Profils de connexion, stratégies de groupe et utilisateurs

Ce chapitre décrit comment configurer les profils de connexion VPN (anciennement appelés « groupes de tunnels »), les stratégies de groupe et les utilisateurs. Ce chapitre comprend les sections suivantes :

- Aperçu des profils de connexion, des stratégies de groupe et des utilisateurs, à la page 1
- Profils de connexion, à la page 3
- Configurer les profils de connexion, à la page 7
- Stratégies de groupe, à la page 34
- Utiliser un serveur Zone Labs Integrity., à la page 77
- Configurer les attributs d'utilisateur, à la page 83
- Bonnes pratiques pour la configuration et l'ajustement de l'ACL du filtre de VPN, à la page 92

Aperçu des profils de connexion, des stratégies de groupe et des utilisateurs

Les groupes et les utilisateurs sont des concepts centraux dans la gestion de la sécurité des réseaux privés virtuels (VPN) et dans la configuration de l'ASA. Ils précisent les attributs qui déterminent l'accès de l'utilisateur et l'utilisation du VPN. Un *groupe* est un ensemble d'utilisateurs traités comme une seule entité. *Les utilisateurs* obtiennent leurs attributs des *stratégies de groupe*. *Un profil de connexion* identifie la stratégie de groupe pour une connexion spécifique. Si vous n'affectez pas de stratégie de groupe particulière à un utilisateur, la stratégie de groupe par défaut pour la connexion s'applique.

En résumé, vous configurez d'abord les profils de connexion pour définir les valeurs de la connexion. Ensuite, vous configurez les stratégies de groupe. Celles-ci définissent des valeurs pour les utilisateurs dans l'agrégation. Vous configurez ensuite les utilisateurs, qui peuvent hériter des valeurs des groupes et configurer certaines valeurs sur la base d'un utilisateur individuel. Ce chapitre décrit comment et pourquoi configurer ces entités.

Remarque Vous configurez les profils de connexion à l'aide des commandes **tunnel-group**. Dans ce chapitre, les termes « connection profile » (profil de connexion) et « tunnel group » (groupe de tunnels) sont souvent utilisés de manière interchangeable.

Les profils de connexion et les stratégies de groupe simplifient la gestion du système. Pour simplifier la tâche de configuration, l'ASA fournit un profil de connexion par défaut de réseau local (LAN) (DefaultL2Lgroup), un profil de connexion d'accès à distance par défaut pour le VPN IKEv2 (DefaultRAgroup), un profil de connexion par défaut pour les connexions SSL sans client et Secure Client (services client sécurisés) SSL (DefaultWEBVPNgroup) et une stratégie de groupe par défaut (DfltGrpPolicy). Les profils de connexion par défaut et la stratégie de groupe fournissent des paramètres qui sont susceptibles d'être communs à de nombreux utilisateurs. Lorsque vous ajoutez des utilisateurs, vous pouvez préciser qu'ils « héritent » des paramètres d'une stratégie de groupe. Ainsi, vous pouvez configurer rapidement l'accès VPN pour un grand nombre d'utilisateurs.

Si vous décidez d'accorder des droits identiques à tous les utilisateurs VPN, vous n'avez pas besoin de configurer des profils de connexion ou des stratégies de groupe spécifiques, mais les VPN fonctionnent rarement de cette manière. Par exemple, vous pourriez permettre à un groupe des finances d'accéder à une partie d'un réseau privé, à un groupe de service à la clientèle d'accéder à une autre partie et à un groupe MIS d'accéder aux autres parties. En outre, vous pouvez autoriser des utilisateurs spécifiques du groupe MIS à accéder à des systèmes auxquels d'autres utilisateurs du groupe MIS n'ont pas accès. Les profils de connexion et les stratégies de groupe offrent la possibilité de le faire de manière sécurisée.

Remarque L'ASA comprend également le concept de groupes d'objets, qui est un surensemble de listes de réseaux. Les groupes d'objets vous permettent de définir l'accès VPN aux ports ainsi qu'aux réseaux. Les groupes d'objets sont liés aux listes de contrôle d'accès plutôt qu'aux stratégies de groupe et aux profils de connexion. Pour en savoir plus sur l'utilisation des groupes d'objets, consultez le chapitre 20, « Objets » dans le guide de configuration sur les opérations générales.

L'appareil de sécurité peut appliquer des valeurs d'attribut à partir d'une variété de sources. Il les applique selon la hiérarchie suivante :

1. enregistrement Dynamic Access Policy (DAP)
2. Nom de l'utilisateur
3. Stratégie de groupe
4. Stratégie de groupe pour le profil de connexion
5. Stratégie de groupe par défaut

Par conséquent, les valeurs DAP d'un attribut ont une priorité plus élevée que celles configurées pour un utilisateur, une stratégie de groupe ou un profil de connexion.

Lorsque vous activez ou désactivez un attribut pour un enregistrement DAP, l'ASA applique cette valeur et l'impose. Par exemple, lorsque vous désactivez le serveur proxy HTTP en mode de configuration dap webvpn, l'ASA ne cherche aucune autre valeur. Lorsque vous utilisez à la place le mot-clé no pour la commande http-proxy, l'attribut n'est pas présent dans l'enregistrement DAP, de sorte que l'appareil de sécurité remonte à l'attribut AAA dans le nom d'utilisateur et, si nécessaire, à la stratégie de groupe pour trouver une valeur à appliquer. La configuration VPN SSL sans client ASA ne prend en charge qu'une seule commande **http-proxy** et une seule commande **https-proxy**. Nous vous recommandons d'utiliser ASDM pour configurer DAP.

Profils de connexion

Un profil de connexion comprend un ensemble d'enregistrements qui déterminent les politiques de connexion du tunnel. Ces enregistrements identifient les serveurs sur lesquels l'utilisateur du tunnel est authentifié, ainsi que les serveurs de comptabilité, le cas échéant, auxquels les informations de connexion sont envoyées. Ils identifient également une stratégie de groupe par défaut pour la connexion et contiennent des paramètres de connexion spécifiques au protocole. Les profils de connexion comprennent un petit nombre d'attributs qui concernent la création du tunnel lui-même. Les profils de connexion comprennent un pointeur vers une stratégie de groupe qui définit les attributs axés sur l'utilisateur.

L'ASA fournit les profils de connexion par défaut suivants : DefaultL2Lgroup pour les connexions de réseau local (LAN à réseau local), DefaultRAgroup pour les connexions d'accès à distance IPSEC et DefaultWEBVPNGroup pour les connexions VPN SSL (basées sur le navigateur et Secure Client (services client sécurisés)). Vous pouvez modifier ces profils de connexion par défaut, mais vous ne pouvez pas les supprimer. Vous pouvez également créer un ou plusieurs profils de connexion spécifiques à votre environnement. Les profils de connexion sont locaux à l'ASA et ne peuvent pas être configurés sur des serveurs externes.

Remarque Certains profils (comme IKEv1 en phase 1) peuvent ne pas être en mesure de déterminer si un terminal est d'accès à distance ou de réseau local (LAN). S'il ne peut pas déterminer le groupe de tunnels, il utilise la valeur par défaut

```
tunnel-group-map default-group <tunnel-group-name>
```

(la valeur par défaut est *DefaultRAGroup*).

Paramètres de connexion du profil de connexion général

Les paramètres généraux sont communs à toutes les connexions VPN. Les paramètres généraux incluent les éléments suivants :

- Nom du profil de connexion : vous spécifiez un nom de profil de connexion lorsque vous ajoutez ou modifiez un profil de connexion. Les considérations suivantes s'appliquent :
  - Pour les clients qui utilisent des clés prépartagées pour s'authentifier, le nom de profil de connexion est le même que le nom de groupe qu'un client transmet à l'ASA.
  - Les clients qui utilisent des certificats pour s'authentifier transmettent ce nom dans le cadre du certificat, et l'ASA extrait le nom du certificat.
- Type de connexion : les types de connexion comprennent l'accès à distance IKEv1, IPsec de LAN à LAN et AnyConnect (SSL/IKEv2). Un profil de connexion ne peut avoir qu'un seul type de connexion.
- Serveurs d'authentification, d'autorisation et de comptabilité : ces paramètres identifient les groupes ou les listes de serveurs que l'ASA utilise aux fins suivantes :
  - Authentification des utilisateurs
  - Obtention de renseignements sur les services auxquels les utilisateurs sont autorisés à accéder
  - Stockage des enregistrements comptables

Un groupe de serveurs peut comprendre un ou plusieurs serveurs.

- Stratégie de groupe par défaut pour la connexion : une stratégie de groupe est un ensemble d'attributs axés sur l'utilisateur. La stratégie de groupe par défaut est la stratégie de groupe dont l'ASA utilise les attributs par défaut lors de l'authentification ou de l'autorisation d'un utilisateur de tunnel.
- Méthode d'affectation d'adresse client : cette méthode comprend des valeurs pour un ou plusieurs serveurs DHCP ou ensembles d'adresses que l'ASA affecte aux clients.
- Gestion des mots de passe : ce paramètre vous permet d'alerter un utilisateur que le mot de passe actuel doit expirer dans un nombre spécifié de jours (la valeur par défaut est de 14 jours), puis d'offrir à l'utilisateur la possibilité de modifier le mot de passe.
- Suppression de groupe et de domaine : ces paramètres dirigent la façon dont l'ASA traite les noms d'utilisateurs qu'il reçoit. Ils s'appliquent uniquement aux noms d'utilisateurs reçus sous la forme user@realm.

  Un domaine est un domaine administratif ajouté à un nom d'utilisateur avec le délimiteur @ (user@abc). Si vous supprimez le domaine, l'ASA utilise le nom d'utilisateur et le groupe (le cas échéant) pour l'authentification. Si vous supprimez le groupe, l'ASA utilise le nom d'utilisateur et le domaine (le cas échéant) pour l'authentification.

  Saisissez la commande strip-realm pour supprimer le qualificateur de domaine, et saisissez la commande strip-group pour supprimer le qualificateur de groupe du nom d'utilisateur lors de l'authentification. Si vous supprimez les deux qualificateurs, l'authentification est basée sur le *nom d'utilisateur* uniquement. Sinon, l'authentification est basée sur la chaîne complète *username@realm* ou *username<delimiter>group*. Vous devez préciser strip-realm si votre serveur ne peut pas analyser les délimiteurs.

  En outre, pour les clients L2TP/IPsec uniquement, lorsque vous spécifiez la commande strip-group, l'ASA sélectionne le profil de connexion (groupe de tunnels) pour les connexions utilisateur en obtenant le nom de groupe à partir du nom d'utilisateur présenté par le client VPN.

- Autorisation requise : ce paramètre vous permet d'exiger une autorisation avant qu'un utilisateur ne puisse se connecter ou de désactiver cette exigence.
- Attributs DN d'autorisation : ce paramètre spécifie les attributs de nom distinctif à utiliser lors de l'autorisation.

Paramètres de connexion de groupe de tunnels IPsec

Les paramètres IPsec comprennent les éléments suivants :

- Une méthode d'authentification du client : clés prépartagées, certificats ou les deux.
  - Pour les connexions IKE basées sur des clés prépartagées, il s'agit de la clé alphanumérique elle-même (jusqu'à 128 caractères de long), associée à la politique de connexion.
  - Exigence de validation de l'identifiant de l'homologue : ce paramètre spécifie s'il faut valider l'identité de l'homologue à l'aide du certificat d'homologue.
  - Si vous spécifiez des certificats ou les deux pour la méthode d'authentification, l'utilisateur final doit fournir un certificat valide afin de s'authentifier.
- Une méthode d'authentification hybride étendue : XAUTH et XAUTH hybride.

Vous utilisez la commande **isakmp ikev1-user-authentication** pour mettre en œuvre l'authentification hybride XAUTH lorsque vous devez utiliser des certificats numériques pour l'authentification ASA et une méthode existante différente pour l'authentification des utilisateurs VPN distants, comme RADIUS, TACACS+ ou SecurID.

- Paramètres keepalive d'ISAKMP (IKE). Cette fonctionnalité permet à l'ASA de surveiller la présence continue d'un homologue distant et de signaler sa propre présence à cet homologue. Si l'homologue ne répond pas, l'ASA supprime la connexion. L'activation des messages keepalive IKE empêche les connexions bloquées lorsque l'homologue IKE perd la connectivité.

  Il existe différentes formes de messages keepalive IKE. Pour que cette fonctionnalité fonctionne, l'ASA et son homologue distant doivent prendre en charge une forme commune. Cette fonctionnalité fonctionne avec les homologues suivants :

  - Cisco AnyConnect VPN Client
  - logiciel Cisco IOS ®
  - Cisco Secure PIX Firewall

  Les clients VPN autres que Cisco ne prennent pas en charge les IKE keepalives.

  Si vous configurez un groupe d'homologues mixtes et que certains de ces homologues prennent en charge les IKE keepalives et d'autres ne le font pas, activez les IKE keepalives pour l'ensemble du groupe. La fonctionnalité n'affecte pas les homologues qui ne la prennent pas en charge.

  Si vous désactivez les IKE keepalives, les connexions avec des homologues qui ne répondent pas restent actives jusqu'à leur expiration. Nous vous recommandons donc de maintenir votre délai d'inactivité court. Pour modifier votre délai d'inactivité, consultez Configurer les stratégies de groupe, à la page 38.

Remarque Pour réduire les coûts de connectivité, désactivez les IKE keepalives si ce groupe comprend des clients se connectant par l'intermédiaire des lignes ISDN. Les connexions ISDN se déconnectent normalement si elles sont inactives, mais le mécanisme IKE keepalive empêche les connexions d'être inactives et donc de se déconnecter.

Si vous désactivez les IKE keepalives, le client se déconnecte uniquement lorsque ses clés IKE ou IPsec expirent. Le trafic en échec ne déconnecte pas le tunnel avec les valeurs du profil de délai d'expiration d'homologue comme il le fait lorsque les IKE keepalives sont activés.

Si vous avez une configuration LAN à LAN en utilisant le mode principal IKE, assurez-vous que les deux homologues ont la même configuration IKE keepalive. Les deux homologues doivent avoir activé les IKE keepalives ou les deux homologues doivent l'avoir désactivé.

- Si vous configurez l'authentification à l'aide de certificats numériques, vous pouvez préciser s'il faut envoyer l'ensemble de la chaîne de certificats (qui envoie à l'homologue le certificat d'identité et tous les certificats émis) ou uniquement les certificats d'autorité émettrice (y compris le certificat racine et tous les certificats d'autorité de certification subordonnés).

