckAndMsg renvoie la valeur transmise comme premier argument.
- Utilisez la fonction EVAL comme premier argument si vous ne souhaitez pas utiliser la comparaison de chaîne. Par exemple :

  ```
  (CheckAndMsg((EVAL(...)) , "true msg", "false msg"))
  ```

  CheckandMsg renvoie le résultat de la fonction EVAL, et l'appareil de sécurité l'utilise pour déterminer s'il faut choisir l'enregistrement DAP. Si l'enregistrement est sélectionné et entraîne la terminaison de la connexion, le périphérique de sécurité affiche le message approprié.

Exemple de correspondance basée sur OU

DAP peut utiliser de nombreux attributs renvoyés par un serveur LDAP dans une expression logique. Consultez la section sur le suivi DAP pour obtenir un exemple de sortie de celui-ci, ou exécutez un suivi DAP de débogage.

Le serveur LDAP renvoie le nom distinctif (DN) de l'utilisateur. Cela identifie implicitement l'endroit du répertoire où se trouve l'objet utilisateur. Par exemple, si le DN de l'utilisateur est CN=Example User, OU=Admins, dc=cisco, dc=com, cet utilisateur se trouve dans OU=Admins, dc=cisco, dc=com. Si tous les administrateurs se trouvent dans cette unité ou dans tout conteneur inférieur à ce niveau, vous pouvez utiliser une expression logique pour correspondre à ce critère comme suit :

```
assert(function()
   if ( (type(aaa.ldap.distinguishedName) == "string") and
        (string.find(aaa.ldap.distinguishedName, "OU=Admins,dc=cisco,dc=com$") ~= nil) )
then
       return true
   end
   return false
end)()
```

Dans cet exemple, la fonction string.find permet une expression régulière. Utilisez le caractère $ à la fin de la chaîne pour ancrer cette chaîne à la fin du champ distinguishedName.

Exemple d'appartenance à un groupe

Vous pouvez créer une expression logique de base pour la mise en correspondance de modèle de l'appartenance au groupe AD. Comme les utilisateurs peuvent être membres de plusieurs groupes, DAP analyse la réponse du serveur LDAP en entrées distinctes dans un tableau. Vous avez besoin d'une fonction avancée pour effectuer les opérations suivantes :

- Comparez le champ memberOf avec une chaîne (dans le cas où l'utilisateur n'appartient qu'à un seul groupe).
- Répétez l'itération sur chaque champ memberOf renvoyé si les données renvoyées sont de type « table ».

La fonction que nous avons écrite et testée à cette fin est indiquée ci-dessous. Dans cet exemple, si un utilisateur est membre d'un groupe se terminant par « -stu », il correspond à cette DAP.

```
assert(function()
   local pattern = "-stu$"
   local attribute = aaa.ldap.memberOf
   if ((type(attribute) == "string") and
       (string.find(attribute, pattern) ~= nil)) then
       return true
   elseif (type(attribute) == "table") then
       local k, v
       for k, v in pairs(attribute) do
           if (string.find(v, pattern) ~= nil) then
               return true
           end
       end
   end
   return false
end)()
```

Exemple de refus d'accès

Vous pouvez utiliser la fonction suivante pour refuser l'accès en l'absence d'un programme antimalware. Utilisez-le avec une DAP dont l'action est définie pour terminer.

```
assert(
    function()
for k,v in pairs(endpoint.am) do

        if (EVAL(v.exists, "EQ", "true", "string")) then

            return false

        end
    end
    return CheckAndMsg(true, "Please install antimalware software before connecting.", nil)
end)()
```

Si un utilisateur sans programme antimalware tente de se connecter, DAP affiche le message suivant :

```
Please install antimalware software before connecting.
```

Exemple d'authentification à certificats multiples

Vous pouvez définir un caractère générique pour le CN de l'émetteur avec l'authentification à certificats multiples dans les règles DAP.

Si vous avez configuré deux certificats émis à deux machines différentes par deux autorités de certification différentes (par exemple abc.cisco.com et xyz.cisco.com), la règle DAP doit avoir une condition d'authentification de plusieurs certificats dans laquelle le CN de l'émetteur est *.cisco.com ou cisco.com.

Vous pouvez utiliser la fonction suivante pour définir une règle DAP pour un certificat avec le caractère générique issuer_cn cisco.com pour les certificats utilisateur et machine :

```
assert(
 function()
  if ((string.find(endpoint.cert[1].issuer.cn[0], "cisco.com") ~= nil) and
   (string.find(endpoint.cert[2].issuer.cn[0], "cisco.com") ~= nil)) then
     return true;
 end
 return false;
end)()
```

Exemples d'expressions DAP EVAL

Étudiez ces exemples pour obtenir de l'aide dans la création d'expressions logiques dans LUA :

Description	Exemple
Vérifications LUA des points terminaux pour Windows 10	`(EVAL(endpoint.os.version,"EQ","Windows 10","string"))`
LUA de point terminal vérifie une correspondance sur les types de clients CLIENTLESS ou CVC.	`(EVAL(endpoint.application.clienttype,"EQ","CLIENTLESS") or EVAL(endpoint.application.clienttype, "EQ","CVC"))`
LUA de point terminal vérifie si un seul programme de protection contre les programmes malveillants Symantec Enterprise Protection est installé sur le PC de l'utilisateur et affiche un message si ce n'est pas le cas.	`(CheckAndMsg(EVAL(endpoint.am["538"].description,"NE","Symantec Endpoint Protection","string"),"Symantec Endpoint Protection was not found on your computer", nil))`
LUA de point terminal vérifie les versions de McAfee Endpoint Protection de 10 à 10.5.3 et les versions ultérieures à 10.6.	`(EVAL(endpoint.am["1637"].version,"GE","10","version") and EVAL(endpoint.am["1637"].version,"LT","10.5.4","version") or EVAL(endpoint.am["1637"].version,"GE","10.6","version"))`
LUA de point terminal vérifie si les définitions de l'antiprogramme malveillant McAfee ont été mises à jour au cours des 10 derniers jours (864000 s) et affiche un message si une mise à jour est nécessaire.	`(CheckAndMsg(EVAL(endpoint.am["1637"].lastupdate,"GT","864000","integer"),"Update needed! Please wait for McAfee to load the latest dat file.", nil))`

Description	Exemple
Vérifiez un correctif rapide spécifique après que le suivi de débogage DAP retourne : endpoint.os.windows.hotfix["KB923414"] = "true";	(CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"],"NE","true"), "The required hotfix is not installed on your PC.",nil))

Vérifier les programmes de protection contre les programmes malveillants et fournir des messages

Vous pouvez configurer des messages afin que les utilisateurs finaux soient au courant des problèmes de leur logiciel anti-programme malveillant et soient en mesure de les résoudre. Si l'accès est autorisé, l'ASA affiche tous les messages générés dans le processus d'évaluation DAP sur la page du portail. Si l'accès est refusé, l'ASA collecte tous les messages pour le DAP qui ont causé l'état « terminer » et les affiche dans le navigateur sur la page de connexion.

L'exemple suivant montre comment utiliser cette fonctionnalité pour vérifier l'état de Symantec Endpoint Protection.

1. Copiez et collez l'expression LUA suivante dans le champ Advanced (Avancé) du volet Add/Edit Dynamic Access Policy (Ajouter/Modifier une politique d'accès dynamique) (cliquez sur la double flèche à l'extrémité droite pour développer le champ).

```
(CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint
Protection","string") and EVAL(endpoint.am["538"].activescan,"NE","ok","string") "Symantec
 Endpoint Protection is disabled. You must enable before being granted access", nil))
```

2. Dans le même champ Advanced (Avancé), cliquez sur le bouton **OR** (OU).
3. Dans la section Attributs d'accès ci-dessous, dans l'onglet **Action** le plus à gauche, cliquez sur **Terminate** (Terminer).
4. Connectez-vous à partir d'un PC sur lequel Symantec Endpoint Protection est installé, mais dont Symantec Endpoint Protection est désactivé. Le résultat attendu est que la connexion n'est pas autorisée et que l'utilisateur verra le message « Symantec Endpoint Protection est désactivé. Vous devez l'activer avant de vous accorder l'accès ».

Vérifier les programmes de protection contre les programmes malveillants et les définitions antérieures à 2 jours

Cet exemple vérifie la présence des programmes anti-programme malveillant Symantec et McAfee et si les définitions de virus sont antérieures à 2 jours (172 800 secondes). Si les définitions sont antérieures à 2 jours, l'ASA met fin à la session avec un message et des liens pour la correction. Pour effectuer cette tâche, procédez comme suit.

1. Copiez et collez l'expression LUA suivante dans le champ Advanced (Avancé) du volet Add/Edit Dynamic Access Policy (Ajouter/Modifier une politique d'accès dynamique) :

```
(CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint
Protection","string") and EVAL(endpoint.am["538"].lastupdate,"GT","172800","integer"),
"Symantec Endpoint Protection Virus Definitions are Out of Date. You must run LiveUpdate
 before being granted access", nil)) or
(CheckAndMsg(EVAL(endpoint.am["1637"].description,"EQ","McAfee Endpoint
Security","string") and EVAL(endpoint.am["1637"].lastupdate,"GT","172800","integer"),
"McAfee Endpoint Security Virus Definitions are Out of Date. You must update your McAfee
 Virus Definitions before being granted access", nil))
```

2. Dans le même champ Advanced (Avancé), cliquez sur **AND** (ET).
3. Dans la section Attributs d'accès ci-dessous, dans l'onglet Action (Action) le plus à gauche, cliquez sur **Terminate** (Terminer).
4. Connectez-vous à partir d'un PC doté de programmes anti-programme malveillant Symantec et McAfee avec des versions antérieures à 2 jours.

   Le résultat attendu est que la connexion n'est pas autorisée et qu'un message est présenté à l'utilisateur indiquant que les définitions de virus sont obsolètes.

Configurer les attributs de la politique d'accès DAP et d'autorisation

Cliquez sur chacun des onglets et configurez les champs contenus.

Procédure

Étape 1 Sélectionnez l'onglet **Action** pour spécifier le traitement spécial à appliquer à une connexion ou une session spécifique.

- Continue (Continuer) : cliquez pour appliquer les attributs de politique d'accès à la session.
- Quarantine (Quarantaine) : au moyen de la mise en quarantaine, vous pouvez restreindre un client particulier qui a déjà un tunnel établi par l'intermédiaire d'un VPN. L'ASA applique des listes de contrôle d'accès restreintes à une session pour former un groupe restreint, en fonction de l'enregistrement DAP sélectionné. Lorsqu'un point terminal n'est pas conforme à une politique définie par l'administrateur, l'utilisateur peut toujours accéder aux services de correction, mais des restrictions sont imposées à l'utilisateur. Après la correction, l'utilisateur peut se reconnecter, ce qui invoque une nouvelle évaluation de la posture. Si cette évaluation réussit, l'utilisateur se connecte. Ce paramètre nécessite une version Secure Client qui prend en charge les fonctionnalités de Cisco Secure Client/.
- Terminate (Mettre fin) : cliquez pour mettre fin à la session.
- User Message (Message utilisateur) : saisissez un message texte à afficher sur la page du portail lorsque cet enregistrement DAP est sélectionné. Maximum 490 caractères. Un message utilisateur s'affiche sous forme d'orbe jaune. Lorsqu'un utilisateur se connecte, il clignote trois fois pour attirer l'attention, puis il reste fixe. Si plusieurs enregistrements DAP sont sélectionnés et que chacun d'entre eux comporte un message d'utilisateur, tous les messages d'utilisateur s'affichent.

  Vous pouvez inclure des URL ou d'autres types de texte intégrés, ce qui nécessite l'utilisation des balises HTML appropriées. Par exemple : tous les sous-traitants lisent Instructions pour connaître la procédure de mise à niveau de votre logiciel anti-programme malveillant.

Étape 2 Sélectionnez l'onglet **Network ACL Filters** (Filtres d'ACL réseau) pour configurer les listes de contrôle d'accès réseau à appliquer à cet enregistrement DAP.

Une liste de contrôle d'accès pour DAP peut contenir des règles d'autorisation ou de refus, mais pas les deux. Si une liste de contrôle d'accès contient des règles d'autorisation et de refus, l'ASA la rejette.

- Liste déroulante Network ACL (ACL réseau) : sélectionnez des listes de contrôle d'accès réseau déjà configurées à ajouter à cet enregistrement DAP. Les listes de contrôle d'accès peuvent être n'importe quelle combinaison de règles d'autorisation et de refus. Ce champ prend en charge les listes de contrôle d'accès unifiées qui peuvent définir des règles d'accès pour le trafic réseau IPv4 et IPv6.
- **Manage** (Gérer) : cliquez pour ajouter, modifier et supprimer des listes de contrôle d'accès réseau.
- **Network ACL list** (Liste d'ACL réseau) : affiche les listes d'ACL réseau pour cet enregistrement DAP.
- **Add** (Ajouter) : cliquez pour ajouter l'ACL réseau sélectionnée dans la liste déroulante à la liste Network ACLs (ACL réseau) sur la droite.
- **Delete** (Supprimer) : cliquez pour supprimer une liste de contrôle d'accès réseau en surbrillance dans la liste Network ACLs (ACL réseau). Vous ne pouvez pas supprimer une liste de contrôle d'accès de l'ASA, sauf si vous l'avez d'abord supprimée des enregistrements DAP.

Étape 3 Sélectionnez l'onglet **Web-Type ACL Filters (clientless) (**Filtres d'ACL de type Web [sans client]) pour configurer les listes de contrôle d'accès de type Web à appliquer à cet enregistrement DAP. Une liste de contrôle d'accès pour DAP ne peut contenir que des règles d'autorisation ou de refus. Si une liste de contrôle d'accès contient des règles d'autorisation et de refus, l'ASA la rejette.

