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 SSLpour 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 36.

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 9 : 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 11 : 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 18
- Stratégies de groupe internes, de site à site, à la page 43

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.

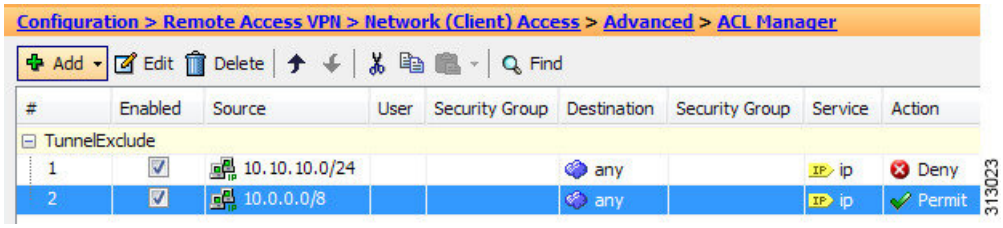
Décochez la case **Inherit** (Hériter) pour choisir l'une de ces options de politique :

- **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 109.
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 92.

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 33
- Configurer la prise en charge des périphériques connectés pour le VPN, à la page 35

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 1 : 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 109.

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 49.
  - 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 50.
  - 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 90.

- 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 56
Profil de connexion, ensemble d'adresses, à la page 56
Profil de connexion, niveau avancé, ajouter ou modifier un ensemble d'adresses IP, à la page 57

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 2 : 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 3 : 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 55 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 57 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 66 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)**.

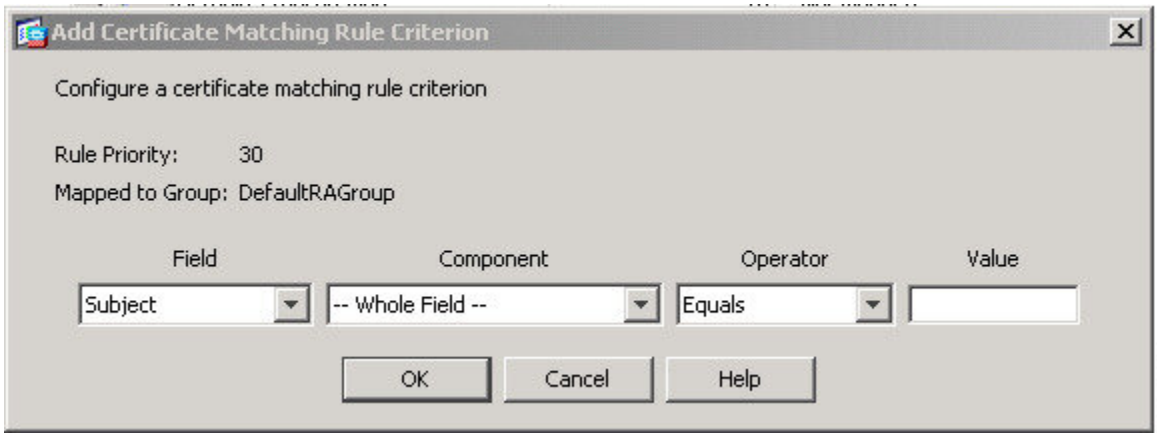
Ce volet comporte une liste des mappages de certificats pour les profils de connexion et des critères de mappage.