- Vous pouvez informer les utilisateurs qui utilisent des versions obsolètes du logiciel client Windows qu'ils doivent mettre à jour leur client, et vous pouvez fournir un mécanisme pour qu'ils obtiennent la version client mise à jour. Vous pouvez configurer et modifier la mise à jour client, soit pour tous les profils de connexion, soit pour des profils de connexion particuliers.
- Si vous configurez l'authentification à l'aide de certificats numériques, vous pouvez spécifier le nom du point de confiance qui identifie le certificat à envoyer à l'homologue IKE.

Paramètres de connexion de profil de connexion pour les sessions VPN SSL

Le tableau ci-dessous fournit une liste des attributs de profil de connexion qui sont spécifiques aux connexions VPN SSL (Secure Client (services client sécurisés) et sans client). En plus de ces attributs, vous configurez les attributs de profil de connexion généraux communs à toutes les connexions VPN.

Remarque Dans les versions antérieures, les « profils de connexion » étaient appelés « groupes de tunnels ». Vous configurez un profil de connexion avec des commandes de groupe de tunnels. Ce chapitre utilise souvent ces termes de manière interchangeable.

Tableau 1 : Attributs de profil de connexion pour le VPN SSL

	Fonction
authentication	Définit la méthode d'authentification AAA ou Certificat.
customization	Identifie le nom d'une personnalisation définie précédemment à appliquer. Les personnalisations déterminent l'apparence des fenêtres que l'utilisateur voit à l'ouverture de session. Vous configurez les paramètres de personnalisation dans le cadre de la configuration du VPN SSL sans client.
nbns-server	Identifie le nom du serveur de service de nom NetBIOS (nbns-server) à utiliser pour la résolution de nom CIFS.
group-alias	Spécifie un ou plusieurs autres noms par lesquels le serveur peut faire référence à un profil de connexion. Lors de la connexion, l'utilisateur sélectionne le nom du groupe dans un menu déroulant.
group-url	Identifie une ou plusieurs URL de groupe. Si vous configurez cet attribut, les utilisateurs entrant sur une URL spécifiée n'ont pas besoin de sélectionner de groupe à la connexion. Un déploiement d'équilibrage de charge qui utilise des URL de groupe pour la connectivité Secure Client (services client sécurisés), nécessite que chaque nœud ASA de la grappe configure une URL de groupe pour l'adresse de grappe virtuelle, ainsi qu'une URL de groupe pour l'adresse publique d'équilibrage de charge du nœud.
dns-group	Identifie le groupe de serveurs DNS qui spécifie le nom du serveur DNS, le nom de domaine, le serveur de noms, le nombre de tentatives et les valeurs de délai d'expiration d'un serveur DNS à utiliser pour un profil de connexion.

	Fonction
hic-fail-group-policy	Spécifie une politique de fonctionnalité VPN si vous utilisez Cisco Secure Desktop Manager pour définir l'attribut de politique basée sur un groupe sur « Use Failure Group-Policy » ou « Use Success Group-Policy, si les critères correspondent ».
override-svc-download	Remplace le téléchargement des attributs de stratégie de groupe ou de nom d'utilisateur configurés pour le téléchargement du client VPN AnyConnect vers l'utilisateur distant.
radius-reject-message	Active l'affichage du message de rejet RADIUS sur l'écran de connexion lorsque l'authentification est rejetée.

Configurer les profils de connexion

Cette section décrit le contenu et la configuration des profils de connexion, tant en mode contexte unique qu'en mode contexte multiple.

Remarque Le mode contexte multiple s'applique uniquement aux VPN de site à site IKEv2 et IKEv1 et ne s'applique pas à Secure Client (services client sécurisés), au VPN SSL sans client, à l'ancien client VPN Cisco, au client VPN natif d'Apple, au client VPN natif de Microsoft ni à cTCP pour IKEv1 IPsec.

Vous pouvez modifier les profils de connexion par défaut et vous pouvez configurer un nouveau profil de connexion pour l'un des trois types de groupe de tunnels. Si vous ne configurez pas explicitement un attribut dans un profil de connexion, cet attribut reçoit sa valeur du profil de connexion par défaut. Le type de profil de connexion par défaut est l'accès à distance. Les paramètres suivants dépendent de votre choix de type de tunnel. Pour voir la configuration actuelle et la configuration par défaut de tous vos profils de connexion, y compris le profil de connexion par défaut, saisissez la commande **show running-config all tunnel-group**.

Profils de connexion

Le nombre maximal de profils de connexion (groupes de tunnels) qu'un ASA peut prendre en charge est une fonction du nombre maximal de sessions VPN simultanées pour la plateforme + 5. La tentative d'ajout d'un groupe de tunnels supplémentaire au-delà de la limite entraîne l'affichage du message suivant : « ERREUR : la limite de 30 groupes de tunnels configurés a été atteinte ».

Configuration par défaut du profil de connexion IPsec d'accès à distance

Le contenu du profil de connexion d'accès à distance par défaut est le suivant :

```
tunnel-group DefaultRAGroup type remote-access
tunnel-group DefaultRAGroup general-attributes
 no address-pool
 no ipv6-address-pool
 authentication-server-group LOCAL
 accounting-server-group RADIUS
 default-group-policy DfltGrpPolicy
```

```
 no dhcp-server
 no strip-realm
 no password-management
 no override-account-disable
 no strip-group
 no authorization-required
 authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup webvpn-attributes
 hic-fail-group-policy DfltGrpPolicy
 customization DfltCustomization
 authentication aaa
 no override-svc-download
 no radius-reject-message
 dns-group DefaultDNS
tunnel-group DefaultRAGroup ipsec-attributes
 no pre-shared-key
 peer-id-validate req
 no chain
 no trust-point
 isakmp keepalive threshold 1500 retry 2
 no radius-sdi-xauth
 isakmp ikev1-user-authentication xauth
tunnel-group DefaultRAGroup ppp-attributes
 no authentication pap
 authentication chap
 authentication ms-chap-v1
 no authentication ms-chap-v2
 no authentication eap-proxy


tunnel-group DefaultRAGroup type remote-access
tunnel-group DefaultRAGroup general-attributes
 no address-pool
 no ipv6-address-pool
 authentication-server-group LOCAL
 accounting-server-group RADIUS
 default-group-policy DfltGrpPolicy
 no dhcp-server
 no strip-realm
 no password-management
 no strip-group
 no authorization-required
 authorization-dn-attributes CN OU
tunnel-group DefaultRAGroup webvpn-attributes
 hic-fail-group-policy DfltGrpPolicy
 customization DfltCustomization
 authentication aaa
 no override-svc-download
 no radius-reject-message
 dns-group DefaultDNS
tunnel-group DefaultRAGroup ipsec-attributes
 no pre-shared-key
 peer-id-validate req
 no chain
 no trust-point
 isakmp keepalive threshold 1500 retry 2
 no radius-sdi-xauth
 isakmp ikev1-user-authentication xauth
tunnel-group DefaultRAGroup ppp-attributes
 no authentication pap
 authentication chap
 authentication ms-chap-v1
 no authentication ms-chap-v2
 no authentication eap-proxy
```

Attributs généraux du groupe de tunnels IPsec

Les attributs généraux sont communs à plus d'un type de groupe de tunnels. Les tunnels d'accès à distance IPsec et de VPN SSL sans client partagent la plupart des mêmes attributs généraux. Les tunnels IPsec de réseau LAN à LAN utilisent un sous-ensemble. Reportez-vous à la *Référence des commandes de la série Cisco Secure Firewall ASA* pour obtenir une description complète de toutes les commandes. Cette section décrit, dans l'ordre, comment configurer les profils d'accès à distance et de connexion LAN à LAN.

Configurer les profils de connexion d'accès à distance.

Utilisez un profil de connexion d'accès à distance lors de la configuration d'une connexion entre les clients distants suivants et un ASA de site central :

- Secure Client (connexion avec SSL ou IPsec/IKEv2)
- VPN SSL sans client (connexion par navigateur avec SSL)
- Client matériel VPN Cisco ASA 5500 Easy (connexion avec IPsec/IKEv1)

Nous fournissons également une stratégie de groupe par défaut nommée DfltGrpPolicy.

Pour configurer un profil de connexion d'accès à distance, configurez d'abord les attributs généraux du groupe de tunnels, puis les attributs d'accès à distance. Consultez les sections suivantes :

- Préciser un nom et un type pour le profil de connexion d'accès à distance, à la page 9.
- Configurer les attributs généraux du profil de connexion d'accès à distance, à la page 10.
- Configurer de la double authentification, à la page 14
- Configurer les attributs IPsec IKEv1 du profil de connexion d'accès à distance, à la page 16.
- Configurer les attributs PPP du profil de connexion à distance IPsec, à la page 18

Préciser un nom et un type pour le profil de connexion d'accès à distance

Procédure

Créez le profil de connexion en précisant son nom et son type, en saisissant la commande **tunnel-group**.

Pour un tunnel d'accès à distance, le type est **remote-access**.

tunnel-group *tunnel_group_name* **type remote-access**

Exemple :

Par exemple, pour créer un profil de connexion d'accès à distance nommé TunnelGroup1, entrez la commande suivante :

```
hostname(config)# tunnel-group TunnelGroup1 type remote-access
hostname(config)#
```

Configurer les attributs généraux du profil de connexion d'accès à distance

Pour configurer ou modifier les attributs généraux du profil de connexion, précisez les paramètres selon les étapes suivantes.

Procédure

Étape 1 Pour configurer les attributs généraux, exécutez la tâche **tunnel-group general-attributes** en mode contexte unique ou multiple, ce qui vous place en mode de configuration tunnel-group general-attributes. L'invite change pour indiquer le changement de mode.

```
hostname(config)# tunnel-group tunnel_group_name general-attributes
hostname(config-tunnel-general)#
```

Étape 2 Précisez le nom du groupe de serveurs d'authentification, le cas échéant. Si vous souhaitez utiliser la base de données LOCAL pour l'authentification en cas d'échec du groupe de serveurs spécifié, ajoutez le mot-clé **LOCAL** :

```
hostname(config-tunnel-general)# authentication-server-group [(interface_name)] groupname
[LOCAL]
hostname(config-tunnel-general)#
```

Le nom du groupe de serveurs d'authentification peut comporter jusqu'à 16 caractères.

Vous pouvez éventuellement configurer une authentification spécifique à une interface en ajoutant le nom de l'interface après celui du groupe. Le nom de l'interface, qui indique où le tunnel se termine, doit être placé entre parenthèses. La commande suivante configure une authentification spécifique à l'interface pour l'interface nommée test, en utilisant le groupe de serveurs servergroup1 pour l'authentification :

```
hostname(config-tunnel-general)# authentication-server-group (test) servergroup1
hostname(config-tunnel-general)#
```

Étape 3 Précisez le nom du groupe de serveurs d'autorisation à utiliser, le cas échéant. Lorsque vous configurez cette valeur, les utilisateurs doivent exister dans la base de données des autorisations pour la connexion :

```
hostname(config-tunnel-general)# authorization-server-group groupname
hostname(config-tunnel-general)#
```

Le nom du groupe de serveurs d'autorisation peut comporter jusqu'à 16 caractères. Par exemple, la commande suivante précise l'utilisation du groupe de serveurs d'autorisation FinGroup :

```
hostname(config-tunnel-general)# authorization-server-groupFinGroup
hostname(config-tunnel-general)#
```

Étape 4 Précisez le nom du groupe de serveurs de comptabilité à utiliser, le cas échéant :

```
hostname(config-tunnel-general)# accounting-server-group groupname
hostname(config-tunnel-general)#
```

Le nom du groupe de serveurs de comptabilité peut comporter jusqu'à 16 caractères. Par exemple, la commande suivante spécifie l'utilisation du groupe de serveurs de comptabilité nommé comptroller :

```
hostname(config-tunnel-general)# accounting-server-group comptroller
hostname(config-tunnel-general)#
```

Étape 5 Précisez le nom de la stratégie de groupe par défaut :

```
hostname(config-tunnel-general)# default-group-policy policyname
hostname(config-tunnel-general)#
```

Le nom de la stratégie de groupe peut comporter jusqu'à 64 caractères. L'exemple suivant définit DfltGrpPolicy comme nom de la stratégie de groupe par défaut :

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

Étape 6 Précisez les noms ou les adresses IP des serveurs DHCP (jusqu'à 10 serveurs), ainsi que les noms des ensembles d'adresses DHCP (jusqu'à 6 ensembles). Les valeurs par défaut sont aucun serveur DHCP et aucun ensemble d'adresses. La commande dhcp-server permet de configurer l'ASA pour qu'il envoie des options supplémentaires aux serveurs DHCP spécifiés lorsqu'il tente d'attribuer des adresses IP aux clients VPN. Pour en savoir plus sur la commande dhcp-server, consultez le guide de référence des commandes Cisco Secure Firewall ASA.

```
hostname(config-tunnel-general)# dhcp-server server1 [...server10]
hostname(config-tunnel-general)# address-pool [(interface name)] address_pool1
[...address_pool6]
hostname(config-tunnel-general)#
```

Remarque
Si vous spécifiez un nom d'interface, vous devez le mettre entre parenthèses.

Vous configurez les ensembles d'adresses à l'aide de la commande **ip local pool** en mode de configuration globale.

Étape 7 Précisez le nom du groupe de serveurs d'authentification NAC, si vous utilisez le contrôle d'admission au réseau, afin d'identifier le groupe de serveurs utilisé pour la validation de posture NAC. Configurez au moins un serveur de contrôle d'accès pour prendre en charge la NAC. Utilisez la commande **aaa-server** pour nommer le groupe ACS. Utilisez ensuite la commande **nac-authentication-server-group** en reprenant le même nom de groupe.

L'exemple suivant identifie acs-group1 comme groupe de serveurs d'authentification utilisé pour la validation de posture NAC :

```
hostname(config-group-policy)# nac-authentication-server-group acs-group1
hostname(config-group-policy)
```

L'exemple suivant montre l'héritage du groupe de serveurs d'authentification à partir du groupe d'accès à distance par défaut :

```
hostname(config-group-policy)# no nac-authentication-server-group
```

```
hostname(config-group-policy)
```

Remarque
La NAC nécessite la présence de Cisco Trust Agent sur l'hôte distant.

Étape 8 Précisez s'il faut supprimer le groupe ou le domaine du nom d'utilisateur avant de le transmettre au serveur AAA. La valeur par défaut est de ne pas supprimer le nom de groupe ou le domaine :

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

Un domaine est un domaine administratif. Si vous supprimez le domaine, l'ASA utilise le nom d'utilisateur et le groupe (le cas échéant) pour l'authentification. Si vous supprimez le groupe, l'ASA utilise le nom d'utilisateur et le domaine (le cas échéant) pour l'authentification. Saisissez la commande **strip-realm** pour supprimer le qualificateur de domaine, et utilisez la commande strip-group pour supprimer le qualificateur de groupe du nom d'utilisateur lors de l'authentification. Si vous supprimez les deux qualificateurs, l'authentification est basée sur le *username* uniquement. Sinon, l'authentification est basée sur la chaîne complète *username@realm* ou *username<delimiter> group*. Vous devez préciser **strip-realm** si votre serveur ne peut pas analyser les délimiteurs.