- Liste déroulante **Web-Type ACL** (ACL de type Web) : sélectionnez des listes de contrôle d'accès de type Web déjà configurées à ajouter à cet enregistrement DAP. Les listes de contrôle d'accès peuvent être n'importe quelle combinaison de règles d'autorisation et de refus.
- **Manage** (Gérer) : cliquez pour ajouter, modifier et supprimer des listes de contrôle d'accès de type Web.
- **Web-Type ACL list** (Liste d'ACL de type Web) : affiche les listes de contrôle d'accès de type Web pour cet enregistrement DAP.
- **Add** (Ajouter) : cliquez pour ajouter l'ACL de type Web sélectionnée dans la liste déroulante à la liste Web-Type ACLs (ACL de type Web) sur la droite.
- **Delete** (Supprimer) : cliquez pour supprimer une liste de contrôle d'accès de type Web dans la liste Web-Type ACLs (ACL de type Web). Vous ne pouvez pas supprimer une liste de contrôle d'accès de l'ASA, sauf si vous l'avez d'abord supprimée des enregistrements DAP.

Étape 4 Sélectionnez l'onglet **Functions** (Fonctions) pour configurer l'entrée et la navigation dans le serveur de fichiers, le proxy HTTP et l'entrée d'URL pour l'enregistrement DAP.

- **File Server Browsing** (Navigation dans le serveur de fichiers) : active ou désactive la navigation CIFS pour les serveurs de fichiers ou les fonctionnalités partagées.

  La navigation nécessite NBNS (Master Browser ou WINS). S'il échoue ou n'est pas configuré, nous utilisons le DNS. La fonctionnalité de navigation CIFS ne prend pas en charge l'internationalisation.
- **File Server Entry** (Entrée du serveur de fichiers) : permet ou interdit à un utilisateur de saisir les chemins et les noms du serveur de fichiers sur la page du portail. Lorsque cette option est activée, place le tiroir d'entrée du serveur de fichiers sur la page du portail. Les utilisateurs peuvent saisir directement les noms de chemin d'accès aux fichiers Windows. Ils peuvent télécharger, modifier, supprimer, renommer et déplacer des fichiers. Ils peuvent également ajouter des fichiers et des dossiers. Les partages doivent également être configurés pour l'accès des utilisateurs sur les serveurs Windows applicables. Il se peut que les utilisateurs doivent être authentifiés avant d'accéder aux fichiers, en fonction des exigences du réseau.

- **HTTP Proxy** (Proxy HTTP) : affecte le transfert d'un proxy HTTP vers le client. Le proxy est utile pour les technologies qui interfèrent avec une transformation appropriée du contenu, telles que Java, ActiveX et Flash. Il contourne la gestion tout en assurant l'utilisation continue du périphérique de sécurité. Le proxy transféré modifie automatiquement l'ancienne configuration du navigateur et redirige toutes les requêtes HTTP et HTTPS vers la nouvelle configuration du proxy. Il prend en charge virtuellement toutes les technologies côté client, y compris HTML, CSS, JavaScript, VBScript, ActiveX et Java. Le seul navigateur qu'il prend en charge est Microsoft Internet Explorer.
- **URL Entry** (Entrée URL) : autorise ou empêche un utilisateur d'entrer des URL HTTP ou HTTPS sur la page du portail. Si cette fonctionnalité est activée, les utilisateurs peuvent saisir des adresses Web dans la zone de saisie d'URL.

L'utilisation du VPN SSL ne garantit pas que la communication avec chaque site est sécurisée. Le VPN SSL garantit la sécurité de la transmission des données entre le PC ou le poste de travail de l'utilisateur distant et l'ASA sur le réseau de l'entreprise. Si un utilisateur accède ensuite à une ressource Web non HTTPS (située sur Internet ou sur le réseau interne), la communication de l'ASA d'entreprise avec le serveur Web de destination n'est pas sécurisée.

Dans une connexion VPN sans client, l'ASA agit comme proxy entre le navigateur Web de l'utilisateur final et les serveurs Web cibles. Lorsqu'un utilisateur se connecte à un serveur Web compatible avec le protocole SSL, l'ASA établit une connexion sécurisée et valide le certificat SSL du serveur. Le navigateur de l'utilisateur final ne reçoit jamais le certificat présenté, il ne peut donc pas examiner et valider le certificat. La mise en œuvre actuelle du VPN SSL ne permet pas la communication avec des sites qui présentent des certificats expirés. L'ASA n'effectue pas non plus la validation du certificat d'autorité de certification de confiance. Par conséquent, les utilisateurs ne peuvent pas analyser le certificat d'un serveur Web compatible avec le protocole SSL avant de communiquer avec celui-ci.

Pour limiter l'accès Internet pour les utilisateurs, choisissez Disable (Désactiver) dans le champ URL Entry (Entrée URL). Cela empêche les utilisateurs de VPN SSL de surfer sur le Web pendant une connexion VPN sans client.

- **Unchanged** (Non modifié) : cliquez pour utiliser les valeurs de la stratégie de groupe qui s'applique à cette session.
- **Enable/Disable** (Activer/Désactiver) : cliquez pour activer ou désactiver la fonctionnalité.
- **Auto-start** (Démarrage automatique) : cliquez pour activer le proxy HTTP et pour que l'enregistrement DAP démarre automatiquement les applets associées fonctionnalités.

Étape 5 Sélectionnez l'onglet **Port Forwarding Lists** pour configurer les listes de transfert de port pour les sessions utilisateur.

Le transfert de port permet aux utilisateurs distants du groupe d'accéder à des applications client/serveur qui communiquent sur les ports TCP/IP connus et fixes. Les utilisateurs distants peuvent utiliser des applications clientes installées sur leur ordinateur local et accéder en toute sécurité à un serveur distant qui prend en charge cette application. Cisco a testé les applications suivantes : Windows Terminal Services, Telnet, Secure FTP (FTP sur SSH), Perforce, Outlook Express et Lotus Notes. D'autres applications basées sur TCP peuvent également fonctionner, mais Cisco ne les a pas testées.

Remarque
Le transfert de port ne fonctionne pas avec certaines versions SSL/TLS.

Mise en garde
Assurez-vous que Sun Microsystems Java Runtime Environment (JRE) est installé sur les ordinateurs distants pour prendre en charge le transfert de port (accès aux applications) et les certificats numériques.

- **Port Forwarding** (Transfert de port) : sélectionnez une option pour les listes de transfert de port qui s'appliquent à cet enregistrement DAP. Les autres attributs dans ce champ ne sont activés que lorsque vous définissez le transfert de port sur activé ou sur démarrage automatique.
- **Unchanged** (Non modifié) : cliquez pour supprimer les attributs de la configuration en cours d'exécution.
- **Enable/Disable** (Activer/Désactiver) : cliquez pour activer ou désactiver le transfert de port.
- **Auto-start** (Démarrage automatique) : cliquez pour activer le transfert de port et pour que l'enregistrement DAP démarre automatiquement les applets de transfert de port associées listes de transfert de port.
- **Liste déroulante Port Forwarding List** (Liste de transfert de port) : sélectionnez les listes de transfert de port déjà configurées à ajouter à l'enregistrement DAP.
- **Nouveau...** : cliquez pour configurer de nouvelles listes de transfert de port.
- **Port Forwarding Lists** (sans étiquette) : affiche les listes de transfert de port pour l'enregistrement DAP.
- **Add** (Ajouter : cliquez pour ajouter la liste de transfert de port sélectionnée dans la liste déroulante à la liste Port Forwarding (Transfert de port) sur la droite.
- **Delete** (Supprimer) : cliquez pour supprimer la liste de transfert de port sélectionnée dans la liste Port Forwarding (Transfert de port). Vous ne pouvez pas supprimer une liste de transfert de port de l'ASA, sauf si vous l'avez d'abord supprimée des enregistrements DAP.

Étape 6 Sélectionnez l'onglet **Bookmarks** (Repères) pour configurer les signets pour certaines URL de session utilisateur.

- **Enable bookmarks** (Activer les signets) : cliquez pour les activer. Lorsque cette option n'est pas cochée, aucun signet ne s'affiche dans la page du portail pour la connexion.
- **Liste déroulante Bookmark** (Signet) : choisissez des signets déjà configurés à ajouter à l'enregistrement DAP.
- **Manage** (Gérer)... : cliquez pour ajouter, importer, exporter et supprimer des signets.
- **Bookmarks** (sans étiquette) : affiche les listes d'URL pour l'enregistrement DAP.
- **Add>>** (Ajouter>>) : cliquez pour ajouter le signet sélectionné dans la liste déroulante à la zone d'URL sur la droite.
- **Delete** (Supprimer) : cliquez pour supprimer le signet sélectionné dans la zone de liste d'URL. Vous ne pouvez pas supprimer un signet dans l'ASA, sauf si vous l'avez d'abord supprimé des enregistrements DAP.

Étape 7 Sélectionnez l'onglet **Access Method** (Méthode d'accès) pour configurer le type d'accès à distance autorisé.

- **Unchanged** (Non modifié) : continuez avec la méthode d'accès à distance actuelle.
- **Secure Client** : connexion à l'aide du module VPN AnyConnect de Cisco Secure Client

  .
- **Web-Portal** (Portail Web) : connexion avec le VPN sans client.
- **Both-default-Web-Portal** (Les deux par défaut—Portail Web) : connexion sans client ou via Secure Client, avec une valeur par défaut sans client.

- **Both-default-Secure Client** (Les deux par défaut) : connexion sans client ou via Secure Client, avec une valeur par défaut Secure Client.

Étape 8 Sélectionnez l'onglet **Secure Client** pour choisir l'état de l'indicateur VPN toujours activé.

- Always-On VPN for (VPN toujours activé pour) Secure Client :déterminez si le paramètre d'indicateur VPN toujours activé dans le profil de service Secure Client est inchangé, désactivé ou si le paramètre de profil Secure Client doit être utilisé.

  Ce paramètre nécessite une version de l'appareil Cisco Web Security qui fournit une prise en charge des licences de solution de mobilité sécu risée pour le module VPN AnyConnect de Cisco Secure Client. Il nécessite également une version Secure Client qui prend en charge les fonctionnalités de la « Secure Mobility Solution » (solution de mobilité sécurisée). Reportez-vous au *Guide de l'administrateur des clients VPN Cisco AnyConnect* pour obtenir plus d'informations.

Étape 9 Sélectionnez l'onglet **Custom Attributes** (Attributs personnalisés) Secure Client pour afficher et associer les attributs personnalisés définis précédemment à cette politique. Vous pouvez également définir des attributs personnalisés, puis les associer à cette politique.

Les attributs personnalisés sont envoyés à et utilisés par Secure Clientpour configurer des fonctionnalités telles que la mise à niveau retardée. Un attribut personnalisé a un type et une valeur nommée. Le type de l'attribut est défini en premier, puis une ou plusieurs valeurs nommées de ce type peuvent être définies. Pour en savoir plus sur les attributs personnalisés à configurer pour une fonctionnalité, consultez le *Guide de l'administrateur de Cisco* pour la version Secure Client que vous utilisez.

Les attributs personnalisés peuvent être prédéfinis dans **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau [client]) > Advanced (Avancé) > Custom Attributes (Attributs personnalisés)** Secure Client et **Custom Attribute Names** (Noms d'attributs personnalisés Secure Client). Les attributs personnalisés prédéfinis sont utilisés par les politiques d'accès dynamique et les stratégies de groupe.

Configurer l'autorisation SAML

Vous pouvez configurer les sélections d'autorisation SAML et de stratégies de groupe à l'aide de DAP, sans avoir à faire appel à un serveur externe (RADIUS ou LDAP) pour récupérer les attributs d'autorisation.

Le fournisseur d'identité SAML peut être configuré pour envoyer des attributs d'autorisation en plus des réclamations d'authentification. Le composant fournisseur de services SAML dans ASA interprète les déclarations SAML et effectue des sélections d'autorisations ou de stratégies de groupe en fonction des déclarations reçues. Les attributs d'assertion sont traités à l'aide des règles DAP configurées par ASDM.

L'attribut de stratégie de groupe doit utiliser le nom d'attribut **cisco_group_policy**. Cet attribut ne dépend pas de la configuration du DAP. Toutefois, si une DAP est configurée, elle peut être utilisée dans la politique DAP.

Sélection de stratégie de groupe

Lorsqu'un attribut **cisco_group_policy** est reçu, la valeur correspondante est utilisée pour sélectionner la stratégie de groupe de connexion.

Lorsqu'une connexion est établie, les informations de stratégie de groupe peuvent être extraites de plusieurs sources et combinées pour former une stratégie de groupe efficace qui est appliquée à la connexion.

Les scénarios suivants sont possibles tout en combinant les informations de stratégie de groupe reçues :

Stratégie de groupe reçue dans l'authentification SAML, autorisation NON configurée

Dans ce scénario, la stratégie de groupe effective est déterminée comme suit dans l'ordre de priorité décroissante :

1. Stratégie de groupe spécifiée dans l'attribut SAML.
2. La stratégie de groupe est spécifiée dans le groupe de tunnels.
3. Stratégie de groupe par défaut.

Stratégie de groupe reçue dans l'authentification SAML, autorisation configurée

Dans ce scénario, la stratégie de groupe effective est déterminée comme suit dans l'ordre de priorité décroissante :

1. Stratégie de groupe spécifiée dans les attributs d'autorisation.
2. Stratégie de groupe d'utilisateurs : utilisez la valeur renvoyée par le serveur d'autorisation, le cas échéant.
3. Stratégie de groupe d'utilisateurs : utilisez la valeur renvoyée dans l'attribut SAML.
4. Stratégie de groupe spécifiée dans le groupe de tunnels.
5. Stratégie de groupe par défaut.

Procédure

Étape 1 Dans ASDM, sélectionnez **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies** > **Add/Edit Dynamic Access Policy** (Configuration > VPN d'accès à distance > Accès au réseau [client] > Politiques d'accès dynamique > Ajouter/Modifier une politique d'accès dynamique).