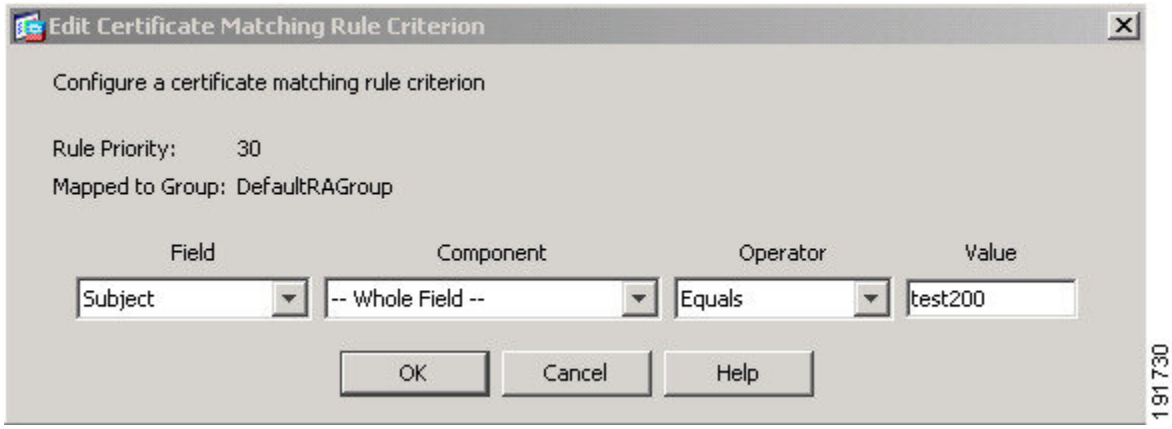
Cartes de profil de connexion et de certificat, ajouter des critères de règle de correspondance de certificat

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 86.
- 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 87.

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.

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 4 : 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

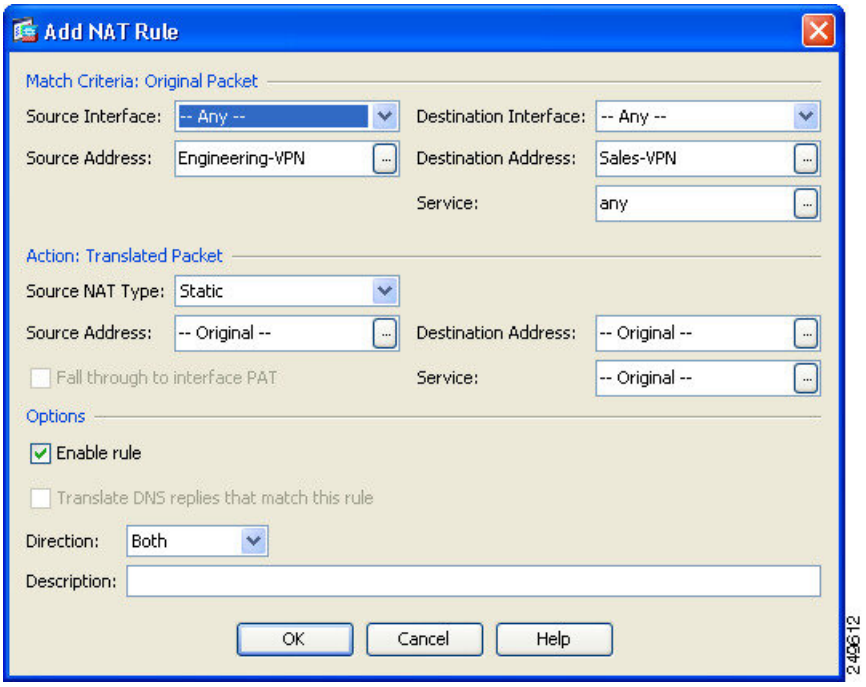
Étape 1 Connectez-vous à ASDM et accédez à **Configuration > Firewall (Pare-feu) > NAT Rules (Règles NAT)**.

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.

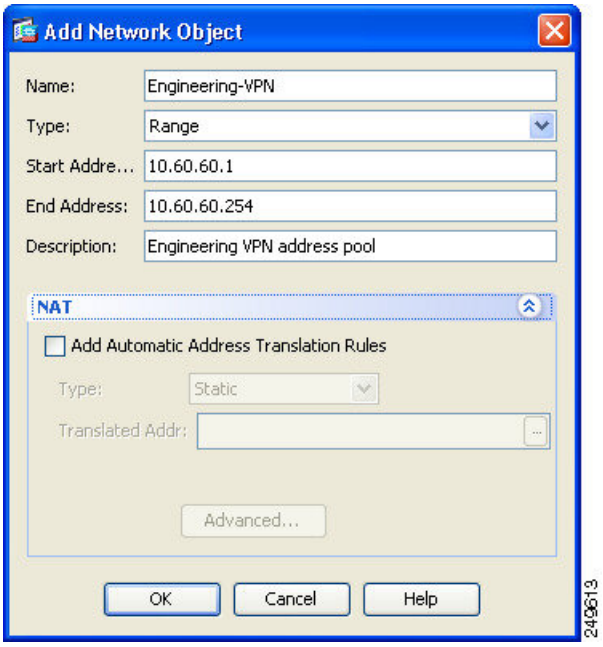
Illustration 1 : Boîte de dialogue Add NAT rule (Ajouter une règle NAT)