Étape 9 En option, si votre serveur est un serveur RADIUS, RADIUS avec NT ou LDAP, vous pouvez également activer la gestion des mots de passe.

Remarque
Si vous utilisez un serveur de répertoire LDAP pour l'authentification, la gestion des mots de passe est prise en charge avec le Sun Microsystems JAVA System Directory Server (anciennement nommé Sun ONE Directory Server) et Microsoft Active Directory.

Le DN configuré sur l'ASA pour accéder à un serveur de répertoire Sun doit pouvoir accéder à la politique de mot de passe par défaut sur ce serveur. Nous vous conseillons d'utiliser l'administrateur de répertoire ou un utilisateur disposant des privilèges d'administrateur de répertoire, comme DN. Vous pouvez également placer une ACI sur la politique de mot de passe par défaut.

Microsoft : vous devez configurer LDAP sur SSL pour activer la gestion des mots de passe avec Microsoft Active Directory.

Cette fonctionnalité, qui est désactivée par défaut, avertit un utilisateur lorsque le mot de passe actuel est sur le point d'expirer. La valeur par défaut est de commencer à avertir l'utilisateur 14 jours avant l'expiration :

```
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

Si le serveur est un serveur LDAP, vous pouvez préciser le nombre de jours (de 0 à 180) avant l'expiration pour commencer à avertir l'utilisateur de l'expiration en attente :

```
hostname(config-tunnel-general)# password-management [password-expire in days n]
hostname(config-tunnel-general)#
```

Remarque

La commande **password-management**, saisie en mode de configuration des attributs généraux du groupe de tunnel, remplace la commande **radius-with-expiry** abandonnée qui était précédemment saisie en mode des attributs ipsec du groupe de tunnel.

Lorsque vous configurez cette commande **password-management**, l'ASA informe l'utilisateur distant lors de la connexion que le mot de passe actuel de l'utilisateur est sur le point d'expirer ou a expiré. L'ASA offre ensuite à l'utilisateur la possibilité de modifier le mot de passe. Si le mot de passe actuel n'a pas encore expiré, l'utilisateur peut toujours se connecter en utilisant ce mot de passe. L'ASA ignore cette commande si l'authentification RADIUS ou LDAP n'a pas été configurée.

Notez que cela ne modifie pas le nombre de jours avant l'expiration du mot de passe, mais plutôt le nombre de jours précédant l'expiration à partir duquel l'ASA commence à avertir l'utilisateur que le mot de passe est sur le point d'expirer.

Si vous spécifiez le mot-clé **password-expire-in-days**, vous devez également préciser le nombre de jours.

Le fait de préciser cette commande avec le nombre de jours défini à 0 désactive cette commande. L'ASA n'informe pas l'utilisateur de l'expiration en attente, mais l'utilisateur peut modifier le mot de passe après son expiration.

Consultez Configurer les paramètres de Microsoft Active Directory pour la gestion des mots de passe, à la page 30 pour de plus amples renseignements.

La version 7.1 de l'ASA et les versions ultérieures prennent généralement en charge la gestion des mots de passe pour le client VPN AnyConnect, le client VPN Cisco IPsec, le client de tunnellisation complète VPN SSL et les connexions sans client lors de l'authentification avec LDAP ou avec toute connexion RADIUS prenant en charge MS-CHAPv2. La gestion des mots de passe *n'est* pas prise en charge pour aucun de ces types de connexion pour Kerberos/AD (mot de passe Windows) ou le domaine NT 4.0.

Certains serveurs RADIUS qui prennent en charge MS-CHAP ne prennent actuellement pas en charge MS-CHAPv2. La commande **password-management** nécessite MS-CHAPv2, veuillez donc vérifier auprès de votre fournisseur.

Remarque
Le serveur RADIUS (par exemple, Cisco ACS) peut transmettre la demande d'authentification à un autre serveur d'authentification. Cependant, du point de vue de l'ASA, il ne communique qu'avec un serveur RADIUS.

Pour LDAP, la méthode de modification de mot de passe est propriétaire des différents serveurs LDAP du marché. Actuellement, l'ASA met en œuvre la logique de gestion des mots de passe propriétaire uniquement pour les serveurs Microsoft Active Directory et Sun LDAP. LDAP natif nécessite une connexion SSL. Vous devez activer LDAP sur SSL avant de tenter d'effectuer la gestion des mots de passe pour LDAP. Par défaut, LDAP utilise le port 636.

Étape 10

Étape 11 Précisez l'attribut ou les attributs à utiliser pour obtenir un nom pour une requête d'autorisation à partir d'un certificat. Cet attribut précise quelle partie du champ DN du sujet utiliser comme nom d'utilisateur pour l'autorisation :

```
hostname(config-tunnel-general)# authorization-dn-attributes {primary-attribute
[secondary-attribute] | use-entire-name}
```

Par exemple, la commande suivante spécifie l'utilisation de l'attribut CN comme nom d'utilisateur pour l'autorisation :

```
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(config-tunnel-general)#
```

Les attributs de authorization-dn-attributes sont **C** (Country), **CN** (Common Name), **DNQ** (DN qualifier), **EA** (E-mail Address), **GENQ** (Generational qualifier), **GN** (Given Name), **I** (Initials), **L** (Locality), **N** (Name), **O** (Organization), **OU** (Organizational Unit), **SER** (Serial Number), **SN** (Surname), **SP** (State/Province), **T** (Title), **UID** (User ID), et **UPN** (User Principal Name).

Étape 12 Précisez s'il faut exiger une autorisation réussie avant de permettre à un utilisateur de se connecter. Par défaut, aucune autorisation n'est exigée.

```
hostname(config-tunnel-general)# authorization-required
hostname(config-tunnel-general)#
```

Configurer de la double authentification

La double authentification est une fonctionnalité facultative qui oblige un utilisateur à saisir des informations d'authentification supplémentaires, telles qu'un deuxième nom d'utilisateur et un deuxième mot de passe, à l'écran de connexion. Précisez les commandes suivantes pour configurer la double authentification.

Procédure

Étape 1 Spécifiez le groupe de serveurs d'authentification secondaire. Cette commande spécifie le groupe de serveurs AAA à utiliser comme serveur AAA secondaire.

Remarque
Cette commande s'applique uniquement aux connexions VPN AnyConnect.

Le groupe de serveurs secondaires ne peut pas préciser un groupe de serveurs SDI. Par défaut, l'authentification secondaire n'est pas requise.

```
hostname(config-tunnel-general)# secondary-authentication-server-group [interface_name]
{none | LOCAL | groupname [LOCAL]} [use-primary-name]
```

Si vous utilisez le mot-clé none (aucun), aucune authentification secondaire n'est requise. La valeur *groupname* spécifie le nom du groupe de serveurs AAA. Local spécifie l'utilisation de la base de données du serveur interne et, lorsqu'il est utilisé avec la valeur groupname, LOCAL spécifie le repli.

Par exemple, pour définir le groupe de serveurs d'authentification principal sur sdi_group et le groupe de serveurs d'authentification secondaire sur ldap_server, entrez les commandes suivantes :

```
hostname(config-tunnel-general)# authentication-server-group
hostname(config-tunnel-general)# secondary-authentication-server-group
```

Remarque

Si vous utilisez le mot-clé **use-primary-name**, la boîte de dialogue de connexion ne demande qu'un seul nom d'utilisateur. En outre, si les noms d'utilisateurs sont extraits d'un certificat numérique, seul le nom d'utilisateur principal est utilisé pour l'authentification.

Étape 2 Si vous obtenez le nom d'utilisateur secondaire à partir d'un certificat, saisissez **secondary-username-from-certificate** :

```
hostname(config-tunnel-general)# secondary-username-from-certificate C | CN | ... | use-script
```

Les valeurs des champs DN à extraire du certificat pour utilisation comme nom d'utilisateur secondaire sont les mêmes que pour la commande **username-from-certificate** principale. Vous pouvez également spécifier le mot-clé use-script, qui ordonne à l'ASA d'utiliser un fichier de script généré par ASDM.

Par exemple, pour spécifier le nom commun comme champ de nom d'utilisateur principal et l'unité organisationnelle comme champ de nom d'utilisateur secondaire, saisissez les commandes suivantes :

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# username-from-certificate cn
hostname(config-tunnel-general)# secondary-username-from-certificate ou
```

Étape 3 Utilisez la commande **secondary-pre-fill-username** en mode tunnel-group webvpn-attributes pour activer l'extraction d'un nom d'utilisateur secondaire d'un certificat client à utiliser dans l'authentification. Utilisez les mots-clés pour préciser si cette commande s'applique à une connexion sans client ou à une connexion de client VPN SSL (AnyConnect) et si vous souhaitez masquer le nom d'utilisateur extrait de l'utilisateur final. Par défaut, cette fonction est désactivée. Les options sans client et client SSL peuvent toutes deux exister en même temps, mais vous devez les configurer dans des commandes distinctes.

```
hostname(config-tunnel-general)# secondary-pre-fill-username-from-certificate
{clientless | client} [hide]
```

Par exemple, pour spécifier l'utilisation de pre-fill-username pour l'authentification principale et secondaire d'une connexion, entrez les commandes suivantes :

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# pre-fill-username client
hostname(config-tunnel-general)# secondary-pre-fill-username client
```

Étape 4 Précisez le serveur d'authentification à utiliser pour obtenir les attributs d'autorisation à appliquer à la connexion. Le serveur d'authentification principal est la sélection par défaut. Cette commande n'est significative que pour la double authentification.

```
hostname(config-tunnel-general)# authentication-attr-from-server {primary | secondary}
```

Par exemple, pour spécifier l'utilisation du serveur d'authentification secondaire, entrez les commandes suivantes :

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# authentication-attr-from-server secondary
```

Étape 5 Précisez le nom d'utilisateur d'authentification, principal ou secondaire, à associer à la session. La valeur par défaut est primary (principale). Lorsque la double authentification est activée, il est possible que deux noms d'utilisateur distincts soient authentifiés pour la session. L'administrateur doit désigner l'un des noms d'utilisateurs authentifiés comme nom d'utilisateur de la session. Le nom d'utilisateur de session est le nom d'utilisateur fourni pour la comptabilité, la base de données de session, les journaux système et la sortie de débogage.

```
hostname(config-tunnel-general)# authenticated-session-username {primary | secondary}
```

Par exemple, pour spécifier que le nom d'utilisateur d'authentification associé à la session doit provenir du serveur d'authentification secondaire, entrez les commandes suivantes :

```
hostname(config-tunnel-general)# tunnel-group test1 general-attributes
hostname(config-tunnel-general)# authenticated-session-username secondary
```

Configurer les attributs IPsec IKEv1 du profil de connexion d'accès à distance

Pour configurer les attributs IPsec IKEv1 d'un profil de connexion d'accès à distance, procédez comme suit. La description suivante suppose que vous avez déjà créé le profil de connexion d'accès à distance. Les profils de connexion d'accès à distance ont plus d'attributs que les profils de connexion LAN à LAN.

Procédure

Étape 1 Pour préciser les attributs IPsec d'un tunnel-group (groupe de tunnels) d'accès à distance, passez en mode tunnel-group ipsec-attributes en saisissant la commande suivante en mode de contexte unique ou multiple L'invite change pour indiquer le changement de mode.

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

Cette commande passe en mode de configuration tunnel-group ipsec-attributes, dans lequel vous configurez les attributs IPsec du tunnel-group d'accès à distance en mode de contexte unique ou multiple

Par exemple, la commande suivante indique que les commandes en mode tunnel-group ipsec-attributes qui suivent s'appliquent au profil de connexion nommé TG1. Remarquez que l'invite change pour indiquer que vous êtes maintenant en mode ipsec-attributes de groupe de tunnels :

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

Étape 2 Précisez la clé prépartagée pour prendre en charge les connexions IKEv1 basées sur des clés prépartagées. Par exemple, la commande suivante spécifie la clé prépartagée xyzx pour prendre en charge les connexions IKEv1 pour un profil de connexion d'accès à distance IPsec IKEv1 :

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
```

```
hostname(config-tunnel-ipsec)#
```

Étape 3 Précisez s'il faut valider l'identité de l'homologue à l'aide du certificat d'homologue :

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

Les valeurs *d'option* possibles sont **req** (required) (obligatoire), **cert (**(if supported by certificate) (si pris en charge par certificat) et **nocheck (** (do not check) (ne pas vérifier). La valeur par défaut est **req**.

Par exemple, la commande suivante indique que la validation du peer-id (identifiant de l'homologue) est requise :

```
hostname(config-tunnel-ipsec)# peer-id-validate req
hostname(config-tunnel-ipsec)#
```

Étape 4 Précisez s'il faut activer l'envoi d'une chaîne de certificats. La commande suivante inclut le certificat racine et tous les certificats d'autorité de certification subordonnés dans la transmission :

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

Cet attribut s'applique à tous les types de groupes de tunnels IPsec.

Étape 5 Précisez le nom d'un point de confiance qui identifie le certificat à envoyer à l'homologue IKE :

```
hostname(config-tunnel-ipsec)# ikev1 trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

La commande suivante spécifie mytrustpoint comme nom du certificat à envoyer à l'homologue IKE :

```
hostname(config-ipsec)# ikev1 trust-point mytrustpoint
```

Étape 6 Précisez le seuil des messages keepalive ISAKMP et le nombre de tentatives autorisées :

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

Le paramètre **threshold** spécifie le nombre de secondes (10 à 3600) pendant lesquelles l'homologue est autorisé à passer en inactivité avant de commencer la surveillance des messages keepalive. Le paramètre **retry** est l'intervalle (de 2 à 10 secondes) entre les tentatives après qu'une réponse keepalive n'a pas été reçue. Les messages keepalive IKE sont activés par défaut. Pour désactiver les messages keepalive ISAKMP, saisissez **isakmp keepalive disable**.

Par exemple, la commande suivante définit la valeur de seuil IKE keepalive à 15 secondes et définit l'intervalle de nouvelle tentative à 10 secondes :

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

La valeur par défaut du paramètre **threshold** est de 300 pour l'accès à distance et de 10 pour LAN à LAN, et la valeur par défaut du paramètre de nouvelle tentative est 2.