Étape 2 Dans la zone de sélection des attributs AAA, cliquez sur **Ajouter** (Ajouter).

a) Dans la liste déroulante **AAA Attribute Type** (Type d'attribut AAA), sélectionnez SAML.
b) Précisez *memberOf* comme **Attribute ID** (ID d'attribut).
c) Saisissez la valeur de l'attribut **Value** (Valeur) de *memberOf* ou cliquez sur **Get AD Group** (Obtenir le groupe AD) si les groupes de serveurs AD sont configurés.

Pour configurer des groupes de serveurs AD supplémentaires, accédez à **Configuration** > **Remote Access VPN (VPN d'accès distant)** > **AAA/Local Users (AAA/Utilisateurs locaux)** > **AAA Server Groups (Groupes de serveurs AAA)**.

Pour configurer les attributs de sélection de stratégie de groupe, sélectionnez les paramètres suivants dans la même politique DAP ou dans une autre politique DAP, selon les besoins :

- **AAA Attribute Type** (Type d'attribut AAA : SAML
- **Attribute ID** (ID d'attribut) : cisco_group_policy
- **Value** (Valeur) : Nom de la stratégie de groupe

Étape 3 Cliquez sur **OK**.

Étape 4 Cliquez sur **OK** pour enregistrer la politique DAP.

Effectuer un suivi DAP

Un suivi DAP affiche les attributs de point terminal DAP pour tous les périphériques connectés.

Procédure

Étape 1 Connectez-vous à l'ASA à partir d'un terminal SSH et passez en mode d'exécution privilégié.

En mode d'exécution privilégié, l'ASA invite : `hostname#`.

Étape 2 Activez les débogages DAP pour afficher tous les attributs DAP de la session dans la fenêtre du terminal :

```
hostname# debug dap trace
endpoint.anyconnect.clientversion="0.16.0021";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.platformversion="4.1";
endpoint.anyconnect.devicetype="iPhone1,2";
endpoint.anyconnect.deviceuniqueid="dd13ce3547f2fa1b2c3d4e5f6g7h8i9j0fa03f75";
```

Étape 3 (Facultatif) Pour rechercher dans la sortie du suivi DAP, envoyez la sortie de la commande à un journal système. Pour en savoir plus sur la journalisation sur l'ASA, consultez *Configurer la journalisation* dans le *Guide de configuration ASDM des opérations générales Cisco ASA*.

Exemples de DAP

- Utiliser DAP pour définir les ressources réseau, à la page 217
- Utiliser DAP pour appliquer une ACL WebVPN, à la page 218
- Effectuer des vérifications CSD et appliquer les politiques via DAP, à la page 219

Utiliser DAP pour définir les ressources réseau

Cet exemple montre comment configurer les politiques d'accès dynamiques comme méthode de définition des ressources réseau pour un utilisateur ou un groupe. La politique DAP nommée Trusted_VPN_Access permet l'accès VPN sans client et l'accès au module VPN AnyConnect de Cisco Secure Client. La politique nommée Untrusted_VPN_Access autorise uniquement l'accès VPN sans client.

Procédure

Étape 1 Dans ASDM, accédez à **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Clientless SSL VPN Access (Accès VPN SSL sans client)** > **Dynamic Access Policies (Politiques d'accès dynamique)** > **Add/Edit Dynamic Access Policy (Ajouter/Modifier une politique d'accès dynamique)** > **Endpoint (Point terminal)**.

Étape 2 Configurez les attributs suivants pour chaque politique :

Attribut	Trusted_VPN_Access	Untrusted_VPN_Access
Politique de type d'attribut de point terminal	Fiable	Non fiable
Attributs de point terminal	ieexplore.exe	—
Évaluation avancée du point terminal	AntiVirus= attribut McAfee	
Emplacement CSD	Fiable	Non fiable
LDAP memberOf	Ingénierie, Responsables	Fournisseurs
ACL		ACL de type Web
Accès	**Secure Client** *et* **portail Web**	**Portail Web**

Utiliser DAP pour appliquer une ACL WebVPN

DAP peut appliquer directement un sous-ensemble d'attributs de politique d'accès, y compris les ACL réseau (pour IPsec et Secure Client), les listes d'URL et les fonctions. Elle ne peut pas appliquer directement, par exemple, une bannière ou la liste de tunnels fractionnés, que les stratégies de groupe appliquent. Les onglets Access Policy Attributes (Attributs de politique d'accès) dans le volet Add/Edit Dynamic Access Policy (Ajouter/modifier une politique d'accès dynamique) fournissent un menu complet des attributs appliqués directement par DAP.

Active Directory/LDAP stocke l'appartenance aux stratégies de groupe des utilisateurs sous la forme de l'attribut « memberOf » dans l'entrée utilisateur. Définissez une DAP de sorte que, pour un utilisateur du groupe AD (memberOf) = Engineering, l'ASA applique une ACL de type Web configurée.

Procédure

Étape 1 Dans ASDM, accédez au volet Add AAA Attributes (Ajouter des attributs AAA), **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Clientless SSL VPN Access (Accès VPN SSL sans client)** > **Dynamic Access Policies (Politiques d'accès dynamique)** > **Add/Edit Dynamic Access Policy (Ajouter/modifier une politique d'accès dynamique)** > **section** > **AAA Attributes (Attributs AAA)** > **Add AAA Attribute (Ajouter un attribut AAA)**.

Étape 2 Pour le type d'attribut AAA, utilisez la liste déroulante pour choisir **LDAP**.

Étape 3 Dans le champ Attribute ID, saisissez memberOf, exactement comme vous le voyez ici. La casse est importante.

Étape 4 Dans le champ Value (Valeur), utilisez la liste déroulante pour choisir =, puis dans le champ adjacent, saisissez Engineering.

Étape 5 Dans la zone Access Policy Attributes (Attributs de politique d'accès) du volet, cliquez sur l'onglet Web-Type ACL Filters (Filtres ACL de type Web).

Étape 6 Utilisez la liste déroulante Web-Type ACL pour choisir l'ACL que vous souhaitez appliquer aux utilisateurs du groupe AD (memberOf) = Engineering.

Effectuer des vérifications CSD et appliquer les politiques via DAP

Cet exemple crée une DAP qui vérifie qu'un utilisateur appartient à deux groupes AD/LDAP spécifiques (Engineering et Employees) et à un groupe de tunnel ASA spécifique. Il applique ensuite une liste de contrôle d'accès à l'utilisateur.

Les listes de contrôle d'accès que DAP applique contrôlent l'accès aux ressources. Elles remplacent toute liste de contrôle d'accès définie dans la stratégie de groupe sur l'ASA. En outre, l'ASA applique les règles d'hérédité de Stratégie de groupe AAA et les attributs habituels pour ceux que DAP ne définit pas ou ne contrôle pas, comme les listes de tunnellisation fractionnée, les bannières et le DNS.

Procédure

Étape 1 Dans ASDM, allez au volet Ajouter des attributs AAA, **Configuration** > **Accès VPN à distance** > **Accès VPN SSL sans client** > **Politiques d'accès dynamique** > **Ajouter/Modifier une politique d'accès dynamique** > **section Attributs AAA** > **Ajouter un attribut AAA**.

Étape 2 Pour le type d'attribut AAA, utilisez la liste déroulante pour choisir LDAP.

Étape 3 Dans le champ Attribute ID (ID d'attribut), saisissez memberOf, exactement comme vous le voyez ici. La casse est importante.

Étape 4 Dans le champ Value (Valeur), utilisez la liste déroulante pour choisir =, puis dans le champ adjacent, saisissez Engineering.

Étape 5 Dans le champ Attribute ID (ID d'attribut), saisissez memberOf, exactement comme vous le voyez ici. La casse est importante.

Étape 6 Dans le champ Value (Valeur), utilisez la liste déroulante pour choisir =, puis dans le champ adjacent, saisissez Employees (Employés).

Étape 7 Pour le type d'attribut AAA, utilisez la liste déroulante pour choisir Cisco.

Étape 8 Cochez la case Tunnel group (Groupe de tunnels), utilisez la liste déroulante pour choisir =, puis dans la liste déroulante adjacente, choisissez le groupe de tunnels approprié (politique de connexion).

Étape 9 Dans l'onglet Network ACL Filters (Filtres ACL réseau) de la zone Access Policy Attributes (Attributs de politique d'accès), choisissez les listes de contrôle d'accès à appliquer aux utilisateurs qui répondent aux critères DAP définis dans les étapes précédentes.

Utiliser DAP pour vérifier la sécurité des jetons de session

Lorsque l'ASA authentifie une demande de connexion VPN à partir de Secure Client, l'ASA renvoie un jeton de session au client. À partir d'AnyConnect 4.9 (MR1), l'ASA et Secure Client prennent en charge un mécanisme qui offre une sécurité renforcée pour le jeton de session. Vous devez configurer une DAP pour vous assurer que Secure Client prend en charge la sécurité par jeton de session.

Utilisez cette DAP avec les paramètres d'attributs de point terminal et le script LUA pour rejeter les tentatives de connexion à partir de versions Secure Client qui ne prennent pas en charge la sécurité par jeton.

Procédure

Étape 1 Dans ASDM, sélectionnez **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies** > **Add/Edit Dynamic Access Policy** (Configuration > VPN d'accès à distance > Accès au réseau [client] > Politiques d'accès dynamique > Ajouter/Modifier une politique d'accès dynamique).

Étape 2 Dans la zone de sélection des attributs de terminal, cliquez sur **Add** (Ajouter).

a) Dans la liste déroulante **Endpoint Attribute Type** (Type d'attribut de terminal), sélectionnez Application.
b) Pour **Client Type** (Type de client), sélectionnez l'opérateur equals (=) [égal à (=)], puis sélectionnez une valeur Secure Client dans la liste déroulante.
c) Cliquez sur **OK**.

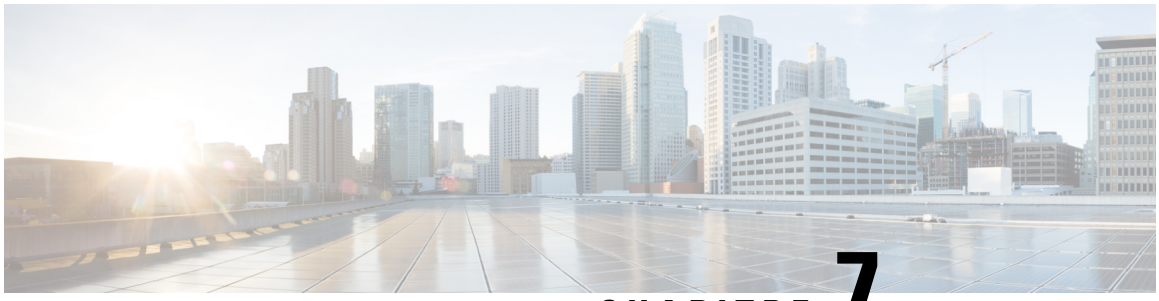
Étape 3 Configurez les critères de sélection **Advanced** (Avancés) :

a) Sélectionnez l'opérateur **AND** (ET).
b) Ajoutez l'expression logique **Add the Logical Expression** (Ajouter l'expression logique).

```
(type(endpoint.anyconnect.session_token_security)~="string" or
EVAL(endpoint.anyconnect.session_token_security,"NE","true","string"))
```

Étape 4 Dans la zone **Action**, sélectionnez **Terminate** (Terminer).

Étape 5 Ajoutez un User Message (Message utilisateur) facultatif et cliquez sur **OK**.



CHAPITRE 7

Serveur proxy de messagerie

Les serveurs proxy de messagerie étendent la capacité de messagerie à distance aux utilisateurs de VPN SSL sans client. Lorsque les utilisateurs tentent d'établir une session par courriel par l'intermédiaire du serveur proxy de messagerie, le client de messagerie établit un tunnel à l'aide du protocole SSL.

Les protocoles du serveur proxy de messagerie sont les suivants :

POP3S

POP3S est l'un des serveurs proxy de messagerie pris en charge par le VPN SSL sans client. Par défaut, l'appareil de sécurité est à l'écoute du port 995, et les connexions sont automatiquement autorisées vers le port 995 ou vers le port configuré. Le serveur proxy POP3 autorise uniquement les connexions SSL sur ce port. Une fois le tunnel SSL établi, le protocole POP3 démarre, puis l'authentification a lieu. POP3S permet de recevoir des courriels.

IMAP4S

IMAP4S est l'un des serveurs proxy de messagerie pris en charge par le VPN SSL sans client. Par défaut, l'appareil de sécurité est à l'écoute du port 993, et les connexions sont automatiquement autorisées vers le port 993 ou vers le port configuré. Le serveur proxy IMAP4 autorise uniquement les connexions SSL sur ce port. Une fois le tunnel SSL établi, le protocole IMAP4 démarre, puis l'authentification a lieu. IMAP4S permet de recevoir des courriels.

SMTPS

SMTPS est l'un des serveurs proxy de messagerie pris en charge par le VPN SSL sans client. Par défaut, l'appareil de sécurité est à l'écoute du port 988, et les connexions sont automatiquement autorisées vers le port 988 ou le port configuré. Le serveur proxy SMTPS autorise uniquement les connexions SSL sur ce port. Après l'établissement du tunnel SSL, le protocole SMTPS démarre, puis l'authentification a lieu. SMTPS permet d'envoyer des courriels.

Configurer le serveur proxy de messagerie

Exigences du serveur proxy de messagerie

- Les utilisateurs qui accèdent au courriel à partir d'emplacements locaux et distants par l'intermédiaire du serveur proxy de messagerie ont besoin de comptes de messagerie distincts dans leur programme de messagerie pour l'accès local et à distance.
- Les sessions de proxy de messagerie nécessitent l'authentification de l'utilisateur.

Définir les groupes de serveurs AAA

Procédure

Étape 1 Accédez à **Configuration** > **Features (Fonctionnalités de configuration)** > **VPN** > **E-mail Proxy (Serveur proxy de messagerie VPN)** > **AAA**.