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 2 : 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
```

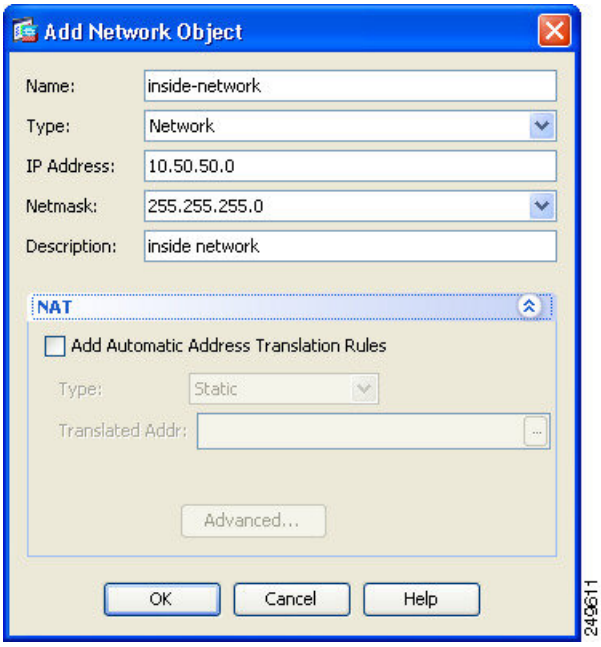
Étape 4 Créez une règle NAT pour que les hôtes de l'ensemble d'adresses VPN Engineering puissent atteindre les autres hôtes de l'ensemble d'adresses VPN Engineering. Créez cette règle exactement comme vous avez créé la règle précédente, sauf que vous spécifiez l'ensemble d'adresses VPN Engineering comme 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 3 : 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.

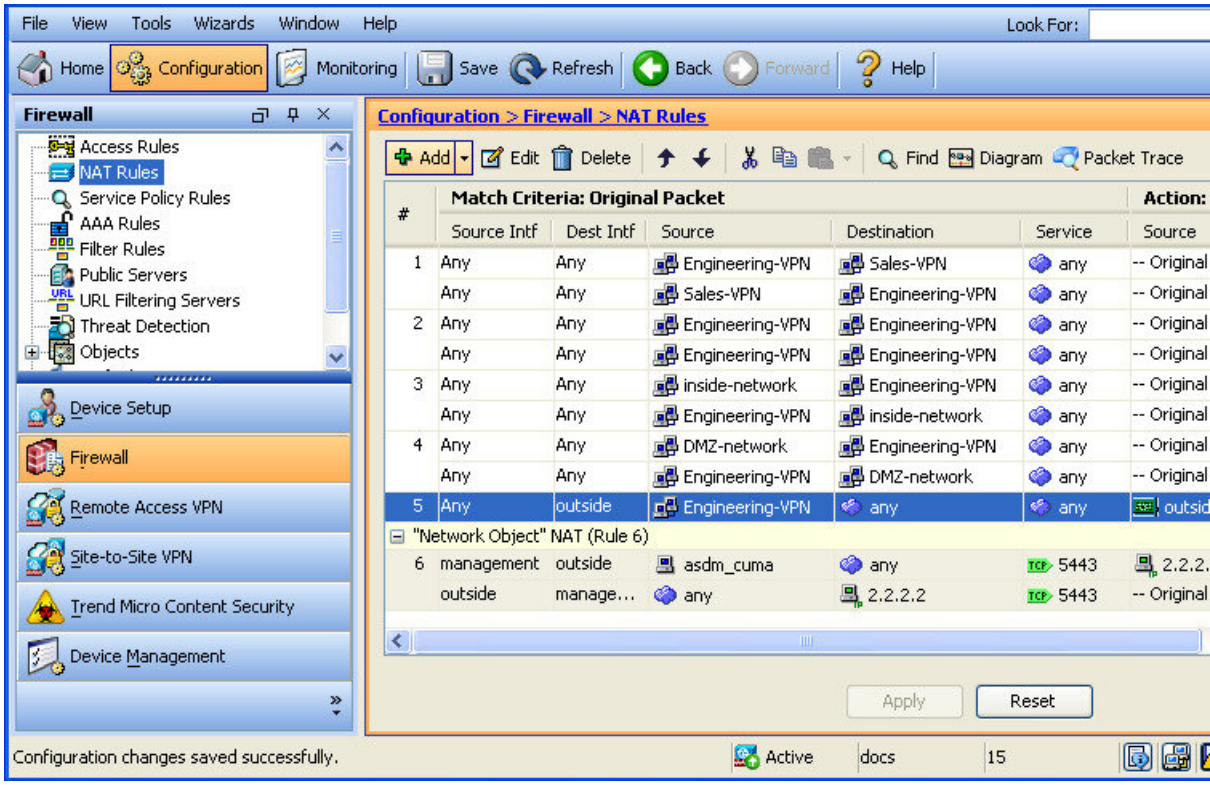
e) Cliquez sur **OK**.

f) Cliquez sur **Apply** (Appliquer).

Exemple de CLI