Pour spécifier que le site central (passerelle sécurisée) ne doit jamais lancer la surveillance ISAKMP, entrez la commande suivante :

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

Étape 7 Précisez la méthode d'authentification hybride ISAKMP, XAUTH ou XAUTH hybride.

Vous utilisez la commande **isakmp ikev1-user-authentication** pour mettre en œuvre l'authentification hybride XAUTH lorsque vous devez utiliser des certificats numériques pour l'authentification ASA et une méthode existante différente pour l'authentification des utilisateurs VPN distants, comme RADIUS, TACACS+ ou SecurID. Hybrid XAUTH décompose la phase 1 d'IKE en deux étapes suivantes, ensemble appelées authentification hybride :

a) L'ASA s'authentifie auprès de l'utilisateur VPN distant à l'aide des techniques de clé publique standard. Cela établit une association de sécurité IKE qui est authentifiée de manière unidirectionnelle.
b) Un échange XAUTH authentifie ensuite l'utilisateur VPN distant. Cette authentification étendue peut utiliser l'une des méthodes d'authentification existantes prises en charge.

Remarque
Avant de pouvoir définir le type d'authentification sur hybride, vous devez configurer le serveur d'authentification, créer une clé prépartagée et configurer un point de confiance.

Vous pouvez utiliser la commande **isakmp ikev1-user-authentication** avec le paramètre interface facultatif pour spécifier une interface particulière. Lorsque vous omettez le paramètre d'interface, la commande s'applique à toutes les interfaces et sert de valeur de secours lorsque la commande par interface n'est pas spécifiée. Lorsque deux commandes **isakmp ikev1-user-authentication** sont spécifiées pour un profil de connexion et que l'une utilise le paramètre **d'interface** et l'autre ne le fait pas, celle qui spécifie l'interface a priorité pour cette interface particulière.

Par exemple, les commandes suivantes activent XAUTH hybride sur l'interface interne pour un profil de connexion appelé example-group :

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication (inside) hybrid
hostname(config-tunnel-ipsec)#
```

Configurer les attributs PPP du profil de connexion à distance IPsec

Pour configurer les attributs du protocole de point à point d'un profil de connexion d'accès à distance, procédez comme suit. Les attributs PPP s'appliquent *uniquement* aux profils de connexion d'accès à distance IPsec. La description suivante suppose que vous ayez déjà créé le profil de connexion d'accès à distance IPsec.

Procédure

Étape 1 Entrez en mode de configuration tunnel-group ppp-attributes, dans lequel vous configurez les attributs PPP du groupe de tunnels d'accès à distance, en entrant la commande suivante. L'invite change pour indiquer le changement de mode :

```
hostname(config)# tunnel-group tunnel-group-name type remote-access
hostname(config)# tunnel-group tunnel-group-name ppp-attributes
hostname(config-tunnel-ppp)#
```

Par exemple, la commande suivante désigne que les commandes de mode ppp-attributes du groupe de tunnels qui suivent concernent le profil de connexion nommé TG1. Remarquez que l'invite change pour indiquer que vous êtes maintenant en mode tunnel-group ppp-attributes :

```
hostname(config)# tunnel-group TG1 type remote-access
hostname(config)# tunnel-group TG1 ppp-attributes
hostname(config-tunnel-ppp)#
```

Étape 2 Précisez s'il faut activer l'authentification à l'aide de protocoles spécifiques pour la connexion PPP. La valeur du protocole peut être l'une des suivantes :

- pap : active l'utilisation du Protocole d'authentification par mot de passe pour la connexion PPP.
- chap : active l'utilisation du Protocole d'authentification par défi pour la connexion PPP.
- ms-chap-v1 ou ms-chap-v2 : active l'utilisation du Protocole Microsoft d'authentification par défi, version 1 ou version 2 pour la connexion PPP.
- eap : active l'utilisation du protocole d'authentification extensible (EAP) pour la connexion PPP.

CHAP et MSCHAPv1 sont activés par défaut.

Voici la syntaxe de la commande :

```
hostname(config-tunnel-ppp)# authentication protocol
hostname(config-tunnel-ppp)#
```

Pour désactiver l'authentification pour un protocole en particulier, utilisez la forme **no** de la commande :

```
hostname(config-tunnel-ppp)# no authentication protocol
hostname(config-tunnel-ppp)#
```

Par exemple, la commande suivante active l'utilisation du protocole PAP pour une connexion PPP :

```
hostname(config-tunnel-ppp)# authentication pap
hostname(config-tunnel-ppp)#
```

La commande suivante permet l'utilisation du protocole MS-CHAP, version 2 pour une connexion PPP :

```
hostname(config-tunnel-ppp)# authentication ms-chap-v2
```

```
hostname(config-tunnel-ppp)#
```

La commande suivante permet l'utilisation du protocole EAP-PROXY pour une connexion PPP :

```
hostname(config-tunnel-ppp)# authentication pap
hostname(config-tunnel-ppp)#
```

La commande suivante désactive l'utilisation du protocole MS-CHAP, version 1 pour une connexion PPP :

```
hostname(config-tunnel-ppp)# no authentication ms-chap-v1
hostname(config-tunnel-ppp)#
```

Configurer les profils de connexion LAN-à-LAN

Un profil de connexion VPN IPsec LAN à LAN s'applique uniquement aux connexions client IPsec LAN à LAN. Alors que de nombreux paramètres que vous configurez sont les mêmes que pour les profils de connexion d'accès à distance IPsec, les tunnels LAN à LAN ont moins de paramètres. Les sections suivantes vous montrent comment configurer un profil de connexion LAN à LAN :

- Préciser un nom et un type pour un profil de connexion LAN à LAN, à la page 20
- Configurer les attributs généraux du profil de connexion LAN-à-LAN, à la page 21
- Configurer les attributs IPsec IKEv1 de site à site (LAN à LAN), à la page 21

Configurer le profil de connexion LAN à LAN par défaut

Le contenu du profil de connexion LAN à LAN par défaut est le suivant :

```
tunnel-group DefaultL2LGroup type ipsec-l2l
tunnel-group DefaultL2LGroup general-attributes
 default-group-policy DfltGrpPolicy
tunnel-group DefaultL2LGroup ipsec-attributes
 no ikev1 pre-shared-key
 peer-id-validate req
 no chain
 no ikev1 trust-point
 isakmp keepalive threshold 10 retry 2
```

Les profils de connexion de réseau local (LAN à réseau local) ont moins de paramètres que les profils de connexion d'accès à distance, et la plupart de ces paramètres sont les mêmes pour les deux groupes. Pour faciliter la configuration de la connexion, elles sont répertoriées séparément ici. Tous les paramètres que vous ne configurez pas explicitement héritent de leurs valeurs du profil de connexion par défaut.

Préciser un nom et un type pour un profil de connexion LAN à LAN

Pour spécifier un nom et un type pour un profil de connexion, entrez la commande **tunnel-group**, comme suit :

```
hostname(config)# tunnel-group tunnel_group_name type tunnel_type
```

Pour un tunnel LAN à LAN, le type est **ipsec-l2l** ; par exemple, pour créer le profil de connexion LAN à LAN nommé docs, saisissez la commande suivante :

```
hostname(config)# tunnel-group docs type ipsec-l2l
hostname(config)#
```

Configurer les attributs généraux du profil de connexion LAN-à-LAN

Pour configurer les attributs généraux du profil de connexion, procédez comme suit :

Procédure

Étape 1 Entrez en mode tunnel-group general-attributes en précisant le mot-clé general-attributes en mode contexte unique ou multiple :

tunnel-group *tunnel-group-name* **general-attributes**

Exemple :

Pour le profil de connexion nommé docs, entrez la commande suivante :

```
hostname(config)# tunnel-group docs general-attributes
hostname(config-tunnel-general)#
```

L'invite change pour indiquer que vous êtes maintenant en mode config-general, dans lequel vous configurez les attributs généraux du groupe de tunnels.

Étape 2 Précisez le nom de la stratégie de groupe par défaut :

default-group-policy *policyname*

Exemple :

La commande suivante spécifie que le nom de la stratégie de groupe par défaut est MyPolicy :

```
hostname(config-tunnel-general)# default-group-policy MyPolicy
hostname(config-tunnel-general)#
```

Configurer les attributs IPsec IKEv1 de site à site (LAN à LAN)

Pour configurer les attributs IPsec IKEv1, procédez comme suit :

Procédure

Étape 1 Pour configurer les attributs IPsec IKEv1 du groupe de tunnels, entrez en mode de configuration tunnel-group ipsec-attributes en utilisant la commande tunnel-group avec le mot-clé ipsec-attributes, en mode de contexte unique ou multiple.

```
hostname(config)# tunnel-group tunnel-group-name ipsec-attributes
hostname(config-tunnel-ipsec)#
```

Par exemple, la commande suivante passe en mode config-ipsec afin que vous puissiez configurer les paramètres du profil de connexion nommé TG1 :

```
hostname(config)# tunnel-group TG1 ipsec-attributes
hostname(config-tunnel-ipsec)#
```

L'invite change pour indiquer que vous êtes maintenant en mode de configuration ipsec-attributes de groupe de tunnels.

Étape 2 Précisez la clé prépartagée pour prendre en charge les connexions IKEv1 basées sur des clés prépartagées.

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key key
hostname(config-tunnel-ipsec)#
```

Par exemple, la commande suivante spécifie la clé prépartagée XYZX pour prendre en charge les connexions IKEv1 pour un profil de connexion LAN-à-LAN :

```
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key xyzx
hostname(config-tunnel-general)#
```

Étape 3 Précisez s'il faut valider l'identité de l'homologue à l'aide du certificat d'homologue :

```
hostname(config-tunnel-ipsec)# peer-id-validate option
hostname(config-tunnel-ipsec)#
```

Les options disponibles sont **req** required (obligatoire), **cert (** if-supported (si pris en charge par certificat) et **nocheck (** do-not-check (ne pas vérifier). La valeur par défaut est **req**. Par exemple, la commande suivante définit l'option peer-id-validate à **nocheck** :

```
hostname(config-tunnel-ipsec)# peer-id-validate nocheck
hostname(config-tunnel-ipsec)#
```

Étape 4 Précisez s'il faut activer l'envoi d'une chaîne de certificats. Cette action inclut le certificat racine et tous les certificats d'autorité de certification subordonnés dans la transmission :

```
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

Vous pouvez appliquer cet attribut à tous les types de groupes de tunnels.

Étape 5 Précisez le nom d'un point de confiance qui identifie le certificat à envoyer à l'homologue IKE :

```
hostname(config-tunnel-ipsec)# trust-point trust-point-name
hostname(config-tunnel-ipsec)#
```

Par exemple, la commande suivante définit le nom du point de confiance comme mytrustpoint :

```
hostname(config-tunnel-ipsec)# trust-point mytrustpoint
hostname(config-tunnel-ipsec)#
```

Vous pouvez appliquer cet attribut à tous les types de groupes de tunnels.

Étape 6 Précisez le seuil keepalive d'ISAKMP (IKE) et le nombre de tentatives autorisées. Le paramètre **threshold** spécifie le nombre de secondes (10 à 3 600) pendant lesquelles l'homologue est autorisé à passer en inactivité avant de commencer la surveillance des messages keepalive. Le paramètre **retry** est l'intervalle (de 2 à 10 secondes) entre les tentatives après qu'une réponse keepalive n'a pas été reçue. Les messages keepalive IKE sont activés par défaut. Pour désactiver les messages keepalive IKE, saisissez la forme **no** de la commande **isakmp** :

```
hostname(config)# isakmp keepalive threshold <number> retry <number>
hostname(config-tunnel-ipsec)#
```

Par exemple, la commande suivante définit le seuil ISAKMP keepalive à 15 secondes et définit l'intervalle de nouvelle tentative à 10 secondes :

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

La valeur par défaut du paramètre **threshold** pour LAN à LAN est 10 et la valeur par défaut du paramètre de nouvelle tentative est 2.

Pour spécifier que le site central (passerelle sécurisée) ne doit jamais lancer la surveillance ISAKMP, entrez la commande suivante :

```
hostname(config-tunnel-ipsec)# isakmp keepalive threshold infinite
hostname(config-tunnel-ipsec)#
```

Étape 7 Précisez la méthode d'authentification hybride ISAKMP, XAUTH ou XAUTH hybride.

Vous utilisez la commande **isakmp ikev1-user-authentication** pour mettre en œuvre l'authentification hybride XAUTH lorsque vous devez utiliser des certificats numériques pour l'authentification ASA et une méthode existante différente pour l'authentification des utilisateurs VPN distants, comme RADIUS, TACACS+ ou SecurID. Hybrid XAUTH décompose la phase 1 d'IKE en deux étapes suivantes, ensemble appelées authentification hybride :

a) L'ASA s'authentifie auprès de l'utilisateur VPN distant à l'aide des techniques de clé publique standard. Cela établit une association de sécurité IKE qui est authentifiée de manière unidirectionnelle.
b) Un échange XAUTH authentifie ensuite l'utilisateur VPN distant. Cette authentification étendue peut utiliser l'une des méthodes d'authentification existantes prises en charge.

Remarque
Avant de pouvoir définir le type d'authentification sur hybride, vous devez configurer le serveur d'authentification, créer une clé prépartagée et configurer un point de confiance.

Par exemple, les commandes suivantes activent XAUTH hybride pour un profil de connexion appelé example-group :