Étape 2 Choisissez l'onglet approprié (POP3S, IMAP4S ou SMTPS) pour associer les groupes de serveurs AAA et configurer la stratégie de groupe par défaut pour ces sessions.

- AAA Server Groups (Groupes de serveurs AAA) : cliquez pour accéder au panneau AAA Server Groups (Groupes de serveurs AAA) (Configuration > Features (Fonctionnalités) > Properties (Propriétés) > AAA Setup (Configuration AAA) > AAA Server Groups (Groupes de serveurs AAA)), où vous pouvez ajouter ou modifier des groupes de serveurs AAA.
- Group Policies (Stratégies de groupe) cliquez pour accéder au panneau Group Policy (Stratégie de groupe) (Configuration > Features (Fonctionnalités) > VPN (VPN) > General (Général) > Group Policy (Stratégie de groupe)), où vous pouvez ajouter ou modifier des stratégies de groupe.
- Authentication Server Group (Groupe de serveurs d'authentification) : sélectionnez le groupe de serveurs d'authentification pour l'authentification de l'utilisateur. La valeur par défaut est de n'avoir aucun serveur d'authentification configuré. Si AAA est défini comme méthode d'authentification (Configuration > Features (Fonctionnalités) > AAA (AAA) > VPN (VPN) > E-Mail Proxy (Serveur proxy de messagerie) > Authentication (Authentification)), vous devez configurer un serveur AAA et le choisir ici, sinon l'authentification échoue toujours.
- Authorization Server Group (Groupe de serveurs d'autorisation) : sélectionnez le groupe de serveurs d'autorisation pour l'autorisation de l'utilisateur. La valeur par défaut est de n'avoir aucun serveur d'autorisation configuré.
- Accounting Server Group (Groupe de serveurs de comptabilité) : sélectionnez le groupe de serveurs de comptabilité pour la comptabilité des utilisateurs. La valeur par défaut est de n'avoir aucun serveur de comptabilité configuré.
- Default Group Policy (Stratégie de groupe par défaut) : sélectionnez la stratégie de groupe à appliquer aux utilisateurs lorsque AAA ne renvoie pas d'attribut CLASSID. La longueur doit être comprise entre 4 et 15 caractères alphanumériques. Si vous ne spécifiez pas de stratégie de groupe par défaut et qu'il n'y a pas de CLASSID, l'ASA ne peut pas établir la session.

- Authorization Settings (Paramètres d'autorisation) : définissez les valeurs des noms d'utilisateur que l'ASA reconnaît pour l'autorisation. Cela s'applique aux utilisateurs qui s'authentifient à l'aide de certificats numériques et nécessitent une autorisation LDAP ou RADIUS.
  - Use the entire DN as the username (Utiliser le DN entier comme nom d'utilisateur) : sélectionnez cette option pour utiliser le nom distinctif pour l'autorisation.
  - Specify individual DN fields as the username (Préciser les champs DN individuels comme nom d'utilisateur) : sélectionnez cette option pour spécifier des champs DN particuliers pour l'autorisation de l'utilisateur.

    Vous pouvez choisir deux champs de nom distinctif, principal et secondaire. Par exemple, si vous choisissez EA, les utilisateurs s'authentifient en fonction de leur adresse courriel. Dans ce cas, un utilisateur portant le nom commun (CN) de John Doe et une adresse de courriel johndoe@cisco.com ne peut pas s'authentifier en tant que John Doe ou johndoe. Il doit s'authentifier en tant que johndoe@cisco.com. Si vous choisissez EA et O, M. Doe doit s'authentifier en tant que johndoe@cisco.com et Cisco Systems, Inc.
  - Primary DN Field (Champ DN principal) : sélectionnez le champ DN principal que vous souhaitez configurer pour l'autorisation. La valeur par défaut est CN. Les options disponibles sont les suivantes :

Champ DN	Définition
Pays (C)	L'abréviation du pays à deux lettres. Ces codes sont conformes aux abréviations de pays ISO 3166.
Nom usuel	Le nom d'une personne, d'un système ou d'une autre entité. Il s'agit du niveau le plus bas (le plus spécifique) dans la hiérarchie d'identification.
DNQ (Qualificatif du DN)	Un attribut de DN spécifique.
Adresses de courriel (EA)	L'adresse courriel de la personne, du système ou de l'entité qui possède le certificat.
GENQ (Qualificatif générationnel)	Un attribut générationnel tel que Jr., Sr. ou III.
Prénom (GN)	Le prénom du propriétaire du certificat.
Initiales (I)	Les premières lettres de chaque partie du nom du propriétaire du certificat.
Localité	La ville ou la localité où se trouve l'organisation.
Nom (N)	Le nom du propriétaire du certificat.
Organisation	Le nom de l'entreprise, de l'établissement, de l'agence, de l'association ou de toute autre entité.
Unité organisationnelle	Le sous-groupe dans l'organisation.
Numéro de série (SER)	Le numéro de série du certificat.
Nom de famille (SN)	Le nom de famille ou le nom de famille du propriétaire du certificat.
État/Province (S/P)	L'état ou la province où se trouve l'organisation.

Champ DN	Définition
Titre (T)	Le titre du propriétaire du certificat, par exemple, Dr.
Identifiant de l'utilisateur (UID)	Le numéro d'identification du propriétaire du certificat.

- Secondary DN Field (Champ DN secondaire) : (facultatif) sélectionnez le champ DN secondaire que vous souhaitez configurer pour l'autorisation. La valeur par défaut est (OU). Les options comprennent toutes celles du tableau précédent, avec l'ajout de **None** (Aucun), que vous choisissez si vous ne souhaitez pas inclure de champ secondaire.

Identifier les interfaces pour le serveur proxy de messagerie

L'écran Email Proxy Access (Accès au serveur proxy de messagerie) vous permet d'identifier les interfaces sur lesquelles configurer le serveur proxy de messagerie. Vous pouvez configurer et modifier des serveurs proxy de messagerie sur des interfaces individuelles, et vous pouvez configurer et modifier des serveurs proxy de messagerie pour une interface, puis appliquer vos paramètres à toutes les interfaces. Vous ne pouvez pas configurer de serveur proxy de messagerie pour les interfaces de gestion uniquement ou pour les sous-interfaces.

Procédure

Étape 1 Accédez à **Configuration** > **VPN** > **E-Mail Proxy** > **Access** (Configuration > VPN > Serveur proxy de messagerie > Accès) pour afficher ce qui est activé pour les interfaces.

- Interface : affiche les noms de toutes les interfaces configurées.
- POP3S Enabled (POP3S activé) : affiche si POP3S est activé pour l'interface.
- IMAP4S Enabled (IMAP4S activé) : affiche si IMAP4S est activé pour l'interface.
- SMTPS Enabled (SMTPS activé) : affiche si SMTPS est activé pour l'interface.

Étape 2 Cliquez sur **Edit** (Modifier) pour modifier les paramètres du serveur proxy de messagerie pour l'interface en surbrillance.

Configurer l'authentification pour le serveur proxy de messagerie

Configurez les méthodes d'authentification pour chacun des types de serveur proxy de messagerie.

Procédure

Étape 1 Accédez à **Configuration** > **Features** > **VPN** > **E-mail Proxy** > **Authentication** (Configuration > Fonctionnalités > VPN > Mandataire de messagerie > Authentification).

Étape 2 Choisissez parmi les multiples méthodes d'authentification :

- AAA —sélectionnez cette option pour exiger l'authentification AAA. Cette option nécessite un serveur AAA configuré. L'utilisateur présente un nom d'utilisateur, un serveur et un mot de passe. Les utilisateurs doivent présenter à la fois le nom d'utilisateur VPN et le nom d'utilisateur de courriel, séparés par le délimiteur de nom VPN, uniquement si les noms d'utilisateur sont différents l'un de l'autre.
- Certificate (Certificat) : sélectionnez cette option pour exiger l'authentification par certificat.

  Remarque
  L'authentification par certificat ne fonctionne pas pour les serveurs proxy de messagerie dans la version logicielle ASA actuelle.

  L'authentification par certificat exige que les utilisateurs disposent d'un certificat que l'ASA peut valider pendant la négociation SSL. Vous pouvez utiliser l'authentification par certificat comme seule méthode d'authentification pour le serveur proxy SMTPS. Les autres serveurs proxy de messagerie nécessitent deux méthodes d'authentification.

  L'authentification des certificats nécessite trois certificats, tous provenant de la même autorité de certification :

  - Un certificat d'autorité de certification sur l'ASA.

  - Un certificat d'autorité de certification sur le PC client.

  - Un certificat de navigateur Web sur le PC client, parfois appelé certificat personnel ou certificat de navigateur Web.
- Piggyback HTTPS (Authentification superposée HTTPS) : sélectionnez cette option pour exiger une authentification superposée.

  Ce schéma d'authentification exige qu'un utilisateur ait déjà établi une session VPN SSL sans client. L'utilisateur présente uniquement un nom d'utilisateur de courriel. Aucun mot de passe n'est requis. Les utilisateurs doivent présenter à la fois le nom d'utilisateur VPN et le nom d'utilisateur de courriel, séparés par le délimiteur de nom VPN, uniquement si les noms d'utilisateur sont différents l'un de l'autre.

  IMAP génère un nombre de sessions qui ne sont pas limitées par le nombre d'utilisateurs simultanés, mais qui sont prises en compte dans le nombre de connexions simultanées autorisées pour un nom d'utilisateur. Si le nombre de sessions IMAP dépasse ce maximum et que la connexion VPN SSL sans client expire, un utilisateur ne peut pas établir de nouvelle connexion par la suite. Il existe plusieurs solutions :

  Le courriel SMTPS utilise le plus souvent l'authentification superposée, car la plupart des serveurs SMTP ne permettent pas aux utilisateurs de se connecter.

  Remarque
  IMAP génère un nombre de sessions qui ne sont pas limitées par le nombre d'utilisateurs simultanés, mais qui sont prises en compte dans le nombre de connexions simultanées autorisées pour un nom d'utilisateur. Si le nombre de sessions IMAP dépasse ce maximum et que la connexion VPN SSL sans client expire, un utilisateur ne peut pas établir de nouvelle connexion par la suite. Il existe plusieurs solutions :

- L'utilisateur peut fermer l'application IMAP pour effacer les sessions avec l'ASA, puis établir une nouvelle connexion VPN SSL sans client.

  L'administrateur peut augmenter les connexions simultanées pour les utilisateurs IMAP (Configuration > Features > VPN > General > Group Policy > Edit Group Policy > General [Configuration > Fonctionnalités > VPN > Général > Stratégie de groupe > Modifier la stratégie de groupe > Général]).

  – Désactivez l'authentification HTTPS/empilage pour le serveur proxy de messagerie.

- Mailhost (hôte de messagerie) : (SMTPS uniquement) sélectionnez cette option pour exiger l'authentification de l'hôte de messagerie. Cette option s'affiche uniquement pour SMTPS, car POP3S et IMAP4S effectuent toujours l'authentification de l'hôte de messagerie. Il nécessite le nom d'utilisateur de courriel, le serveur et le mot de passe de l'utilisateur.

Identifier les serveurs proxy

Ce panneau Default Server (Serveur par défaut) vous permet d'identifier les serveurs proxy auprès de l'ASA et de configurer un serveur par défaut, un port et une limite de session non authentifiée pour les serveurs proxy de messagerie.

Procédure

Étape 1 Accédez à **Configuration** > **Features** > **(Fonctionnalités de configuration)** > **VPN** > **E-mail Proxy (Proxy de messagerie)** > **Default Servers (Serveurs par défaut).**

Étape 2 Configurez les champs suivants :

- Name or IP Address (Nom ou adresse IP) : saisissez le nom DNS ou l'adresse IP du serveur proxy de messagerie par défaut.
- Port : saisissez le numéro de port sur lequel l'ASA écoute le trafic du serveur proxy de messagerie. Les connexions sont automatiquement autorisées sur le port configuré. Le serveur proxy de messagerie autorise uniquement les connexions SSL sur ce port. Une fois le tunnel SSL établi, le serveur proxy de messagerie démarre, puis l'authentification a lieu.

  Les valeurs par défaut sont les suivantes :

  - 995 (pour POP3S)
  - 993 (pour IMAP4S)
  - 988 (pour SMTPS)

- Enable non-authenticated session limit (Activer la limite de session non authentifiée) : sélectionnez cette option pour restreindre le nombre de sessions de serveur proxy de messagerie non authentifiées. Vous permet de définir une limite pour les sessions en cours d'authentification, empêchant ainsi les attaques DOS. Lorsqu'une nouvelle session dépasse la limite définie, l'ASA met fin à la connexion non authentifiée la plus ancienne. S'il n'existe aucune connexion non authentifiée, la connexion en cours d'authentification la plus ancienne est terminée sans mettre fin aux sessions authentifiées.

Les connexions du serveur proxy de messagerie ont trois états :

- Unauthenticated (Non authentifié) : état des nouvelles connexions par courriel.
- Authenticating (Authentification) : état lorsque la connexion présente un nom d'utilisateur.
- Authenticated (Authentifié) : état lorsque l'ASA authentifie la connexion.

Configurer les délimiteurs

Ce panneau configure les délimiteurs de nom d'utilisateur/mot de passe et les délimiteurs de serveur pour l'authentification du serveur proxy de messagerie.