```
nat (any,outside) source dynamic Engineering-VPN interface
```

Illustration 4 : 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.

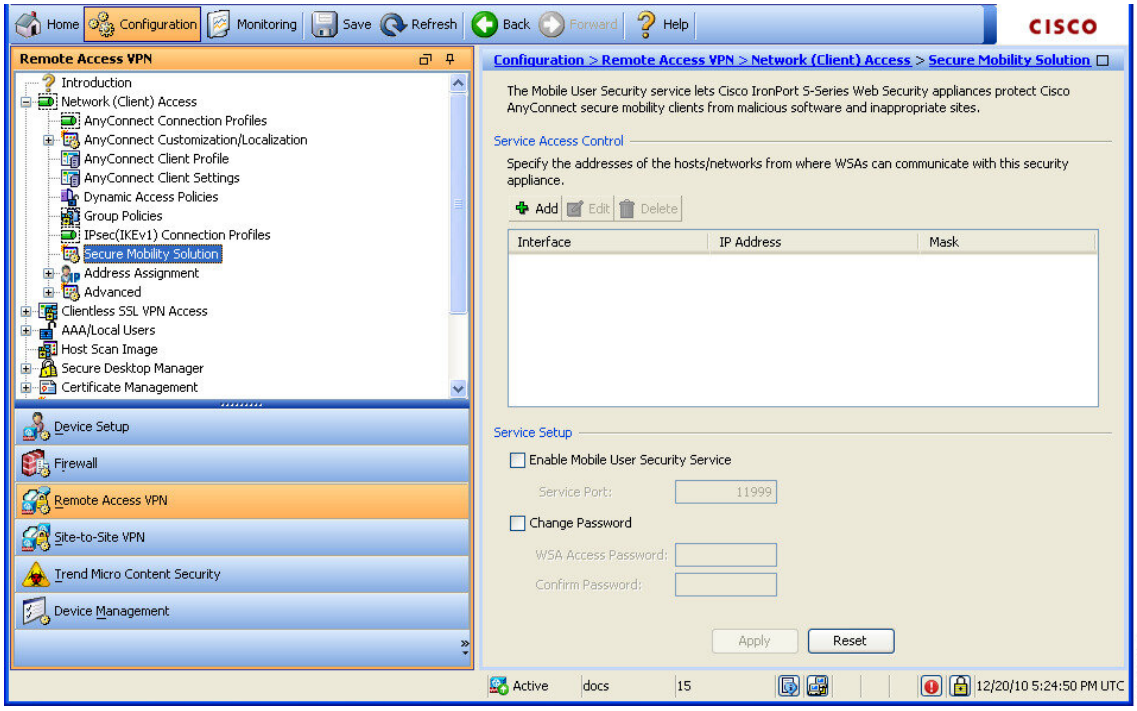
Solution Secure Client

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 5 : 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 28.

  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.

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.