```
hostname(config)# tunnel-group example-group type remote-access
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication hybrid
hostname(config-tunnel-ipsec)#
```

À propos des groupes de tunnels pour les clients IKEv2 basés sur les normes

Un groupe de tunnels est un ensemble d'enregistrements qui contiennent des politiques de connexion de tunnel. Vous configurez un groupe de tunnels pour identifier les serveurs AAA, préciser les paramètres de connexion et définir une stratégie de groupe par défaut. L'ASA stocke les groupes de tunnels en interne.

Le groupe de tunnels par défaut pour l'accès à distance IPsec est DefaultRAGroup. Vous pouvez modifier le groupe de tunnels par défaut, mais pas le supprimer.

IKEv2 permet la configuration de méthodes d'authentification asymétriques (c'est-à-dire l'authentification par clé prépartagée pour l'initiateur, mais l'authentification par certificat ou l'authentification EAP pour le répondeur) à l'aide d'interfaces de ligne de commande d'authentification locale et distante distinctes. Par conséquent, avec IKEv2, vous avez une authentification asymétrique, dans laquelle un côté s'authentifie avec un identifiant et l'autre côté utilise un autre identifiant (une clé prépartagée, un certificat ou un EAP).

Le groupe DefaultRAGroup doit être configuré pour l'authentification EAP, car ces connexions client ne peuvent pas être mappées à un groupe de tunnels spécifique, sauf si l'authentification par certificat est utilisée avec la correspondance du DN du certificat.

Prise en charge des attributs IKEv2 basée sur les normes

L'ASA prend en charge les attributs IKEv2 suivants :

- INTERNAL_IP4_ADDRESS / INTERNAL_IP6_ADDRESS : adresse IPv4 ou IPv6

Remarque La double pile (affectation d'une adresse IPv4 et IPv6) n'est pas prise en charge pour IKEv2. Si une adresse IPv4 et une adresse IPv6 sont demandées et que les deux adresses peuvent être attribuées, seule une adresse IPv4 est attribuée.

- INTERNAL_IP4_NETMASK : masque réseau d'adresses IPv4
- INTERNAL_IP4_DNS/INTERNAL_IP6_DNS : adresse DNS principale/secondaire
- INTERNAL_IP4_NBNS : adresse WINS principale/secondaire
- INTERNAL_IP4_SUBNET/INTERNAL_IP6_SUBNET : listes de tunnellisation fractionnée

- APPLICATION_VERSION : ignoré. Aucune réponse n'est envoyée pour éviter de communiquer des informations de version sur l'ASA pour des raisons de sécurité. Cependant, la demande de charge utile de configuration du client peut inclure cet attribut, et la chaîne apparaît sur l'ASA dans la sortie de commande **vpn-sessiondb** et dans le journal système.

Prise en charge DAP

Pour autoriser la configuration de politiques DAP par type de connexion, un nouveau type de client, IPsec-IKEv2-Generic-RA, peut être utilisé pour appliquer une politique propre à ce type de connexion.

Sélection de groupe de tunnels pour les clients d'accès à distance

Le tableau suivant fournit une liste des clients d'accès à distance et des options de groupe de tunnels disponibles :

Client d'accès à distance	Liste des groupes de tunnels	URL du groupe	Mise en correspondance du nom distinctif du certificat	Groupe par défaut (Groupe de RA par défaut)	Autre
Cisco AnyConnect VPN Client	Oui	Oui	Oui	Oui	S. O.
Windows L2TP/IPsec (Mode principal IKEv1)	Non	Non	• Oui (lors de l'utilisation de certificats de machine locale) • Non (lors de l'utilisation d'un protocole PSK)	Oui	S. O.
IKEv2 basé sur les normes	Non	Non	• Oui (lors de l'utilisation de certificats de machine locale) • Non (lors de l'utilisation de l'authentification EAP)	Oui **Remarque** Vous devez utiliser le groupe de tunnels DefaultRAGroup.	s.o.

Prise en charge de l'authentification pour les clients IKEv2 basés sur les normes

Le tableau suivant fournit une liste des clients IKEv2 basés sur les normes et les méthodes d'authentification prises en charge :

Remarque Les limites de la méthode d'authentification sont basées sur le manque de prise en charge sur le client, et non sur l'ASA. Toute l'authentification EAP est relayée par l'ASA en tant que proxy entre le client et le serveur EAP. La prise en charge des méthodes EAP dépend du client et du serveur EAP pour la méthode EAP.

Type de client/Méthode d'authentification	EAP-TLS	EAP-MSCHAPv2	EAP-MD5	Certificat uniquement	PSK
StrongSwan sur Linux	S. O.	• ISE : oui • ACS : oui • FreeRadius : oui • AD via FreeRadius : oui	• ISE : oui • ACS : oui • FreeRadius : oui • AD via FreeRadius : oui	Oui	Oui
StrongSwan sur Android	S. O.	• ISE : oui • ACS : oui • FreeRadius : oui • AD via FreeRadius : oui	Non	Oui	S.O.
Windows 7/8/8.1	• ISE : oui • ACS : oui • FreeRadius : oui • AD via FreeRadius : oui	• ISE : oui • ACS : oui • FreeRadius : oui • AD via FreeRadius : oui	s.o.	Oui	S.O.
Windows Phone	• ISE : oui • ACS : oui • FreeRadius : oui • AD via FreeRadius : oui	• ISE : oui • ACS : oui • FreeRadius : oui • AD via FreeRadius - Oui	s.o.	s.o.	s.o.

Type de client/Méthode d'authentification	EAP-TLS	EAP-MSCHAPv2	EAP-MD5	Certificat uniquement	PSK
Samsung Knox	S. O.	• ISE : oui • ACS : oui • FreeRadius : oui • AD via FreeRadius - Oui	• ISE : oui • ACS : oui • FreeRadius : oui • AD via FreeRadius - Oui	Oui	S. O.
iOS 8	• ISE : oui • ACS : oui • FreeRadius : oui • AD via FreeRadius - Oui	• ISE : oui • ACS : oui • FreeRadius : oui • AD via FreeRadius : oui	S. O.	Oui	Oui
Client natif Android	S. O.	• ISE : oui • ACS : oui • FreeRadius : oui • AD via FreeRadius	S. O.	Oui	Oui

Authentification de plusieurs certificats

Le protocole d'authentification agrégé a été étendu pour définir l'échange de protocole pour l'authentification à certificats multiples et l'utiliser pour les deux types de sessions. Une fois que le client a établi une connexion SSL et est entré dans l'authentification agrégée, une autre connexion SSL est établie et l'ASA voit que le client nécessite une authentification par certificat et demande le certificat client.

L'ASA configure l'authentification requise pour une connexion Secure Client (services client sécurisés) d'un groupe de tunnels de type accès à distance. Un mappage de groupe de tunnels est effectué avec les méthodes existantes telles que le mappage de règle de certificat, l'URL de groupe, etc., mais les méthodes d'authentification requises sont négociées avec le client.

Exemple

groupe de tunnels <name> attributs-webvpn

authentification {aaa [certificat | certificat multiple] | certificat multiple [aaa | saml] | saml [certificat | certificat multiple]}

Les options d'authentification sont AAA uniquement, certificat uniquement, certificats multiples uniquement, AAA et certificat, AAA et certificats multiples, SAML, SAML et certificat, ou certificats multiples et SAML.

```
ASA(config)# tunnel-group AnyConnect webvpn-attributes
ASA(config-tunnel-webvpn)# authentication?
tunnel-group-webvpn mode commands/options:
aaa         Use username and password for authentication
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
saml   Use SAML for authentication
ASA(config-tunnel-webvpn)# authentication multiple-certificate?

tunnel-group-webvpn mode commands/options:
aaa  Use username and password for authentication
saml  Use SAML for authentication
<cr>

ASA(config-tunnel-webvpn)# authentication aaa?

tunnel-group-webvpn mode commands/options:
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
<cr>ASA(config-tunnel-webvpn)# authentication aaa?

ASA(config-tunnel-webvpn)# authentication saml?
tunnel-group-webvpn mode commands/options:
certificate Use certificate for authentication
multiple-certificate Use multiple certificates for authentication
<cr>
```

Configurer l'option query-identity pour la récupération de l'identité EAP

Le client Microsoft Windows 7 IKEv2 envoie une adresse IP comme identité Internet Key Exchange (IKE), ce qui empêche le serveur Cisco ASA de l'utiliser efficacement pour la recherche du groupe de tunnels. L'ASA doit être configuré avec l'option **query-identity** pour l'authentification EAP afin de permettre à l'ASA de récupérer une identité EAP valide du client.

Pour l'authentification basée sur les certificats, le serveur ASA et les certificats client Microsoft Windows 7 doivent comporter un champ Extended Key Usage (EKU) comme suit :

- Pour le certificat client, champ EKU = certificat d'authentification du client.
- Pour le certificat de serveur, champ EKU = certificat d'authentification du serveur.

Vous pouvez obtenir les certificats auprès du serveur de certificats Microsoft ou d'un autre serveur d'autorité de certification.

Pour l'authentification EAP, le client Microsoft Windows 7 IKEv2 attend une demande d'identité EAP avant toute autre demande EAP. Assurez-vous de configurer le mot-clé **query-identity** dans le profil de groupe de tunnels sur le serveur ASA IKEv2 afin d'envoyer au client une demande d'identité EAP.

Remarque L'interception DHCP est prise en charge pour IKEv2 afin de permettre à Windows d'effectuer la tunnellisation fractionnée. Cette fonctionnalité ne fonctionne qu'avec les attributs de tunnellisation fractionnée IPv4.

Procédure

Étape 1 Pour définir le type de connexion sur l'accès à distance IPsec, saisissez la commande **tunnel-group**. La syntaxe est **tunnel-group** *nom* **type***type*, où nom est le nom que vous attribuez au groupe de tunnels, et type est le type de tunnel.

Dans l'exemple suivant, la clé prépartagée IKEv2 est configurée comme suit : 44kkaol59636jnfx

```
hostname(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 44kkaol59636jnfx
```

Remarque
Vous devez configurer la commande **ikev2 remote-authentication pre-shared-key** ou la commande **ikev2 remote-authentication certificate** pour terminer l'authentification.

Étape 2 Pour préciser le protocole EAP (Extensible Authentication Protocol) comme méthode prenant en charge l'authentification des utilisateurs avec des clients tiers d'accès à distance IKEv2 conformes aux normes, utilisez la commande **ikev2 remote-authentication eap** [**query-identity**].

Remarque
Avant de pouvoir activer EAP pour l'authentification à distance, vous devez configurer l'authentification locale à l'aide d'un certificat et configurer un point de confiance valide à l'aide de la commande **ikev2 local-authentication** {**certificate** *trustpoint*}. Sinon, la demande d'authentification EAP est rejetée.

Vous pouvez configurer plusieurs options qui permettent au client d'utiliser n'importe laquelle des options configurées, mais non pas toutes, pour l'authentification à distance.

Pour les connexions IKEv2, le mappage du groupe de tunnels doit déterminer quelles méthodes d'authentification autoriser pour l'authentification à distance (PSK, certificat et EAP) et pour l'authentification locale (PSK et certificat), ainsi que le point de confiance à utiliser pour l'authentification locale. Actuellement, le mappage est effectué à l'aide de l'ID IKE, extrait de la valeur du champ de l'homologue ou du certificat homologue au moyen de la carte de certificats. Si les deux options échouent, la connexion entrante est mappée au groupe de tunnels d'accès à distance par défaut, DefaultRAGroup. Une carte de certificats est une option applicable uniquement lorsque l'homologue distant est authentifié par un certificat. Cette carte permet le mappage vers différents groupes de tunnels. Pour l'authentification par certificat uniquement, la recherche de groupe de tunnels est effectuée à l'aide de règles ou à l'aide du paramètre par défaut. Pour l'authentification EAP et PSK, la recherche du groupe de tunnels est effectuée à l'aide de l'ID IKE sur le client, lequel correspond au nom du groupe de tunnels, ou à l'aide du paramètre par défaut.

Pour l'authentification EAP, vous devez utiliser le groupe de tunnels DefaultRAGroup, sauf si le client autorise la configuration indépendante de l'identifiant IKE et du nom d'utilisateur.

L'exemple suivant montre le refus d'une demande EAP d'authentification :

```
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 12345678
ERROR: The local-authentication method is required to be certificate based
if remote-authentication allows EAP
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

Étape 3 Enregistrez vos modifications.

```
hostname(config)# write memory
hostname(config)#
```

Pour vérifier que le tunnel est établi et fonctionnel, utilisez la commande **show vpn-sessiondb summary** ou **show crypto ipsec sa**.

Configurer les paramètres de Microsoft Active Directory pour la gestion des mots de passe

Si vous utilisez un serveur de répertoire LDAP pour l'authentification, la gestion des mots de passe est prise en charge avec le Sun Microsystems JAVA System Directory Server (anciennement nommé Sun ONE Directory Server) et Microsoft Active Directory.

- Sun : le DN configuré sur l'ASA pour accéder à un serveur de répertoire Sun doit pouvoir accéder à la politique de mot de passe par défaut sur ce serveur. Nous vous conseillons d'utiliser l'administrateur de répertoire ou un utilisateur disposant des privilèges d'administrateur de répertoire, comme DN. Vous pouvez également placer une ACI sur la politique de mot de passe par défaut.
- Microsoft : vous devez configurer LDAP sur SSL pour activer la gestion des mots de passe avec Microsoft Active Directory.

Pour utiliser la gestion des mots de passe avec Microsoft Active Directory, vous devez définir certains paramètres Active Directory et configurer également la gestion des mots de passe sur l'ASA. Cette section décrit les paramètres Active Directory associés à diverses actions de gestion de mots de passe. Ces descriptions supposent que vous ayez également activé la gestion des mots de passe sur l'ASA et configuré les attributs correspondants de gestion des mots de passe. Les étapes précises de cette section renvoient à la terminologie Active Directory sous Windows 2000. Cette section suppose que vous utilisez un serveur de répertoire LDAP pour l'authentification.

Utiliser Active Directory pour forcer l'utilisateur à modifier le mot de passe lors de la prochaine connexion

Pour forcer un utilisateur à modifier le mot de passe d'utilisateur lors de la connexion suivante, spécifiez la commande **password-management** en mode de configuration des attributs généraux du groupe de tunnels sur l'ASA et effectuez les étapes suivantes sous Active Directory :

Procédure

Étape 1 Choisissez **Start (Démarrer)** > **Programs (Programmes)** > **Administrative Tools (Outils d'administration)** > **Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory**.

Étape 2 Cliquez avec le bouton droit pour choisir **Username (Nom d'utilisateur)** > **Username (Nom d'utilisateur)** > **Account (Compte)**.

Étape 3 Cochez la case **User must change password at next logon** (L'utilisateur doit changer le mot de passe à la prochaine connexion).

Lors de la prochaine connexion de cet utilisateur, l'ASA affiche l'invite suivante : « New password required (Nouveau mot de passe requis). Changement de mot de passe requis You must enter a new password with a minimum length *n* to continue ». (Vous devez saisir un nouveau mot de passe d'une longueur minimale de n pour continuer.) Vous pouvez définir la longueur minimale de mot de passe requise, *n*, dans le cadre de la configuration Active Directory en accédant à Start (Démarrer) > Programs (Programmes) > Administrative Tools (Outils d'administration) > Domain Security Policy (Politique de sécurité de domaine) > Windows Settings (Paramètres Windows) > Security Settings (Paramètres de sécurité) > Account Policies (Politiques de compte) > Password Policy (Politique de mot de passe). Sélectionnez **Minimum password length** (Longueur minimale du mot de passe).

Utiliser Active Directory pour préciser l'ancienneté maximale du mot de passe

Pour renforcer la sécurité, vous pouvez spécifier que les mots de passe expirent après un certain nombre de jours. Pour spécifier un âge de mot de passe maximal pour un mot de passe d'utilisateur, spécifiez la commande **password-management** en mode de configuration d'attributs généraux de groupe de tunnel sur l'ASA et effectuez les étapes suivantes sous Active Directory :

Remarque La commande **radius-with-expiry**, précédemment configurée dans le cadre de la configuration tunnel-group remote-access pour gérer l'âge du mot de passe, est obsolète. La commande **password-management**, saisie en mode tunnel-group general-attributes, la remplace.