Procédure

Étape 1 Accédez à **Configuration** > **Features** > **(Fonctionnalités de configuration)** > **VPN** > **E-mail Proxy (Serveur proxy de messagerie VPN)** > **Delimiters (Délimiteurs).**

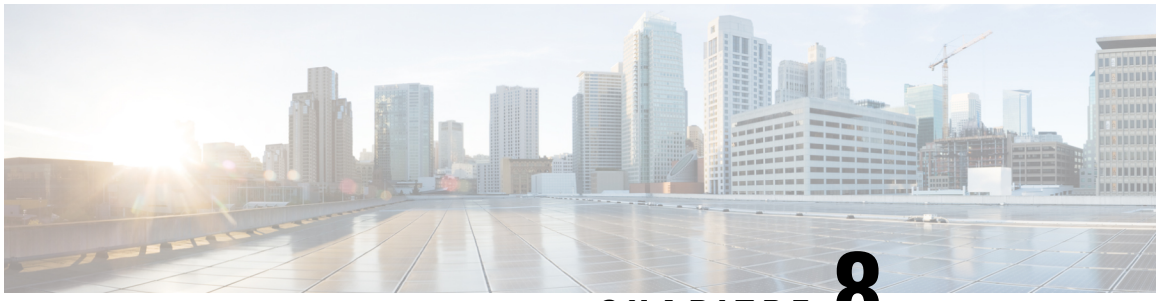
Étape 2 Configurez les champs suivants :

- Délimiteur de nom d'utilisateur/mot de passe : sélectionnez un délimiteur pour séparer le nom d'utilisateur du VPN du nom d'utilisateur du courriel. Les utilisateurs ont besoin des deux noms d'utilisateur lors de l'utilisation de l'authentification AAA pour le serveur proxy de messagerie, et le nom d'utilisateur du VPN et le nom d'utilisateur du courriel sont différents. Lorsqu'ils se connectent à une session de serveur proxy de messagerie, les utilisateurs saisissent les deux noms d'utilisateur, séparés par le délimiteur que vous configurez ici, ainsi que le nom du serveur de messagerie.

  Remarque
  Les mots de passe des utilisateurs du serveur proxy de messagerie VPN SSL sans client ne peuvent pas contenir de caractères utilisés comme délimiteur.

- Délimiteur de serveur : sélectionnez un délimiteur pour séparer le nom d'utilisateur du nom du serveur de messagerie. Il doit être différent du délimiteur de nom VPN. Les utilisateurs saisissent leur nom d'utilisateur et leur serveur dans le champ de nom d'utilisateur lorsqu'ils se connectent à une session de serveur proxy de messagerie.

  Par exemple, en utilisant : comme limiteur de nom VPN et @ comme limiteur de serveur, lors de la connexion à un programme de messagerie par courriel proxy, les utilisateurs saisiraient leur nom d'utilisateur au format suivant : vpn_username:e-mail_username@server.



CHAPITRE 8

Surveillance du VPN

Surveiller les graphiques de connexion VPN

Consultez les écrans suivants pour afficher les données de connexion VPN sous forme graphique ou tabulaire pour l'ASA.

Surveiller les tunnels IPsec

Monitoring (Surveillance) > VPN > VPN Connection Graphs (Graphiques de connexion VPN) > IPSec Tunnels (Tunnels IPSec)

Pour spécifier les graphiques et les tableaux des types de tunnels IPsec que vous souhaitez afficher ou préparer à l'exportation ou à l'impression.

Surveiller les sessions

Monitoring (Surveillance) > VPN > VPN Connection Graphs (Graphiques de connexion VPN) > Sessions (Sessions)

Pour préciser les graphiques et le tableau des types de sessions VPN que vous souhaitez afficher ou préparer à l'exportation ou à l'impression.

Surveiller les statistiques VPN

Consultez les écrans suivants pour afficher les paramètres et les statistiques détaillés pour une session d'accès à distance ou de réseau local (LAN) spécifique. Les paramètres et les statistiques varient selon le protocole de session. Le contenu des tableaux statistiques dépend du type de connexion que vous choisissez. Les tableaux de détail affichent tous les paramètres pertinents pour chaque session.

Fenêtre de surveillance de session

Monitoring (Supervision) > VPN > VPN Statistics (Statistiques VPN) > Sessions

Pour afficher les statistiques de session VPN pour l'ASA. Le contenu du deuxième tableau de ce volet dépend de la sélection dans la liste Filter By (Filtrer par).

Remarque Un administrateur peut faire le suivi du nombre d'utilisateurs à l'état inactif et peut consulter les statistiques. Les sessions inactives depuis le plus longtemps sont marquées comme inactives (et automatiquement déconnectées) afin que la capacité de licence ne soit pas atteinte et que de nouveaux utilisateurs puissent se connecter. Vous pouvez également accéder à ces statistiques à l'aide de la commande CLI **show vpn-sessiondb** (consultez la version appropriée du Guide de référence des commandes Cisco ASA).

- Tout accès à distance

  Indique que les valeurs dans ce tableau sont liées au trafic d'accès à distance (clients de logiciel et de matériel IPsec).

- Username/Connection Profile (Nom d'utilisateur/profil de connexion) : affiche le nom d'utilisateur ou le nom de connexion et le profil de connexion (groupe de tunnels) pour la session. Si le client utilise un certificat numérique pour l'authentification, le champ affiche le CN du sujet ou l'OU du sujet à partir du certificat.
- Group Policy Connection Profile (Profil de connexion de stratégie de groupe) : affiche le profil de connexion de stratégie de groupe de tunnel pour la session.
- Assigned IP Address/Public IP Address (Adresse IP affectée/adresse IP publique) : affiche l'adresse IP privée (« affectée ») affectée au client distant pour cette session. C'est également ce qu'on appelle l'adresse IP « interne » ou « virtuelle », et elle permet au client de sembler être un hôte sur le réseau privé. Affiche également l'adresse IP publique du client pour cette session d'accès à distance. C'est ce qu'on appelle l'adresse IP « externe ». Il est généralement affecté au client par le fournisseur de services Internet, et il permet au client de fonctionner en tant qu'hôte sur le réseau public.
- Ping : envoie un paquet ping ICMP (Packet Internet Groper) afin de tester la connectivité réseau. Plus précisément, l'ASA envoie un message de demande d'écho ICMP à un hôte sélectionné. Si l'hôte est accessible, il renvoie un message Echo Reply et l'ASA affiche un message Success (Réussite) avec le nom de l'hôte testé, ainsi que le temps écoulé entre l'envoi de la demande et la réception de la réponse. Si le système est inaccessible pour une raison quelconque (par exemple : hôte en panne, ICMP ne s'exécute pas sur l'hôte, route non configurée, routeur intermédiaire en panne, réseau en panne ou congestionné), l'ASA affiche un écran d'erreur avec le nom de l'hôte testé.
- Logout By (Déconnecter par) : choisit un critère à utiliser pour filtrer les sessions à déconnecter. Si vous choisissez une valeur autre que --All Sessions-- (Toutes les sessions), la zone située à droite de la liste Logout By (Déconnecter par) devient active. Si vous choisissez la valeur Protocol (Protocole) pour Logout By (Déconnecter par), la zone devient une liste dans laquelle vous pouvez choisir un type de protocole à utiliser comme filtre de déconnexion. La valeur par défaut de cette liste est IPsec. Pour tous les choix autres que Protocol (Protocole), vous devez fournir une valeur appropriée dans cette colonne.

Surveiller les sessions actives VPN

Monitoring (Supervision) > VPN > VPN Statistics (Statistiques de VPN) > Sessions

Pour l'affichage des sessions Secure Client triées par nom d'utilisateur, adresse IP, type d'adresse ou adresse publique.

Surveiller les détails des sessions VPN

Monitoring (Supervision) > VPN > VPN Statistics (Statistiques VPN) > Sessions > Details (Détails)

Pour afficher les paramètres de configuration, les statistiques et les informations d'état de la session sélectionnée.

- Résultat NAC et jeton de posture

L'ASDM affiche les valeurs dans cette colonne uniquement si vous avez configuré le contrôle d'admission au réseau sur l'ASA.

- Accepted (Accepté) : l'ACS a validé avec succès la posture de l'hôte distant.
- Rejected (Rejeté) : l'ACS n'a pas pu valider avec succès la posture de l'hôte distant.
- Exempté : l'hôte distant est exempté de la validation de la posture selon la liste d'exceptions de validation de la posture configurée sur l'ASA.
- Non-Responsive (Sans réponse) : l'hôte distant n'a pas répondu au message EAPoUDP Hello.
- Hold-off (Attente) : l'ASA a perdu la communication EAPoUDP avec l'hôte distant après la validation réussie de la posture.
- N/A (S/O) : la NAC est désactivée pour l'hôte distant conformément à la stratégie de groupe VPN NAC.
- Unknown (Inconnu) : la validation de la posture est en cours.

Le jeton de posture est une chaîne de texte d'information qui peut être configurée sur le serveur de contrôle d'accès. L'ACS télécharge le jeton de posture sur l'ASA à titre informatif afin de faciliter la surveillance, la création de rapports, le débogage et la journalisation du système. Le jeton de posture typique qui suit le résultat NAC est le suivant : Healthy (En bonne santé), Checkup (Contrôle), Quarantine (Quarantaine), Infected (Infecté) ou Unknown (Inconnu).

L'onglet Details (Détails) du volet Session Details (Détails de la session) affiche les colonnes suivantes :

- ID : ID unique affecté dynamiquement à la session. L'ID sert d'index ASA pour la session. Il utilise cet index pour conserver et afficher les renseignements sur la session.
- Type : type de session : IKE, IPsec ou NAC.
- Local Addr., Subnet Mask, Protocol, Port, Remote Addr., Subnet Mask, Protocol et Port : adresses et ports affectés à l'homologue réel (local) ainsi qu'à ceux affectés à cet homologue aux fins du routage externe.
- Encryption (Chiffrement) : algorithme de chiffrement des données utilisé par cette session, le cas échéant.
- Assigned IP Address and Public IP Address (Adresse IP affectée et adresse IP publique) : affiche l'adresse IP privée affectée à l'homologue distant pour cette session. Également appelée adresse IP interne ou virtuelle, l'adresse IP affectée permet à l'homologue distant de sembler se trouver sur le réseau privé. Le deuxième champ affiche l'adresse IP publique de l'ordinateur distant pour cette session. Également appelée adresse IP externe, l'adresse IP publique est généralement affectée à l'ordinateur distant par le fournisseur de services Internet. Elle permet à l'ordinateur distant de fonctionner comme hôte sur le réseau public.
- Other (Autre) : attributs divers associés à la session.

Les attributs suivants s'appliquent aux sessions IKE, aux sessions IPsec et aux sessions NAC :

- Revalidation Time Interval (Intervalle de revalidation) : intervalle en secondes requis entre chaque validation de posture réussie.

- Time Until Next Revalidation (Temps jusqu'à la prochaine revalidation) : 0 si la dernière tentative de validation de posture a échoué. Sinon, la différence entre l'intervalle de revalidation et le nombre de secondes depuis la dernière validation réussie de la posture.
- Status Query Time Interval (Intervalle de requête d'état) : temps en secondes autorisé entre chaque validation de posture ou réponse de requête d'état réussie et la réponse de requête d'état suivante. Une requête d'état est une demande effectuée par l'ASA à l'hôte distant afin d'indiquer si l'hôte a connu des changements de posture depuis la dernière validation de posture.
- EAPoUDP Session Age (Âge de la session EAPoUDP) : nombre de secondes depuis la dernière validation de posture réussie.
- Hold-Off Time Remaining (Temps d'attente restant) : 0 seconde si la dernière validation de posture a réussi. Sinon, le nombre de secondes restantes avant la prochaine tentative de validation de la posture.
- Posture Token (Jeton de posture) : chaîne de texte informatif configurable sur le serveur de contrôle d'accès. L'ACS télécharge le jeton de posture sur l'ASA à des fins informatives afin de faciliter la surveillance, la création de rapports, le débogage et la journalisation du système. Un jeton de posture typique est Healthy (En bonne santé), Checkup (Contrôle), Quarantine (Quarantaine), Infected (Infecté) ou Unknown (Inconnu).
- Redirect URL (URL de redirection) : après la validation de posture ou l'authentification sans client, l'ACS télécharge la politique d'accès de la session vers l'ASA. L'URL de redirection constitue une partie facultative de la charge utile de la politique d'accès. L'ASA redirige toutes les demandes HTTP (port 80) et HTTPS (port 443) de l'hôte distant vers l'URL de redirection, le cas échéant. Si la politique d'accès ne contient pas d'URL de redirection, l'ASA ne redirige pas les requêtes HTTP et HTTPS de l'hôte distant.

  Les URL de redirection restent en vigueur jusqu'à la fin de la session IPsec ou jusqu'à la revalidation de la posture, pour laquelle l'ACS télécharge une nouvelle politique d'accès qui peut contenir une URL de redirection différente ou aucune URL de redirection.

  More (Plus) : appuyez sur ce bouton pour revalider ou initialiser la session ou le groupe de tunnels.

L'onglet ACL affiche l'ACL contenant les ACE correspondant à la session.

Surveiller les charges de grappe

Monitoring (Supervision) > VPN > VPN Statistics (Statistiques VPN) > Cluster Loads (Charges de grappe)

Pour afficher la répartition actuelle de la charge du trafic entre les serveurs d'une grappe d'équilibrage de charge VPN. Si le serveur ne fait pas partie d'une grappe, vous recevez un message d'information indiquant que ce serveur ne participe pas à une grappe d'équilibrage de charge VPN.

Surveiller les statistiques cryptographiques

Monitoring (Supervision) > VPN > VPN Statistics (Statistiques VPN) > Crypto Statistics (Statistiques cryptographiques)

Pour afficher les statistiques cryptographiques des sessions utilisateur et administrateur actuellement actives sur l'ASA. Chaque ligne dans le tableau représente une statistique cryptographique.

Surveiller les statistiques de compression

Monitoring (Supervision) > VPN > VPN Statistics (Statistiques VPN) > Compression Statistics (Statistiques de compression)

Pour afficher les statistiques de compression pour les sessions utilisateur et administrateur actuellement actives sur l'ASA. Chaque ligne dans le tableau représente une statistique de compression.

Surveiller les statistiques de chiffrement

Monitoring (Supervision) > VPN > VPN Statistics (Statistiques VPN) > Encryption Statistics (Statistiques de chiffrement)

Pour afficher les algorithmes de chiffrement des données utilisés par les sessions utilisateur et administrateur actuellement actives sur l'ASA. Chaque ligne dans le tableau représente un type d'algorithme de chiffrement.

Surveiller les statistiques globales IKE/IPsec

Monitoring (Supervision) > VPN > VPN Statistics (Statistiques VPN) > Global IKE/IPsec Statistics (Statistiques globales IKE/IPsec)

Pour afficher les statistiques globales IKE/IPsec pour les sessions utilisateur et administrateur actuellement actives sur l'ASA. Chaque ligne dans le tableau représente une statistique globale.

Surveiller le résumé des sessions NAC

Pour afficher les sessions de contrôle d'admission au réseau actives et cumulatives.

- Active NAC Sessions (Sessions NAC actives) : statistiques générales sur les homologues distants soumis à la validation de posture.
- Cumulative NAC Sessions (Sessions NAC cumulatives) : statistiques générales sur les homologues distants qui sont ou ont été soumis à une validation de posture.
- Accepted (Accepté) : nombre d'homologues ayant réussi la validation de posture et s'étant vu affecter une politique d'accès par un serveur de contrôle d'accès.
- Rejected (Rejeté) : nombre d'homologues ayant échoué à la validation de posture ou ne s'étant pas vu affecter de politique d'accès par un serveur de contrôle d'accès.
- Exempté : nombre d'homologues qui ne sont pas soumis à la validation de la posture, car ils correspondent à une entrée dans la liste d'exceptions de validation de posture configurée sur l'ASA.
- Non-responsive (Sans réponse) : nombre d'homologues ne répondant pas aux demandes UDP du protocole EAP (Extensible Authentication Protocol) pour la validation de posture. Les homologues sur lesquels aucun CTA n'est en cours d'exécution ne répondent pas à ces demandes. Si la configuration ASA prend en charge les hôtes sans client, le serveur de contrôle d'accès télécharge vers l'ASA la politique d'accès associée aux hôtes sans client pour ces homologues. Sinon, l'ASA attribue la politique par défaut du NAC.
- Hold-off (En attente) : nombre d'homologues pour lesquels l'ASA a perdu les communications EAPoUDP après une validation de posture réussie. L'attribut NAC Hold Timer (Minuterie d'attente NAC) (Configuration > VPN > NAC) détermine le délai entre ce type d'événement et la prochaine tentative de validation de posture.
- N/A (S/O) : nombre d'homologues pour lesquels la NAC est désactivée conformément à la stratégie de groupe VPN NAC.

- Revalidate All (Revalider tout) : cliquez si la posture des homologues ou les politiques d'accès affectées (c'est-à-dire les ACL téléchargées) ont changé. Le fait de cliquer sur ce bouton lance de nouvelles validations de posture inconditionnelles pour toutes les sessions NAC gérées par l'ASA. La validation de posture et la politique d'accès affectée qui étaient en vigueur pour chaque session avant que vous ne cliquiez sur ce bouton demeurent en vigueur jusqu'à ce que la nouvelle validation de posture réussisse ou échoue. Le fait de cliquer sur ce bouton n'affecte pas les sessions exemptées de validation de posture.
- Initialize All (Initialiser tout) : cliquez si la posture des homologues ou les politiques d'accès affectées (c'est-à-dire les ACL téléchargées) ont changé et que vous souhaitez effacer les ressources affectées aux sessions. Le fait de cliquer sur ce bouton purge les associations EAPoUDP et les politiques d'accès affectées utilisées pour les validations de posture de toutes les sessions NAC gérées par l'ASA et lance de nouvelles validations de posture inconditionnelles. L'ACL NAC par défaut est active pendant les revalidations, de sorte que les initialisations de session peuvent perturber le trafic utilisateur. Le fait de cliquer sur ce bouton n'affecte pas les sessions exemptées de validation de posture.

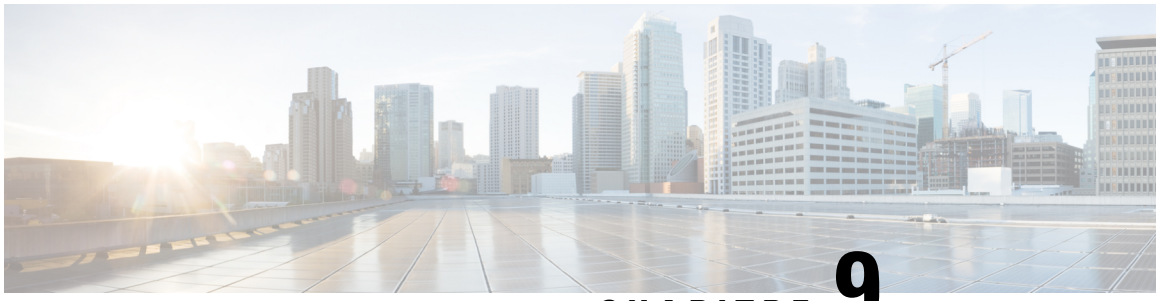
Surveiller les statistiques de protocole

Monitoring (Supervision) > VPN > VPN Statistics (Statistiques VPN) > Protocol Statistics (Statistiques de protocole)

Pour afficher les protocoles utilisés par les sessions utilisateur et administrateur actuellement actives sur l'ASA. Chaque ligne dans le tableau représente un type de protocole.

Surveiller les sessions de mappage VLAN

Pour afficher le nombre de sessions affectées à un VLAN de sortie, tel que déterminé par la valeur du paramètre Restrict Access to VLAN (Restreindre l'accès au VLAN) de chaque stratégie de groupe utilisée. L'ASA transfère tout le trafic vers le VLAN sélectionné.



CHAPITRE 9

Paramètres SSL

Paramètres SSL

Configurez les paramètres SSL à l'un des emplacements suivants :

- **Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > SSL Settings (Paramètres SSL)**
- **Configuration > Remote Access VPN (VPN d'accès à distance) > Advanced (Avancé) > SSL Settings (Paramètres 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. En outre, DTLS est utilisé pour les connexions des clients VPN Secure Client . Le volet SSL Settings (Paramètres SSL) vous permet de configurer les versions SSL et les algorithmes de chiffrement pour les clients et les serveurs. Il vous permet également d'appliquer des points de confiance configurés précédemment à des interfaces spécifiques et de configurer un point de confiance de repli pour les interfaces qui n'ont pas de point de confiance associé.

Remarque Pour la version 9.3(2), SSLv3 a été abandonné. La valeur par défaut est maintenant **tlsv1** au lieu de **any**. Le mot-clé **any** est maintenant obsolète. Si vous choisissez **any**, **sslv3** ou **sslv3**-only, les paramètres sont acceptés avec un avertissement. Cliquez sur **OK** pour continuer. Dans la prochaine version majeure d'ASA, ces mots-clés seront supprimés de l'ASA.

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; veuillez consulter https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf pour connaître la compatibilité

Champs

- **Server SSL Version** (Version SSL du serveur) : spécifiez la version minimale du protocole SSL/TLS que l'ASA utilise lorsqu'il agit en tant que serveur dans la liste déroulante.

N'importe quel	Accepte les messages client hello SSLv2 et négocie la version commune la plus élevée.
SSLv3	Accepte les messages client hello SSLv2 et négocie SSLv3 (ou une version supérieure).
TLS V1	Accepte les messages client hello SSLv2 et négocie TLSv1 (ou version supérieure).
TLSV1.1	Accepte les messages client hello SSLv2 et négocie TLSv1.1 (ou version supérieure).
TLSV1.2	Accepte les messages client hello SSLv2 et négocie TLSv1.2 (ou version supérieure).
TLSV1.3	Accepte les hellos de clients SSLv2 et négocie TLSv1.3 (ou version ultérieure).
DTLSv1	Accepte les messages client hello DTLSv1 et négocie DTLSv1 (ou version supérieure).
DTLS1.2	Accepte les messages client hello DTLSv1.2 et négocie DTLSv1.2 (ou une version supérieure).

Remarque La configuration et l'utilisation de DTLS s'appliquent uniquement aux .

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 celle de DTLS. DTLSV1.2 prend en charge TLSV1.2 et TLSV1.3. Toute version TLS peut être utilisée avec DTLS1, car elles sont toutes égales ou supérieures à DTLS 1.

TLSv1.3 nécessite Cisco Secure Client version 5.0 ou ultérieure.

- **Client SSL Version** (Version SSL du client) : précisez la version minimale du protocole SSL/TLS que l'ASA utilise lorsqu'il agit comme client, dans la liste déroulante. (DTLS non disponible pour le rôle de client SSL)

N'importe lequel	Transmet les messages client hello SSLv3 et négocie SSLv3 (ou version supérieure).
SSL v3	Transmet les messages client hello SSLv3 et négocie SSLv3 (ou version supérieure).
TLS V1	Transmet les messages client hello TLSv1 et négocie TLSv1 (ou version supérieure).
TLSV1.1	Transmet les messages client hello TLSv1.1 et négocie TLSv1.1 (ou version supérieure).
TLSV1.2	Transmet les messages client hello TLSv1.2 et négocie TLSv1.2 (ou version supérieure).
TLSv1.3	Transmet les messages client hello TLSv1.3 (ou version ultérieure).

- **Diffie-Hellmann group to be used with SSL**(Groupe Diffie-Hellman à utiliser avec SSL : choisissez un groupe dans la liste déroulante. Les options disponibles sont Group1 - module de 768 bits, Group2 - module de 1024 bits, Group5 - module de 1536 bits, Group14 - module de 2048 bits, ordre premier de 224 bits, et Group24 - module de 2048 bits, ordre premier de 256 bits. La valeur par défaut est Group2.

- **ECDH group to be used with SSL** (Groupe ECDH à utiliser avec SSL) : choisissez un groupe dans la liste déroulante. Les options disponibles sont Groupe19 – EC 256 bits, Groupe20 – EC 384 bits et Groupe21 – EC 521 bits. La valeur par défaut est Group19.

Remarque Les chiffrements ECDSA et DHE ont la priorité la plus élevée.

- **Encryption** (Chiffrement) : spécifiez la version, le niveau de sécurité et les algorithmes de chiffrement SSL que vous souhaitez prendre en charge. Cliquez sur **Edit** (Modifier) pour définir ou modifier une entrée du tableau à l'aide de la boîte de dialogue Configure Cipher Algorithms/Custom String (Configurer les algorithmes de chiffrement / la chaîne personnalisée). Choisissez le niveau de sécurité du chiffrement SSL, puis cliquez sur **OK**.
  - **Cipher Version** (Version du chiffrement) : répertorie la version du chiffrement que l'ASA prend en charge et utilise pour les connexions SSL.
  - **Cipher Security Level** (Niveau de sécurité du chiffrement) : répertorie les niveaux de sécurité du chiffrement que l'ASA prend en charge et utilise pour les connexions SSL. Choisissez une des options suivantes :

    Tout comprend tous les chiffrements, y compris NULL-SHA.

    Faible comprend tous les chiffrements, sauf NULL-SHA.

    Medium (Moyen) : comprend tous les chiffrements, sauf NULL-SHA, DES-CBC-SHA, RC4-MD5 (valeur par défaut), RC4-SHA et DES-CBC3-SHA.

    High (Élevé) : comprend uniquement AES-256 avec les chiffrements SHA-2 et s'applique uniquement à TLS version 1.2 et aux chiffrements pris en charge par TLS version 1.3.

    Personnalisé comprend un ou plusieurs chiffrements que vous spécifiez dans la zone Algorithmes de chiffrement/chaîne personnalisée. Cette option vous fournit un contrôle total de la suite de chiffrement à l'aide de chaînes de définition de chiffrement OpenSSL.
  - **Cipher Algorithms/Custom String** (Algorithmes de chiffrement/chaîne personnalisée) : répertorie les algorithmes de chiffrement que l'ASA prend en charge et utilise pour les connexions SSL. Pour plus d'informations sur les chiffrements à l'aide d'OpenSSL, consultez https://www.openssl.org/docs/manmaster/man1/ciphers.html

    L'ASA spécifie l'ordre de priorité des chiffrements pris en charge comme suit : d'abord les chiffrements pris en charge uniquement par TLSv1.3/TLSv1.2, puis les chiffrements non pris en charge par TLSv1.1, TLSv1.2 ou TLSv1.3.

Les chiffrements suivants sont pris en charge :

- **Server Name Indication (SNI)** (Indication du nom de serveur) : spécifie le nom de domaine et le point de confiance à associer à ce domaine. Cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) pour définir ou modifier, pour chaque interface, un domaine et un point de confiance à l'aide de la boîte de dialogue Add/Edit Server Name Indication (SNI) (Ajouter/Modifier l'indication du nom de serveur [SNI]).

Chiffre	TLSv1.1/DTLSv1	TLSv1.2 / DTLSV 1.2	TLSv1.3
TLS_AES_128_GCM_SHA256	Non	Non	Oui

Chiffre	TLSv1.1/DTLSv1	TLSv1.2 / DTLSV 1.2	TLSv13
TLS_CHACHA20_POLY1305_SHA256	Non	Non	Oui
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
DERS-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 Le tunnel DTLS1.2 fonctionne avec TLSv1.3, cependant, DTLS1.2 ne prend pas en charge les chiffrements TLSv1.3. Le chiffrement pris en charge de priorité la plus élevée est choisi pour le tunnel DTLS1.2.