Procédure

Étape 1 Choisissez **Start (Démarrer)** > **Programs (Programmes)** > **Administrative Tools (Outils d'administration) ,** > **Domain Security Policy (Politique de sécurité du domaine)** > **Windows Settings (Paramètres Windows) ,** > **Security Settings (Paramètres de sécurité) ,** > **Account Policies (Politiques de compte) ,** > **Password Policy (Politique de mot de passe)**.

Étape 2 Double-cliquez sur Âge maximal du mot de passe.

Étape 3 Cochez la case **Define this policy setting** (Définir ce paramètre de politique) et précisez l'âge maximal du mot de passe, en jours, que vous souhaitez autoriser.

Utiliser Active Directory pour appliquer la longueur minimale du mot de passe

Pour appliquer une longueur minimale pour les mots de passe, spécifiez la commande **password-management** en mode de configuration d'attributs généraux de groupe de tunnels sur l'ASA et effectuez les étapes suivantes sous Active Directory :

Procédure

Étape 1 Choisissez **Start (Démarrer)** > **Programs (Programmes)** > **Administrative Tools (Outils administratifs)** > **Domain Security Policy (Stratégie de sécurité du domaine)**.

Étape 2 Choisissez **Paramètres de Windows** > **Paramètres de sécurité** > **Politiques de compte** > **Politique de mot de passe**.

Étape 3 Double-cliquez sur **Minimum Password Length** (Longueur minimale du mot de passe).

Étape 4 Cochez la case **Define this policy setting** (Définir ce paramètre de politique), puis indiquez le nombre minimal de caractères requis pour le mot de passe.

Utiliser Active Directory pour appliquer la complexité du mot de passe

Pour appliquer des mots de passe complexes, par exemple, pour exiger qu'un mot de passe contienne des lettres majuscules et minuscules, des chiffres et des caractères spéciaux, saisissez la commande **password-management** en mode de configuration des attributs généraux du groupe de tunnels sur l'ASA et effectuez les étapes suivantes sous Active Directory :

Procédure

Étape 1 Choisissez **Start (Démarrer)** > **Programs (Programmes)** > **Administrative Tools (Outils d'administration)** > **Domain Security Policy (Politique de sécurité du domaine). Sélectionnez Windows Settings (Paramètres Windows)** > **Security Settings (Paramètres de sécurité)** > **Account Policies (Politiques de compte)** > **Password Policy (Politique de mot de passe)**.

Étape 2 Double-cliquez sur Password must meet complexity requirements (Le mot de passe doit respecter les exigences de complexité) pour ouvrir la boîte de dialogue Security Policy Setting (Paramètre de stratégie de sécurité).

Étape 3 Cochez la case Define this policy setting (Définir ce paramètre de politique) et sélectionnez **Enable** (Activer).

L'application de la complexité des mots de passe ne prend effet que lorsque l'utilisateur modifie son mot de passe ; par exemple, lorsque vous avez configuré Enforce password change at next login (Forcer le changement de mot de passe à la prochaine ouverture de session) ou Password expires in *n* days (Le mot de passe expire dans n jours). Au moment de la connexion, l'utilisateur reçoit un message pour saisir un nouveau mot de passe, et le système n'acceptera qu'un mot de passe complexe.

Configurer le profil de connexion pour la prise en charge des messages RADIUS/SDI pour Secure Client (services client sécurisés)

Cette section décrit les procédures pour s'assurer que le client VPN AnyConnect utilisant des jetons du logiciel RSA SecureID peut répondre correctement aux invites d'utilisateur fournies au client par l'intermédiaire d'un proxy RADIUS vers un ou plusieurs serveurs SDI.

Remarque Si vous avez configuré la fonctionnalité de double authentification, l'authentification SDI est prise en charge uniquement sur le serveur d'authentification principal.

Lorsqu'un utilisateur distant se connecte à l'ASA avec le client VPN AnyConnect et tente de s'authentifier à l'aide d'un jeton RSA SecurID, l'ASA communique avec le serveur RADIUS, qui à son tour, communique avec le serveur SDI au sujet de l'authentification.

Lors de l'authentification, le serveur RADIUS présente des messages de défi d'accès à l'ASA. Ces messages de défi comprennent des messages de réponse contenant du texte du serveur SDI. Le texte du message est différent lorsque l'ASA communique directement avec un serveur SDI que lorsqu'il communique par l'intermédiaire du proxy RADIUS. Par conséquent, afin d'apparaître en tant que serveur SDI natif auprès du Secure Client (services client sécurisés), l'ASA doit interpréter les messages du serveur RADIUS.

De plus, comme les messages SDI sont configurables sur le serveur SDI, le texte du message sur l'ASA doit correspondre (en tout ou en partie) au texte du message sur le serveur SDI. Sinon, les invites affichées à l'utilisateur du client distant peuvent ne pas être appropriées pour l'action requise lors de l'authentification. Le Secure Client (services client sécurisés) peut ne pas répondre et l'authentification peut échouer.

Configurer l'appareil de sécurité pour prendre en charge les messages RADIUS/SDI, à la page 33 décrit comment configurer l'ASA pour assurer une authentification réussie entre le client et le serveur SDI.

Configurer l'appareil de sécurité pour prendre en charge les messages RADIUS/SDI

Pour configurer l'ASA afin qu'il interprète les messages de réponse RADIUS propres à SDI et invite l'utilisateur Secure Client (services client sécurisés) à prendre la mesure appropriée, procédez comme suit :

Procédure

Étape 1 Configurez un profil de connexion (groupe de tunnels) pour transférer les messages de réponse RADIUS de manière à simuler une communication directe avec un serveur SDI à l'aide de la commande **proxy-auth sdi**, en mode de configuration tunnel-group webvpn. Les utilisateurs s'authentifiant auprès du serveur SDI doivent se connecter sur ce profil de connexion.

Exemple :

```
hostname(config)# tunnel-group sales webvpn attributes
hostname(tunnel-group-webvpn)# proxy-auth sdi
```

Étape 2 Configurez sur l'ASA le texte du message de réponse RADIUS pour qu'il corresponde, en tout ou en partie, au texte du message envoyé par le serveur RADIUS à l'aide de la commande **proxy-auth_map sdi**, en mode de configuration tunnel-group webvpn.

Le texte du message par défaut utilisé par l'ASA est le texte du message par défaut utilisé par le serveur Cisco Secure Access Control Server (ACS). Si vous utilisez Cisco Secure ACS et qu'il utilise le texte de message par défaut, vous n'avez pas besoin de configurer le texte de message sur l'ASA. Sinon, utilisez la commande **proxy-auth_map sdi** pour vous assurer que le texte du message correspond.

Le tableau ci-dessous présente le code de message, le texte du message de réponse RADIUS par défaut et la fonction de chaque message. Comme l'appareil de sécurité recherche les chaînes dans l'ordre où elles apparaissent dans le tableau, vous devez vous assurer que la chaîne utilisée pour le texte du message n'est pas un sous-ensemble d'une autre chaîne.

Par exemple, « nouveau NIP » est un sous-ensemble du texte de message par défaut pour new-pin-sup et next-ccode-and-reauth. Si vous configurez new-pin-sup comme « nouveau NIP », lorsque l'appareil de sécurité reçoit « nouveau NIP avec le code de carte suivant » du serveur RADIUS, il fera correspondre le texte au code new-pin-sup plutôt qu'au code next-ccode-and-reauth.

Codes d'opération SDI, texte du message par défaut et fonction du message

Code de message	Texte du message de réponse RADIUS par défaut	Fonction
code suivant	Veuillez entrer le code d'accès suivant	Indique que l'utilisateur doit saisir le NEXT tokencode sans le NIP.
new-pin-sup	N'oubliez pas votre nouveau NIP	Indique que le nouveau NIP système a été fourni et affiche ce NIP pour l'utilisateur.
new-pin-meth	Voulez-vous saisir votre propre code NIP	Demande à l'utilisateur quelle nouvelle méthode de code NIP utiliser pour créer un nouveau NIP.
new-pin-req	Entrez votre nouveau NIP alphanumérique	Indique un NIP généré par l'utilisateur et demande à l'utilisateur de saisir le NIP.
new-pin-reenter	Saisir de nouveau le NIP :	Utilisé en interne par l'ASA pour la confirmation du NIP fourni par l'utilisateur. Le client confirme le NIP sans demander à l'utilisateur de le saisir.
new-pin-sys-ok	Nouveau NIP accepté	Indique que le NIP fourni par l'utilisateur a été accepté.
next-ccode-and-reauth	nouveau NIP avec le code de carte suivant	Fait suite à une opération de NIP et indique que l'utilisateur doit attendre le prochain tokencode et saisir à la fois le nouveau NIP et le tokencode suivant pour s'authentifier.
ready-for-sys-pin	Accepter un NIP généré par le système	Utilisé en interne par l'ASA pour indiquer que l'utilisateur est prêt à recevoir le NIP généré par le système.

L'exemple suivant passe en mode aaa-server-host et modifie le texte du message de réponse RADIUS new-pin-sup :

```
hostname(config)# aaa-server radius_sales host 10.10.10.1
hostname(config-aaa-server-host)# proxy-auth_map sdi new-pin-sup "This is your new PIN"
```

Stratégies de groupe

Cette section décrit les stratégies de groupe et comment les configurer.

Une stratégie de groupe est un ensemble de paires d'attributs/valeurs orientées utilisateur pour les connexions IPsec qui sont stockées en interne (localement) sur le périphérique ou en externe sur un serveur RADIUS. Le profil de connexion utilise une politique de groupe qui définit les conditions de connexions des utilisateurs après l'établissement du tunnel. Les stratégies de groupe vous permettent d'appliquer des ensembles complets d'attributs à un utilisateur ou à un groupe d'utilisateurs, plutôt que d'avoir à spécifier chaque attribut individuellement pour chaque utilisateur.

Saisissez les commandes **group-policy** en mode de configuration globale pour affecter une stratégie de groupe aux utilisateurs ou pour modifier une stratégie de groupe pour des utilisateurs spécifiques.

L'ASA comprend une stratégie de groupe par défaut. En plus de la stratégie de groupe par défaut, que vous pouvez modifier mais pas supprimer, vous pouvez créer une ou plusieurs stratégies de groupe spécifiques à votre environnement.

Vous pouvez configurer des stratégies de groupe internes et externes. Les groupes internes sont configurés sur la base de données interne de l'ASA. Les groupes externes sont configurés sur un serveur d'authentification externe, tel que RADIUS. Les stratégies de groupe comprennent les attributs suivants :

- Identité
- Définitions de serveur
- Paramètres de pare-feu client
- Protocoles de tunnelisation
- Paramètres IPsec
- Paramètres matériels
- Filtres
- Paramètres de configuration client
- Paramètres de connexion

Modifier la stratégie de groupe par défaut

L'ASA fournit une stratégie de groupe par défaut. Vous pouvez modifier cette stratégie de groupe par défaut, mais vous ne pouvez pas la supprimer. Une stratégie de groupe par défaut, nommée DfltGrpPolicy, existe toujours sur l'ASA, mais cette stratégie de groupe par défaut ne prend effet que si vous configurez l'ASA pour l'utiliser. Lorsque vous configurez d'autres stratégies de groupe, tout attribut que vous ne spécifiez pas explicitement hérite de sa valeur de la stratégie de groupe par défaut.

Remarque Les profils Secure Client (services client sécurisés), y compris tout ou tous les types de profils Secure Client (services client sécurisés) (comme Network Access Manager, Umbrella, etc.) configurés sur DfltGrpPolicy (et qui lui sont affectés) ne sont pas hérités par d'autres stratégies de groupe, sauf si les autres stratégies de groupe sont explicitement configurées pour hériter de DfltGrpPolicy. En d'autres termes, les profils Secure Client (services client sécurisés) associés à DfltGrpPolicy ne sont pas hérités lorsque des profils Secure Client (services client sécurisés) spécifiques sont configurés dans une stratégie de groupe.

Pour afficher la stratégie de groupe par défaut, saisissez la commande suivante :

```
hostname(config)# show running-config all group-policy DfltGrpPolicy
hostname(config)#
```

Pour configurer la stratégie de groupe par défaut, saisissez la commande suivante :

```
hostname(config)# group-policy DfltGrpPolicy internal
hostname(config)#
```

Remarque La stratégie de groupe par défaut est toujours interne. Malgré le fait que la syntaxe de la commande est hostname(config)# group-policy DfltGrpPolicy {internal | external}, vous ne pouvez pas modifier son type en externe.

Pour modifier l'un des attributs de la stratégie de groupe par défaut, utilisez la commande **group-policy attributes** pour passer en mode attributs, puis précisez les commandes pour modifier les attributs souhaités :

```
hostname(config)# group-policy DfltGrpPolicy attributes
```

Remarque Le mode d'attributs s'applique uniquement aux stratégies de groupe internes.

La stratégie de groupe par défaut, DfltGrpPolicy, que fournit l'ASA est la suivante :

```
hostname# show run all group-policy DfltGrpPolicy
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 wins-server none
 dns-server value 10.10.10.1.1
 dhcp-network-scope none
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-idle-timeout alert-interval 1
 vpn-session-timeout none
 vpn-session-timeout alert-interval 1
 vpn-filter none
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client

 password-storage disable
 ip-comp disable
 re-xauth disable
 group-lock none
 pfs disable
 ipsec-udp disable
 ipsec-udp-port 10000
 split-tunnel-policy tunnelall
 ipv6-split-tunnel-policy tunnelall
 split-tunnel-network-list none
 default-domain value cisco.com
 split-dns none
 split-tunnel-all-dns disable
 intercept-dhcp 255.255.255.255 disable
 secure-unit-authentication disable
 user-authentication disable
 user-authentication-idle-timeout 30
 ip-phone-bypass disable
 client-bypass-protocol disable
 gateway-fqdn none
 leap-bypass disable
 nem disable
 backup-servers keep-client-config
 msie-proxy server none
 msie-proxy method no-modify
```

```
 msie-proxy except-list none
 msie-proxy local-bypass disable
 msie-proxy pac-url none
 msie-proxy lockdown enable
 vlan none
 nac-settings none
 address-pools none
 ipv6-address-pools none
 smartcard-removal-disconnect enable
 scep-forwarding-url none
 client-firewall none
 client-access-rule none
 webvpn
  url-list none
  filter none
  homepage none
  html-content-filter none

  http-proxy disable

  anyconnect ssl dtls enable
  anyconnect mtu 1406
  anyconnect firewall-rule client-interface private none
  anyconnect firewall-rule client-interface public none
  anyconnect keep-installer installed
  anyconnect ssl keepalive 20
  anyconnect ssl rekey time none
  anyconnect ssl rekey method none
  anyconnect dpd-interval client 30
  anyconnect dpd-interval gateway 30
  anyconnect ssl compression none
  anyconnect dtls compression lzs
  anyconnect modules none
  anyconnect profiles none
  anyconnect ask none
  customization none
  keep-alive-ignore 4
  http-comp gzip
  download-max-size 2147483647
  upload-max-size 2147483647
  post-max-size 2147483647
  user-storage none
  storage-objects value cookies,credentials
  storage-key none
  hidden-shares none

  activex-relay enable
  unix-auth-uid 65534
  unix-auth-gid 65534
  file-entry enable
  file-browsing enable
  url-entry enable
  deny-message value Login was successful, but because certain criteria have not been met
or due to some specific group policy, you do not have permission to use any of the VPN
features. Contact your IT administrator for more information

  anyconnect ssl df-bit-ignore disable
  anyconnect routing-filtering-ignore disable

  always-on-vpn profile-setting
```

Vous pouvez modifier la stratégie de groupe par défaut et vous pouvez également créer une ou plusieurs stratégies de groupe spécifiques à votre environnement.