- Specify domain (Préciser le domaine) : saisissez le nom de domaine.
- Select trustpoint to associate with domain (Sélectionner le point de confiance à associer au domaine) : choisissez le point de confiance dans la liste déroulante

- **Certificates** (Certificats) : attribuez les certificats à utiliser pour l'authentification SSL sur chaque interface. Cliquez sur **Edit** (Modifier) pour définir ou modifier le point de confiance pour chaque interface à l'aide de la boîte de dialogue Select SSL Certificate (Sélectionner le certificat SSL).
  - Primary Enrolled Certificate (Certificat inscrit principal) : sélectionnez le point de confiance à utiliser pour les certificats sur cette interface.
  - Load Balancing Enrolled Certificate (Certificat inscrit pour l'équilibrage de charge) : sélectionnez un point de confiance à utiliser pour les certificats lorsque l'équilibrage de charge VPN est configuré.
- **Fallback Certificate** (Certificat de repli) : cliquez pour choisir un certificat à utiliser pour les interfaces auxquelles aucun certificat n'est associé. Si vous choisissez **None** (Aucun), l'ASA utilise la paire de clés et le certificat RSA par défaut.
- **Forced Certification Authentication Timeout** (Délai d'authentification de certification forcée) : configurez le nombre de minutes à attendre avant l'expiration de l'authentification par certificat.
- **Apply** (Appliquer) : cliquez pour enregistrer vos modifications.
- **Reset** (Réinitialiser) : cliquez pour annuler les modifications apportées et rétablir les paramètres SSL aux valeurs précédemment définies.

Paramètres SSL

CHAPITRE 10

Virtual Tunnel Interface

Ce chapitre décrit comment configurer un tunnel VTI.

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 d'entrée 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 et à les inclure dans la liste d'accès 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 248.

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 l'établissement des 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 250.

Comment un ASA crée un tunnel VTI dynamique pour une session VPN

1. Créez un modèle virtuel sur l'ASA).

   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 en étoile.
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' de commande 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.
- Vous pouvez configurer un maximum de 1 024 VTI statiques et dynamiques 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 configurés 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 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.
- 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 avec le profil IPsec. Configurez l'homologue distant avec des paramètres de proposition IPsec et de profil IPsec identiques. La négociation SA commencera lorsque tous les paramètres de tunnel seront configurés.

Remarque Pour l'ASA qui fait partie des deux domaines VTI du VPN et qui a une contiguïté de 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 activer le trafic IPsec dans l'ASA sans vérifier les listes de contrôle d'accès :

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** .

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

Étape 1 Choisissez **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Advanced (Avancé)** > **IPsec Proposals (Transform Sets) (Propositions IPsec [ensembles de transformation])**.

Étape 2 Configurez IKEv1 ou IKEv2 pour établir l'association de sécurité.

- Configurez IKEv1.

a) Dans le panneau des propositions IKEv1 IPsec (ensembles Transform), cliquez sur **Add** (Ajouter).
b) Saisissez le **Set Name** (Nom de l'ensemble).
c) Conservez la sélection par défaut de la case **Tunnel**.
d) Sélectionnez **ESP Encryption** (Chiffrement ESP) et **ESP Authentication** (Authentification ESP).
e) Cliquez sur **OK**.

- Configurez IKEv2.

a) Dans le panneau des propositions IKEv2 IPsec, cliquez sur **Add** (Ajouter).
b) Saisissez **Name** (Nom), et **Encryption** (Chiffrement).
c) Choisissez **Integrity Hash** (Hachage d'intégrité).
d) Cliquez sur **OK**.

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 Choisissez **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Advanced (Avancé)** > **IPsec Proposals (Transform Sets) (Propositions IPsec [ensembles de transformation])**.

Étape 2 Dans le panneau **IPsec Profile** (Profil IPsec), cliquez sur **Add** (Ajouter).

Étape 3 Saisissez le **Name** (Nom) du profil IPsec.

Étape 4 Saisissez la **proposition IKE v1 IPsec** ou la **proposition IKE v2 IPsec** créée pour le profil IPsec. Vous pouvez choisir un ensemble de transformation IKEv1 ou une proposition IKEv2 IPsec.

Étape 5 Si vous avez besoin d'une extrémité du tunnel VTI pour agir uniquement en tant que répondeur, cochez la case **Responder only** (Répondeur uniquement.

- 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 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 6 (Facultatif) Cochez la case **Enable security association lifetime** (Activer la durée de vie de l'association de sécurité) et saisissez les valeurs de durée de l'association de sécurité en **kilo-octets** et **en secondes**.

Étape 7 (Facultatif) Cochez la case des **PFS Settings** (Paramètres PFS) pour activer PFS, puis sélectionnez le groupe Diffie-Hellman requis.

La confidentialité de transmission parfaite (PFS) génère une clé de session unique pour chaque échange chiffré. La 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.

Cela détermine la robustesse de l'algorithme de dérivation de la clé de chiffrement. L'ASA utilise cet algorithme pour dériver les clés de chiffrement et de hachage.

Étape 8 (Facultatif) Cochez la case **Enable sending certificate** (Activer l'envoi du certificat) et sélectionnez un **Trustpoint** (Point de confiance) qui définit le certificat à utiliser lors de l'initialisation d'une connexion de tunnel VTI. Cochez la case **Chain** (Chaîne), le cas échéant.

Étape 9 Cochez la case **Enable Reverse Route Injection** (Activer l'injection de route inverse) pour activer l'injection de route inverse (RRI) pour ce profil IPsec.

La RRI renseigne la table de routage d'un routeur interne exécutant des protocoles de routage dynamiques tels qu'OSPF, EIGRP sur ASA, ou RIP pour les clients VPN d'accès à distance ou les sessions LAN à LAN. 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 soit 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.

Étape 10 Cochez la case **Dynamic** (Dynamique) pour définir la route inverse comme dynamique.

Étape 11 Cliquez sur **OK**.

Étape 12 Dans le panneau principal **IPsec Proposals (Transform Sets) (Propositions IPsec [Ensembles de transformation])**, cliquez sur **Apply** (Appliquer).

Étape 13 Dans la boîte de dialogue **Preview CLI Commands** (Aperçu des commandes CLI), cliquez sur **Send** (Envoyer).

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 Choisissez **Configuration** > **Device Setup (Configuration du périphérique)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**.

Étape 2 Choisissez **Add (Ajouter)** > **VTI Interface (Interface VTI)**. La fenêtre **Add VTI Interface** (Ajouter une interface VTI) s'affiche.

Étape 3 Dans l'onglet **General** (Général) :

a) Saisissez l'**ID VTI**. La plage est de 0 à 10 413. Jusqu'à 10413 interfaces VTI sont prises en charge.

b) Saisissez l'**Interface Name** (Nom de l'interface).

c) Assurez-vous que la case **Enable Interface** (Activer l'interface) est cochée.

d) Choisissez **IPv4** ou **IPv6** dans la liste déroulante **Path Monitoring** (Surveillance du chemin d'accès) et saisissez l'adresse IP de l'homologue.

e) Saisissez le **coût**. La plage est de 1 à 65 535.

Le coût détermine la priorité pour équilibrer la charge du trafic sur plusieurs VTI. Ce serveur a la priorité la plus élevée.

f) Pour configurer l'adresse IP :

Cliquez sur le bouton radio **Address** (Adresse) pour configurer une adresse IP et le masque de sous-réseau.

Ou

Cliquez sur le bouton radio **Unnumbered** (Non numéroté) pour choisir une interface dans la liste déroulante **IP Unnumbered** (IP non numérotée) afin d'emprunter son adresse IP. Vous pouvez choisir une interface de boucle ou une interface physique dans la liste.

Étape 4 Dans l'onglet **Advanced** (Avancé) :

a) Saisissez l'**adresse IP de destination**.

b) Choisissez l'interface source du tunnel dans la liste déroulante **Source Interface** (Interface source).

Vous pouvez sélectionner une interface de boucle ou une interface physique.

c) Sélectionnez la stratégie IPsec dans le champ **Tunnel Protection with IPsec Policy** (Protection du tunnel avec stratégie IPsec).
d) Sélectionnez le profil IPsec dans le champ **Tunnel Protection with IPsec Profile** (Protection du tunnel avec profil IPsec).
e) Cochez la case **Enable Tunnel Mode IPv4 IPsec** (Activer le mode tunnel IPsec IPv4).

Étape 5 Cliquez sur **OK**.

Étape 6 Dans le panneau **Interfaces**, cliquez sur **Apply** (Appliquer).

Étape 7 Dans la boîte de dialogue **Preview CLI Commands** (Aperçu des commandes CLI), cliquez sur **Send** (Envoyer).

Après le chargement de la configuration mise à jour, le nouveau VTI apparaît dans la liste des interfaces. Ce nouveau VTI peut être utilisé pour créer un VPN de site à site IPsec.

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 Choisissez **Configuration** > **Device Setup (Configuration du périphérique)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**.

Étape 2 Choisissez **Add (Ajouter)** > **DVTI Interface (Interface DVTI)**. La fenêtre **Add DVTI Interface** (Ajouter une interface DVTI) s'affiche.

Étape 3 Dans l'onglet **General** (Général) :

a) Saisissez l'**ID DVTI**. Cet ID peut être n'importe quelle valeur comprise entre 1 et 10413. Jusqu'à 1 024 interfaces VTI sont prises en charge par périphérique.

b) Saisissez l'**Interface Name** (Nom de l'interface).

c) Cochez la case **Enable Interface** (Activer l'interface).

d) Choisissez une interface dans la liste déroulante **IP Unnumbered**.

Le modèle virtuel hérite de l'adresse IP de l'interface sélectionnée. Veillez à utiliser une adresse IP différente de l'adresse IP source du tunnel. Vous pouvez choisir n'importe quelle interface physique ou une adresse de boucle avec retour configurée sur le périphérique.

e) Saisissez une description pour le VTI dynamique dans le champ **Description**.

Étape 4 Dans l'onglet **Advanced** (Avancé) :

a) Choisissez une interface source du tunnel dans la liste déroulante **Source Interface** (Interface source). L'adresse IP de cette interface sera l'adresse IP de destination pour le site distant. Vous pouvez sélectionner uniquement les interfaces physiques et de boucle dans la liste.

b) Cochez la case **Enable IPv6 Source Address** (Activer l'adresse source IPv6) pour accepter les demandes de session VPN uniquement à partir de l'interface configurée avec l'adresse IP source du tunnel. Si vous n'activez pas cette option, l'ASA accepte les demandes de session VPN de n'importe quelle interface.

L'interface d'accès virtuel hérite également 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 à partir de laquelle l'ASA accepte la demande de session VPN.

c) Choisissez le profil IPsec dans la liste déroulante **Tunnel Protection with IPsec Profile** (Protection du tunnel avec profil IPsec).

d) Cochez la case **Enable Tunnel Mode IP Overlay for IPSec (Activer la superposition IP en mode tunnel pour IPsec)** et sélectionnez le bouton radio **IPv4** ou **IPv6** pour activer le mode de tunnel IPsec.

Étape 5 Dans l'onglet **IPv6** :

a) Cliquez sur le bouton de navigation **IPv6 Address Unnumbered** (Adresse IPv6 non numérotée) et choisissez une adresse IPv6 dans la liste.

Toutes les interfaces d'accès virtuelles clonées à partir du modèle virtuel auront la même adresse IP.

b) Cliquez sur **OK**.

Étape 6 Dans la boîte de dialogue **Preview CLI Commands** (Aperçu des commandes CLI), vous pouvez afficher les commandes de modèle virtuel.

Étape 7 Cliquez sur **Send** (envoyer).

Prochaine étape

Associez ce modèle à un groupe de tunnels. Pour en savoir plus, consultez Groupes de tunnels de site à site, à la page 139.

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. Écrans nouveaux/modifiés : **Configuration > Device Setup > Interface Settings > Interfaces > Add > DVTI Interface**
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. Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Add VTI Interface (ajouter une interface VTI)** > **Advanced (avancé)**.
Prise en charge de l'ID de tunnel local	9.17(1)	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.
Prise en charge d'IPv6 sur VTI statique	9.16(1)	L'ASA prend en charge les adresses IPv6 dans les configurations Virtual Tunnel Interfaces (VTI). 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. 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.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de 1024 interfaces VTI par périphérique	9.16(1)	Le nombre de VTI maximum à configurer sur un périphérique est passé de 100 à 1 024. 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. Écrans nouveaux ou modifiés : aucun
Prise en charge du serveur relais DHCP sur VTI	9.14(1)	L'ASA permet de configurer les interfaces VTI comme interfaces de connexion du serveur relais DHCP. Nous avons modifié l'écran suivant pour spécifier une interface VTI pour le relais DHCP : **Configuration** > **Device Management (Gestion des périphériques)** > **DHCP** > **DHCP Relay (Relais DHCP)** > **DHCP Relay Interface Servers (Serveurs d'interface de relais DHCP)**
Prise en charge d'IKEv2, de l'authentification par certificat et de l'ACL dans VTI	9.8(1)	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. Nous avons introduit des options pour sélectionner le point de confiance pour l'authentification par certificat dans l'écran suivant : **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Advanced (Avancé)** > **IPsec Proposals (Transform Sets) (Propositions IPsec (ensembles de transformation))** > **IPsec Profile (Profil IPsec)** > **Add (Ajouter)**

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de Virtual Tunnel Interface (VTI)	9.7(1)	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. Nous avons introduit les écrans suivants : **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Advanced (Avancé)** > **IPsec Proposals (Transform Sets) (Propositions IPsec (ensembles de transformation))** > **IPsec Profile (Profil IPsec)** **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Advanced (Avancé)** > **IPsec Proposals (Transform Sets) (Propositions IPsec (ensembles de transformation))** > **IPsec Profile (Profil IPsec)** > **Add (Ajouter)** > **Add IPsec Profile (Ajouter un profil IPsec)** **Configuration** > **Device Setup (Configuration du périphérique)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add (Ajouter)** > **VTI Interface (Interface VTI)** **Configuration** > **Device Setup (Configuration du périphérique)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add (Ajouter)** > **VTI Interface (Interface VTI)** > **General (Général)** **Configuration** > **Device Setup (Configuration du périphérique)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add (Ajouter)** > **VTI Interface (Interface VTI)** > **Advanced (Avancé)**

CHAPITRE 11

Configurer un serveur AAA externe pour le VPN

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, affecter 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 défini dans la politique 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. Stratégies de groupe affectées par le profil de connexion (également appelé groupes de tunnels) : le profil de connexion contient les paramètres préliminaires pour la connexion et comprend une 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 les attributs d'utilisateur renvoyés par le serveur AAA ou dans la stratégie de groupe affectée à l'utilisateur.

5. Stratégie de groupe par défaut affectée par l'ASA (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 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 avant la connexion (SBL) avec cette fonctionnalité.

L'option de préremplissage du nom d'utilisateur permet à un champ du deuxième certificat (utilisateur) d'être analysé et utilisé pour l'authentification AAA ultérieure 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 spécifier de quel certificat les noms d'utilisateur principal et secondaire doivent provenir lors de la configuration de l'authentification par 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 Profil de connexion Secure Client, attributs d'authentification, à la page 113

Avec l'authentification par certificats multiples, deux certificats sont authentifiés : le deuxième certificat (utilisateur) reçu du client est celui à partir duquel les noms d'utilisateurs principaux et secondaires sont analysés.

Vous pouvez également configurer l'authentification par certificats multiples avec SAML.

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.

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:

- Application de la politique aux attributs basés sur l'utilisateur, à la page 257
- Appliquer l'affectation d'adresse IP statique pour les tunnels Secure Client , à la page 259
- Appliquer l'autorisation ou le refus d'accès entrant, à la page 261
- Appliquer les règles d'heures de connexion et d'heure du jour, à la page 263

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 affecter une stratégie de groupe à la connexion

Application de 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.

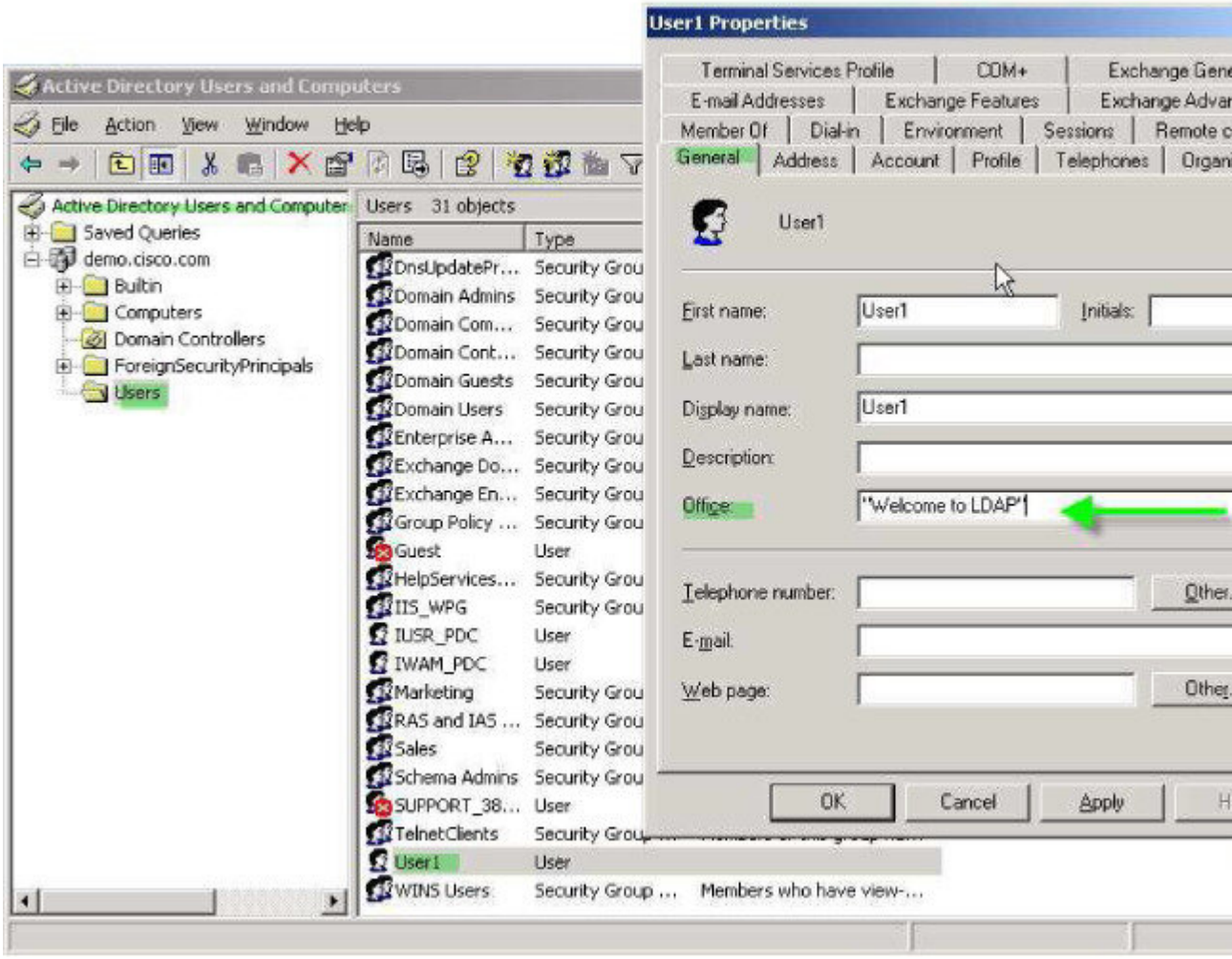
Pour appliquer une bannière simple à un utilisateur configuré sur un serveur LDAP AD, utilisez le champ Office sous l'onglet General (Général) pour saisir le texte de la bannière. Ce champ utilise l'attribut nommé

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 Bannière et faites correspondre l'attribut AD/LDAP PhysicalDeliveryOfficeName à l'attribut Cisco Bannière1 :

```
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.

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 et associez la bannière de carte d'attributs 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

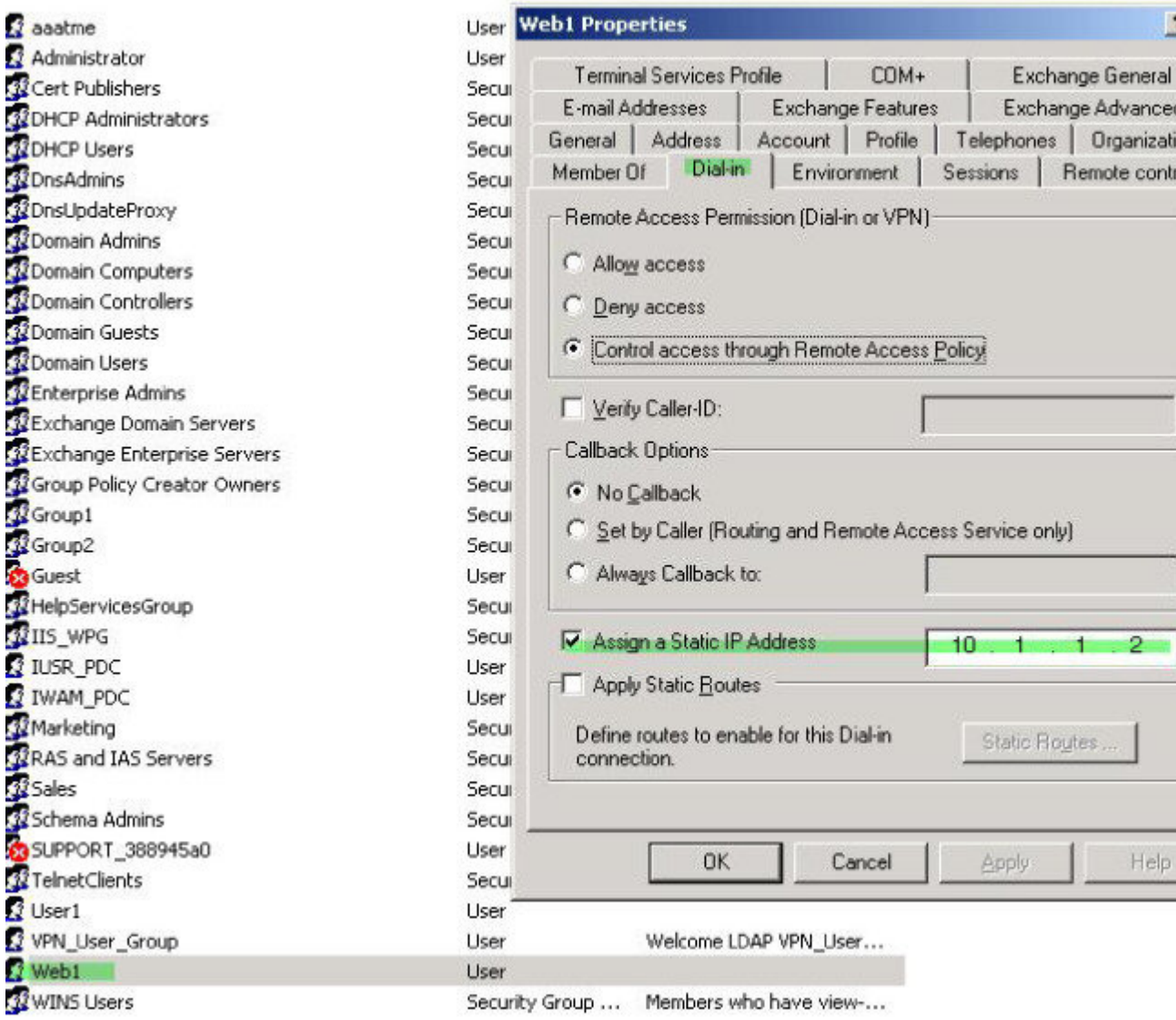
Cet exemple s'applique aux clients de tunnel complet, tels que le client IPsec et les clients VPN SSL.

Pour appliquer les affectations d'adresses IP statiques Secure Client, configurez l'utilisateur Web1 Secure Client pour qu'il reçoive une adresse IP statique, saisissez l'adresse dans le champ Assign Static IP Address (affecter 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** (affecter une adresse IP statique) et saisissez l'adresse IP 10.1.1.2.



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 Secure Client. 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 affectée :

```
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 tunnellisation 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 tunnellisation
1	PPTP
2	L2TP
4	IPsec (IKEv1)
8	L2TP/IPsec
16	SSL sans client
32	Client SSL—Secure Client ou client VPN SSL
64	IPsec (IKEv2)

[1] (1) IPsec et L2TP sur IPsec ne sont pas pris en charge simultanément. Par conséquent, les valeurs 4 et 8 s'excluent mutuellement.
[2] (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, 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 tunnellisation) :

```
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 tunnellisation autorisé en fonction de la carte d'attributs.

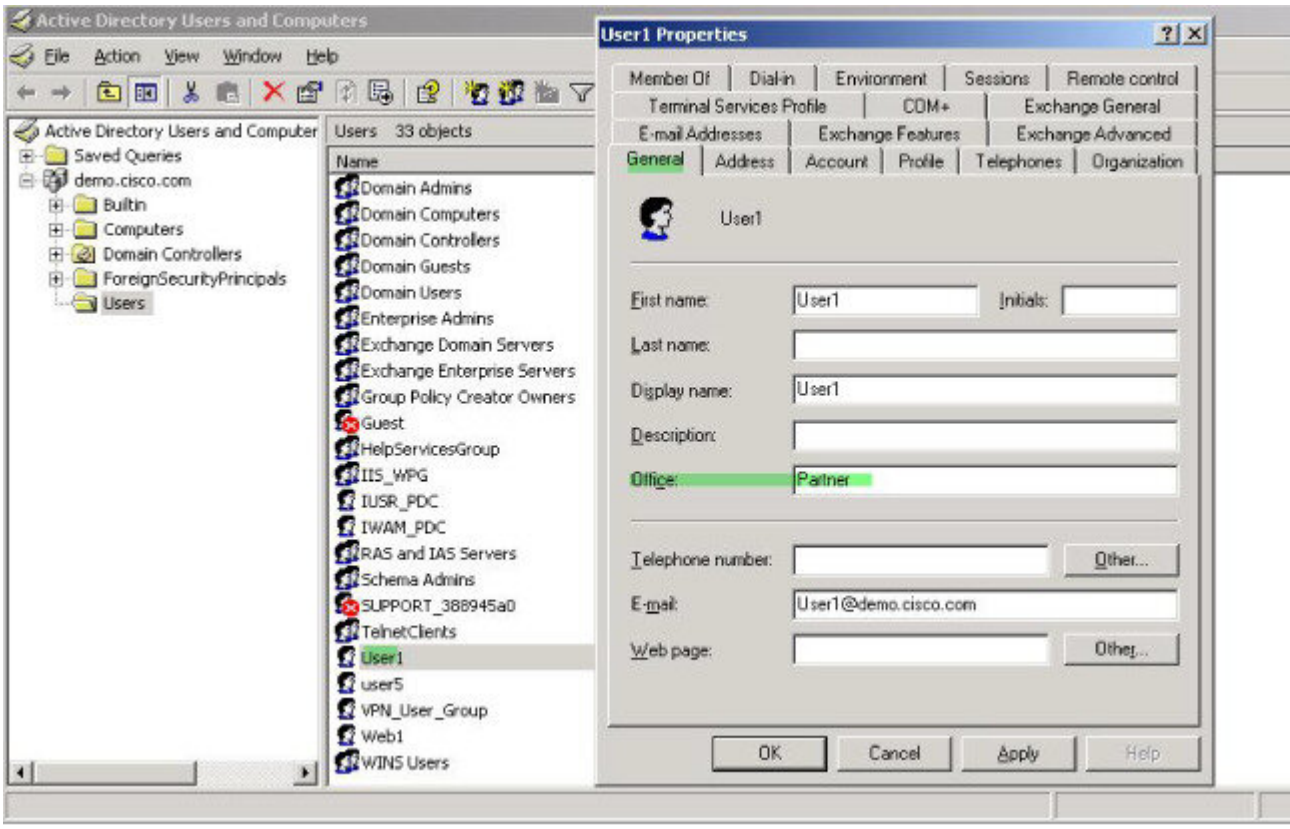
Appliquer les règles d'heures de connexion et d'heure du jour

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 Créez 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.