Configurer les stratégies de groupe

Une stratégie de groupe peut s'appliquer à tout type de tunnel. Dans chaque cas, si vous ne définissez pas explicitement de paramètre, le groupe prend la valeur de la stratégie de groupe par défaut.

Vous pouvez effectuer ces tâches de configuration en mode contexte unique ou en mode multi-contexte :

Remarque Le mode multi-contexte s'applique uniquement aux connexions site à site IKEv2 et IKEv1 et ne s'applique pas à AnyConnect, au VPN SSL sans client, au client VPN natif Apple, au client VPN natif Microsoft ou à cTCP pour IKEv1 IPsec.

Configurer une stratégie de groupe externe

Les stratégies de groupe externes tirent leurs valeurs d'attribut du serveur externe que vous spécifiez. Pour une stratégie de groupe externe, vous devez identifier le groupe de serveurs AAA que l'ASA peut interroger pour les attributs et préciser le mot de passe à utiliser lors de la récupération des attributs du groupe de serveurs AAA externe. Si vous utilisez un serveur d'authentification externe et si vos attributs de stratégie de groupe externes existent dans le même serveur RADIUS que les utilisateurs que vous prévoyez d'authentifier, vous devez vous assurer qu'il n'y a pas de duplication de nom entre eux.

Remarque Les noms de groupes externes sur l'ASA font référence aux noms d'utilisateur sur le serveur RADIUS. En d'autres termes, si vous configurez le groupe externe X sur l'ASA, le serveur RADIUS voit la requête comme une demande d'authentification pour l'utilisateur X. Ainsi, les groupes externes ne sont en fait que des comptes d'utilisateurs sur le serveur RADIUS qui ont une signification particulière pour l'ASA. Si vos attributs de groupe externe existent dans le même serveur RADIUS que les utilisateurs que vous prévoyez d'authentifier, il ne doit y avoir aucune duplication de nom entre eux.

L'ASA prend en charge l'autorisation utilisateur sur un serveur LDAP ou RADIUS externe. Avant de configurer l'ASA pour utiliser un serveur externe, vous devez configurer le serveur avec les attributs d'autorisation ASA appropriés et, à partir d'un sous-ensemble de ces attributs, attribuer des autorisations spécifiques aux utilisateurs individuels. Suivez les instructions dans Configurer un serveur AAA externe pour le VPN pour configurer votre serveur externe.

Procédure

Pour configurer une stratégie de groupe externe, effectuez l'étape suivante et spécifiez un nom et un type pour la stratégie de groupe, ainsi que le nom du groupe de serveurs et un mot de passe :

```
hostname(config)# group-policy group_policy_name type server-group server_group_name password
 server_password
hostname(config)#
```

Remarque
Pour une stratégie de groupe externe, RADIUS est le seul type de serveur AAA pris en charge.

Par exemple, la commande suivante crée une stratégie de groupe externe nommée ExtGroup qui obtient ses attributs d'un serveur RADIUS externe nommé ExtRAD et spécifie que le mot de passe à utiliser lors de la récupération des attributs est newpassword :

```
hostname(config)# group-policy ExtGroup external server-group ExtRAD password newpassword
hostname(config)#
```

Remarque
Vous pouvez configurer plusieurs attributs spécifiques au fournisseur (VSA), comme décrit dans Configurer un serveur AAA externe pour le VPN. Si un serveur RADIUS est configuré pour renvoyer l'attribut de classe (n° 25), l'ASA utilise cet attribut pour authentifier le nom de groupe. Sur le serveur RADIUS, l'attribut doit être formaté comme suit : OU=*groupname* ; où le *nom de groupe* est identique au nom de groupe configuré sur l'ASA — par exemple, OU=Finance.

Créer une stratégie de groupe interne

Pour configurer une stratégie de groupe interne, passez en mode de configuration, utilisez la commande group-policy, spécifiez un nom et le type **internal** pour la stratégie de groupe :

```
hostname(config)# group-policy group_policy_name internal
hostname(config)#
```

Par exemple, la commande suivante crée la stratégie de groupe interne nommée GroupPolicy1 :

```
hostname(config)# group-policy GroupPolicy1 internal
hostname(config)#
```

Remarque Vous ne pouvez pas modifier le nom d'une stratégie de groupe après sa création.

Vous pouvez configurer les attributs d'une stratégie de groupe interne en copiant les valeurs d'une stratégie de groupe préexistante, en ajoutant le mot-clé **from** et en précisant le nom de la stratégie existante :

```
hostname(config)# group-policy group_policy_name internal from group_policy_name
hostname(config-group-policy)#
```

Par exemple, la commande suivante crée la stratégie de groupe interne nommée GroupPolicy2 en copiant les attributs de GroupPolicy1 :

```
hostname(config)# group-policy GroupPolicy2 internal from GroupPolicy1
hostname(config-group-policy)#
```

Configurer les attributs généraux de la stratégie de groupe interne

Nom de la stratégie de groupe

Le nom de la stratégie de groupe a été choisi lors de la création de la stratégie de groupe interne. Vous ne pouvez pas modifier le nom d'une stratégie de groupe une fois qu'elle a été créée. Consultez Créer une stratégie de groupe interne, à la page 39 pour de plus amples renseignements.

Configurer la bannière de message de stratégie de groupe

Précisez la bannière ou le message de bienvenue, le cas échéant, que vous souhaitez afficher. La valeur par défaut est Sans bannière. Le message que vous spécifiez s'affiche sur les clients distants lorsqu'ils se connectent. Pour spécifier une bannière, saisissez la commande **banner** en mode de configuration de la stratégie de groupe. Le texte de la bannière peut comporter jusqu'à 500 caractères.

Remarque Assurez-vous d'utiliser des sauts de ligne normaux dans la boîte de dialogue de la bannière et non « \n ».

La longueur totale de la bannière, qui s'affiche après l'ouverture de session sur le client VPN distant, est passée de 510 à 4 000 caractères dans la version 9.5.1 de l'ASA.

Remarque Un retour chariot et un saut de ligne inclus dans la bannière comptent comme deux caractères.

Pour supprimer une bannière existante, utilisez la forme **no** de cette commande. Sachez que l'utilisation de la version **no** de la commande supprime toutes les bannières de la stratégie de groupe.

Une stratégie de groupe peut hériter de cette valeur d'une autre stratégie de groupe. Pour éviter d'hériter d'une valeur, saisissez le mot-clé **none** au lieu de spécifier une valeur pour la chaîne de bannière, comme suit :

```
hostname(config-group-policy)# banner {value banner_string | none}
```

L'exemple suivant montre comment créer une bannière pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems ASA 9.0.
```

Préciser les ensembles d'adresses pour les connexions d'accès à distance

Lorsque les clients d'accès à distance se connectent à l'ASA, celui-ci peut attribuer au client une adresse IPv4 ou IPv6 en fonction de la stratégie de groupe spécifiée pour la connexion.

Vous pouvez spécifier une liste de six ensembles d'adresses maximum à utiliser pour l'attribution d'adresses locales. L'ordre dans lequel vous spécifiez les ensembles est important. L'ASA attribue les adresses de ces ensembles d'adresses dans l'ordre dans lequel ces ensembles d'adresses apparaissent dans cette commande.

Attribuer un ensemble d'adresses IPv4 à une stratégie de groupe interne

Avant de commencer

Créez l'ensemble d'adresses IPv4.

Procédure

Étape 1 Entrez en mode de configuration de la stratégie de groupe.

group-policy *value* **attributes**

Exemple :

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

Étape 2 Attribuez l'ensemble d'adresses nommé ipv4-pool1, ipv4-pool2 et ipv4pool3 à la stratégie de groupe FirstGroup. Vous êtes autorisé à spécifier jusqu'à 6 ensembles d'adresses pour la stratégie de groupe.

address-pools value *pool-name1 pool-name2 pool-name6*

Exemple :

```
asa4(config-group-policy)# address-pools value ipv4-pool1 ipv4-pool2 ipv4-pool3
asa4(config-group-policy)#
```

Étape 3 (Facultatif) Utilisez la commande **no address-pools value pool-name** pour supprimer les ensembles d'adresses de la configuration de la stratégie de groupe et rétablir l'héritage des informations d'ensemble d'adresses à partir d'autres sources, telles que DfltGrpPolicy.

no address-pools value *pool-name1 pool-name2 pool-name6*

Exemple :

```
hostname(config-group-policy)# no address-pools value ipv4-pool1 ipv4-pool2 ipv4-pool3
hostname(config-group-policy)#
```

Étape 4 (Facultatif) La commande **address-pools none** désactive cet attribut afin qu'il ne soit pas hérité d'autres sources de politique, telles que DefltGrpPolicy.

```
hostname(config-group-policy)# address-pools none
hostname(config-group-policy)#
```

Étape 5 (Facultatif) La commande **no address pools none** supprime la commande **address-pools none** de la stratégie de groupe, en restaurant la valeur par défaut, qui est d'autoriser l'hérédité.

```
hostname(config-group-policy)# no address-pools none
```

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

Attribuer un ensemble d'adresses IPv6 à une stratégie de groupe interne

Avant de commencer

Créez l'ensemble d'adresses IPv6. Consultez Adresses IP pour les VPN.

Procédure

Étape 1 Entrez en mode de configuration de la stratégie de groupe.

group-policy *value* **attributes**

Exemple :

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

Étape 2 Attribuez l'ensemble d'adresses nommé ipv6-pool à la stratégie de groupe FirstGroup. Vous pouvez affecter jusqu'à six ensembles d'adresses IPv6 à une stratégie de groupe.

Exemple :

Cet exemple montre ipv6-pool1, ipv6-pool2 et ipv6-pool3 affectés à la stratégie de groupe FirstGroup.

```
hostname(config-group-policy)# ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3
hostname(config-group-policy)#
```

Étape 3 (Facultatif) Utilisez la commande **no ipv6-address-pools value pool-name** pour supprimer les ensembles d'adresses de la configuration de la stratégie de groupe et rétablir l'héritage des informations d'ensemble d'adresses à partir d'autres sources telles que DfltGroupPolicy.

no ipv6-address-pools value pool-name1 pool-name2 pool-name6

Exemple :

```
hostname(config-group-policy)# no ipv6-address-pools value ipv6-pool1 ipv6-pool2 ipv6-pool3
hostname(config-group-policy)#
```

Étape 4 (Facultatif) Utilisez la commande **ipv6-address-pools none** pour désactiver cet attribut afin qu'il ne soit pas hérité d'autres sources de politique, telles que DfltGrpPolicy.

```
hostname(config-group-policy)# ipv6-address-pools none
hostname(config-group-policy)#
```

Étape 5 (Facultatif) Utilisez la commande **no ipv6-address pools none** pour supprimer la commande **ipv6-address-pools none** de la stratégie de groupe et rétablir la valeur par défaut, qui est d'autoriser l'héritage.

```
hostname(config-group-policy)# no ipv6-address-pools none
hostname(config-group-policy)#
```

Préciser le protocole de tunnelisation pour la stratégie de groupe

Précisez le type de tunnel VPN pour cette stratégie de groupe en saisissant la commande **vpn-tunnel-protocol**{ IKEv1 | IKEv2 | l2tp-ipsec | ssl-client} en mode de configuration de stratégie de groupe.

La valeur par défaut consiste à hériter des attributs de la stratégie de groupe par défaut. Pour supprimer l'attribut de la configuration en cours d'exécution, saisissez la forme **no** de cette commande.

Les valeurs des paramètres pour cette commande sont les suivantes :

- IKEv1 : négocie un tunnel IPsec IKEv1 entre deux homologues (le client VPN Cisco ou une autre passerelle sécurisée). Crée des associations de sécurité qui régissent l'authentification, le chiffrement, l'encapsulation et la gestion des clés.
- IKEv2 : négocie un tunnel IPsec IKEv2 entre deux homologues (Secure Client (services client sécurisés) ou une autre passerelle sécurisée). Crée des associations de sécurité qui régissent l'authentification, le chiffrement, l'encapsulation et la gestion des clés.
- **l2tp-ipsec** : négocie un tunnel IPsec pour une connexion L2TP.
- ssl-client : négocie un tunnel SSL en utilisant TLS ou DTLS avec Secure Client (services client sécurisés).

Entrez cette commande pour configurer un ou plusieurs modes de tunnellisation. Au moins un mode de tunnellisation doit être configuré pour que les utilisateurs puissent se connecter sur un tunnel VPN.

L'exemple suivant montre comment configurer le mode de tunnellisation IPsec IKEv1 pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol ikev1
hostname(config-group-policy)#
```

Préciser un réseau VLAN pour l'accès à distance ou appliquer une règle de contrôle d'accès unifiée à la stratégie de groupe

Les filtres consistent en des règles qui déterminent s'il faut autoriser ou rejeter les paquets de données tunnellisés en fonction de critères comme l'adresse source, l'adresse de destination et le protocole. Vous pouvez spécifier une liste de contrôle d'accès unifiée IPv4 ou IPv6 pour votre stratégie de groupe ou lui permettre d'hériter des listes de contrôle d'accès spécifiées dans la stratégie de groupe par défaut.

Choisissez l'une des options suivantes pour spécifier un VLAN de sortie (également appelé « mappage VLAN ») pour l'accès à distance ou spécifier une liste de contrôle d'accès pour filtrer le trafic :

Remarque Lors du mappage du VLAN avec IPv6, l'adresse externe (destination) doit être unique pour chacun des VLAN afin que le trafic déchiffré soit acheminé vers les réseaux internes. Vous ne pouvez pas avoir le même réseau de destination avec des VLAN et des mesures de routage différents.

- Entrez la commande suivante en mode de configuration de stratégie de groupe pour préciser le VLAN de sortie pour les sessions VPN d'accès à distance attribuées à cette stratégie de groupe ou à une stratégie de groupe qui hérite de cette stratégie de groupe :

  [**no**] **vlan** {*vlan_id* |**none**}

  no vlan supprime *vlan_id* de la stratégie de groupe. La stratégie de groupe hérite de la valeur vlan de la stratégie de groupe par défaut.

  none supprime *vlan_id* de la stratégie de groupe et désactive le mappage VLAN pour cette stratégie de groupe. La stratégie de groupe n'hérite pas de la valeur vlan de la stratégie de groupe par défaut.

  vlan_id est le numéro de VLAN, au format décimal, à affecter aux sessions VPN d'accès à distance qui utilisent cette stratégie de groupe. Le VLAN doit être configuré sur cet ASA conformément aux instructions de la section « Configuration des sous-interfaces VLAN et de la liaison 802.1Q » dans le guide de configuration des opérations générales.

Remarque Pour les connexions VPN sans client, la fonctionnalité VLAN de sortie fonctionne uniquement pour le protocole HTTP.

- Précisez le nom de la règle de contrôle d'accès (ACL) à appliquer à la session VPN en utilisant la commande **vpn-filter** en mode de stratégie de groupe. Vous pouvez spécifier une liste de contrôle d'accès IPv4 ou IPv6 à l'aide de la commande vpn-filter.

Remarque Vous pouvez également configurer cet attribut en mode nom d'utilisateur, auquel cas la valeur configurée sous nom d'utilisateur remplace la valeur de stratégie de groupe.

```
hostname(config-group-policy)# vpn-filter {value ACL name | none}
hostname(config-group-policy)#
```

Vous configurez les listes de contrôle d'accès pour autoriser ou refuser différents types de trafic pour cette stratégie de groupe. Vous saisissez ensuite la commande **vpn-filter** pour appliquer ces listes de contrôle d'accès.

Pour supprimer la liste de contrôle d'accès, y compris une valeur nulle créée en entrant la commande **vpn-filter none**, saisissez la forme **no** de cette commande. L'option **no** permet l'hérédité d'une valeur d'une autre stratégie de groupe.

Une stratégie de groupe peut hériter de cette valeur d'une autre stratégie de groupe. Pour éviter d'hériter d'une valeur, saisissez le mot-clé **none** au lieu de spécifier un nom d'ACL. Le mot-clé **none** indique qu'il n'y a pas d'ACL et définit une valeur nulle, interdisant ainsi une ACL.

L'exemple suivant montre comment définir un filtre qui invoque une liste de contrôle d'accès nommée acl_vpn pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter acl_vpn
hostname(config-group-policy)#
```

La commande **vpn-filter** s'applique au trafic post-déchiffré après sa sortie du tunnel et au trafic préchiffré avant son entrée dans le tunnel. Une liste de contrôle d'accès utilisée pour un vpn-filter ne doit pas également être utilisée pour un access-group d'interface. Lorsqu'une commande **vpn-filter** est appliquée à une stratégie de groupe qui régit les connexions des clients VPN d'accès à distance, l'ACL doit être configurée avec les adresses IP attribuées au client dans la position **src_ip** de l'ACL et le réseau local dans la position **dest_ip** de l'ACL.

Lorsqu'une commande **vpn-filter** est appliquée à une stratégie de groupe qui régit une connexion LAN à LAN, l'ACL doit être configurée avec le réseau distant dans la position **src_ip** de l'ACL et le réseau local dans la position **dest_ip** de l'ACL.

La prudence doit être utilisée lors de la construction des listes de contrôle d'accès à utiliser avec la fonctionnalité vpn-filter. Les listes de contrôle d'accès sont bâties en gardant à l'esprit le trafic post-déchiffré. Cependant, les listes de contrôle d'accès sont également appliquées au trafic dans le sens opposé. Pour ce trafic préchiffré qui est destiné au tunnel, les listes de contrôle d'accès sont bâties avec les positions **src_ip** et **dest_ip** permutées.

Notez que le filtre VPN s'applique aux connexions initiales uniquement. Il ne s'applique pas aux connexions secondaires, comme une connexion de support SIP, qui sont ouvertes en raison de l'action de l'inspection d'application.

Dans l'exemple suivant : le vpn-filter est utilisé avec un client VPN d'accès à distance. Cet exemple suppose que l'adresse IP attribuée au client est 10.10.10.1/24 et que le réseau local est 192.168.1.0/24.

L'ACE suivant permet au client VPN d'accès à distance d'établir une connexion Telnet vers le réseau local :

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255
192.168.1.0 255.255.255.0 eq 23
```

L'ACE suivant permet au réseau local d'établir une connexion Telnet vers le client d'accès à distance :

```
hostname(config-group-policy)# access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq
 23 192.168.1.0 255.255.255.0
```

Remarque L'ACE **access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23** permet au réseau local d'établir une connexion avec le client d'accès à distance sur n'importe quel port TCP s'il utilise un port source de 23. L'ACE **access-list vpnfilt-ra permit 10.10.10.1 255.255.255.255 eq 23 192.168.1.0 255.255.255.0** permet au client d'accès à distance d'établir une connexion au réseau local sur n'importe quel port TCP s'il utilise un port source de 23.

Dans l'exemple suivant, le vpn-filter est utilisé avec une connexion VPN de site à site. Cet exemple suppose que le réseau distant est 10.0.0.0/24 et que le réseau local est 192.168.1.0/24. L'ACE suivant permet au réseau distant de communiquer avec le réseau local :

```
hostname(config-group-policy)# access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0
192.168.1.0 255.255.255.0 eq 23
```

L'ACE suivant permet au réseau local d'établir une connexion Telnet vers le réseau distant :

```
hostname(config-group-policy)# access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 eq 23
 192.168.1.0 255.255.255.0
```

Remarque L'ACE **access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 192.168.1.0 255.255.255.0 eq 23** permet au réseau local d'établir une connexion avec le réseau distant sur n'importe quel port TCP s'il utilise un port source de 23. L'ACE **access-list vpnfilt-l2l permit 10.0.0.0 255.255.255.0 eq 23 192.168.1.0 255.255.255.0** permet au réseau distant d'établir une connexion avec le réseau local sur n'importe quel port TCP s'il utilise un port source de 23.

Préciser les heures d'accès au VPN pour une stratégie de groupe

Avant de commencer

Créer une plage horaire Consultez le guide de configuration sur les opérations générales ASA pour plus d'informations.

Procédure

Étape 1 Entrez en mode de configuration de la stratégie de groupe.

group-policy *value* **attributes**

Exemple :

```
hostname> en
hostname# config t
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

Étape 2 Vous pouvez définir les heures d'accès VPN en associant une politique de plage temporelle configurée à une stratégie de groupe à l'aide de la commande **vpn-access-hours** en mode de configuration de stratégie de groupe. Cette commande attribue une plage horaire d'accès VPN nommée heures de travail à la stratégie de groupe nommée FirstGroup.

Une stratégie de groupe peut hériter d'une valeur de plage temporelle d'une stratégie de groupe par défaut ou d'une stratégie de groupe spécifiée. Pour éviter cet héritage, saisissez le mot-clé **none** au lieu du nom d'une plage temporelle dans cette commande. Ce mot-clé définit les heures d'accès VPN à une valeur nulle, ce qui n'autorise aucune politique de plage temporelle.

vpn-access-hours value {*time-range-name* | **none**}

Exemple :

```
hostname(config-group-policy)# vpn-access-hours value business-hours
hostname(config-group-policy)#
```

Préciser les connexions VPN simultanées pour une stratégie de groupe

Vous pouvez définir une limite au nombre de sessions simultanées qu'un utilisateur donné peut maintenir pour une stratégie de groupe. La valeur par défaut est de 3 sessions simultanées.

Les sessions périmées Secure Client (services client sécurisés), client IPsec ou sans client (sessions terminées de manière anormale) peuvent rester dans la base de données des sessions, même si une « nouvelle » session a été établie avec le même nom d'utilisateur.

Si le nombre autorisé de sessions simultanées est de 1 et que le même utilisateur se connecte à nouveau après une interruption anormale, la session périmée est supprimée de la base de données et une nouvelle session est établie. Si, toutefois, la session existante est toujours une connexion active et que le même utilisateur se connecte à nouveau, peut-être à partir d'un autre ordinateur, la première session est déconnectée et supprimée de la base de données, et une nouvelle session est établie.

Si le nombre de sessions simultanées autorisées est supérieur à 1, puis, lorsque l'utilisateur a atteint ce nombre maximal et tente de se connecter à nouveau, la session avec le temps d'inactivité le plus long est déconnectée. Si toutes les sessions actuelles sont inactives depuis une durée égale, la session la plus ancienne est déconnectée. Cette action libère une session et permet la nouvelle connexion.

Une fois que la limite maximale de sessions est atteinte, il faut un certain temps au système pour supprimer la session la plus ancienne. Ainsi, un utilisateur pourrait ne pas être en mesure de se connecter immédiatement et pourrait devoir réessayer la nouvelle connexion avant qu'elle ne se termine avec succès. Cela ne devrait pas être un problème si les utilisateurs déconnectent leurs sessions comme prévu. Vous pouvez éventuellement supprimer le retard en configurant le système pour ne pas attendre que la suppression soit terminée et autoriser immédiatement la connexion du nouvel utilisateur.

Procédure

	Commande ou action	Objectif

Étape 1	Précisez le nombre de connexions simultanées autorisées pour un utilisateur, à l'aide de la commande **vpn-simultaneous-logins** *nombre entier* en mode de configuration de stratégie de groupe.	**vpn-simultaneous-logins** *integer*
		La valeur par défaut est 3. La plage est un nombre entier compris entre 0 et 2147483647. Une stratégie de groupe peut hériter de cette valeur d'une autre stratégie de groupe. Saisissez 0 pour désactiver la connexion et empêcher l'accès de l'utilisateur. L'exemple suivant montre comment autoriser un maximum de 4 connexions simultanées pour la stratégie de groupe nommée FirstGroup :
		`hostname(config)# group-policy FirstGroup attributes`
		`hostname(config-group-policy)# vpn-simultaneous-logins 4`
		Remarque

	Commande ou action	Objectif
		• Bien que la limite maximale du nombre de connexions simultanées soit très élevée, autoriser plusieurs connexions simultanées peut compromettre la sécurité et affecter les performances. • Lorsque vous vous connectez à différents groupes de tunnels avec des stratégies de groupe différentes, **vpn-simultaneous-logins** supprime les sessions d'utilisateur même si les sessions existantes utilisent une stratégie de groupe différente.

Étape 2	(Facultatif) Lorsque la limite de connexions simultanées est atteinte, configurez le système pour établir de nouvelles sessions sans attendre que la session la plus ancienne soit supprimée.	**vpn-simultaneous-login-delete-no-delay**
		Cette option est désactivée par défaut.
		`hostname(config)# group-policy FirstGroup attributes`
		`hostname(config-group-policy)# vpn-simultaneous-login-delete-no-delay`

Restreindre l'accès à un profil de connexion précis

Précisez s'il faut restreindre les utilisateurs distants afin qu'ils accèdent uniquement par le profil de connexion, à l'aide de la commande **group-lock** en mode de configuration group-policy.

```
hostname(config-group-policy)# group-lock {value tunnel-grp-name | none}
hostname(config-group-policy)# no group-lock
hostname(config-group-policy)#
```

La variable *tunnel-grp-name* précise le nom d'un profil de connexion existant que l'ASA exige pour que l'utilisateur puisse se connecter. Le verrouillage de groupe restreint les utilisateurs en vérifiant si le groupe configuré dans le client VPN est le même que le profil de connexion auquel l'utilisateur est affecté. Si ce n'est pas le cas, l'ASA empêche l'utilisateur de se connecter. Si vous ne configurez pas group-lock, l'ASA authentifie les utilisateurs sans tenir compte du groupe attribué. Le verrouillage de groupe est désactivé par défaut.

Pour supprimer l'attribut **group-lock** de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cette option permet d'hériter d'une valeur provenant d'une autre stratégie de groupe.

Pour désactiver le verrouillage de groupe, saisissez la commande **group-lock** avec le mot-clé **none**. Le mot-clé none définit group-lock à une valeur nulle, de sorte qu'aucune restriction de verrouillage de groupe n'est appliquée. Cela empêche également d'hériter d'une valeur de verrouillage de groupe d'une stratégie de groupe par défaut ou précisée.

Préciser le délai de connexion VPN maximal dans une stratégie de groupe

Procédure

Étape 1 (Facultatif) Configurez une durée maximale pour les connexions VPN en utilisant la commande **vpn-session-timeout** {*minutes* dans le mode de configuration de stratégie de groupe ou dans le mode de configuration du nom d'utilisateur.

La durée minimale est de 1 minute et la durée maximale est de 35 791 394 minutes. Il n'y a pas de valeur par défaut. À la fin de cette période, l'ASA met fin à la connexion.

L'exemple suivant montre comment définir un délai d'expiration de session VPN de 180 minutes pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

L'exemple suivant montre comment définir un délai d'expiration de session VPN de 180 minutes pour l'utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-session-timeout 180
hostname(config-username)#
```

Autres actions utilisant la commande [**no**] **vpn-session-timeout** {*minutes* | **none**} :

- Pour supprimer l'attribut de cette stratégie et autoriser l'héritage, saisissez la forme **no vpn-session-timeout** de cette commande.
- Pour autoriser un délai d'expiration illimité et ainsi empêcher l'héritage d'une valeur de délai d'expiration, saisissez **vpn-session-timeout none**.

Étape 2 Configurez le moment où un message d'alerte d'expiration de session s'affiche à l'utilisateur au moyen de la commande **vpn-session-timeout alert-interval** {*minutes* | } .

Ce message d'alerte indique aux utilisateurs le nombre de minutes restantes avant la déconnexion automatique de leur session VPN. L'exemple suivant montre comment spécifier que les utilisateurs seront informés 20 minutes avant la déconnexion de leur session VPN. Vous pouvez spécifier une plage de 1 à 30 minutes.

```
hostname(config-webvpn)# vpn-session-timeout alert-interval 20
```

Autres actions utilisant la commande [**no**] **vpn-session-timeout alert-interval** {*minutes* | **none**} :

- Utilisez la forme no de la commande pour indiquer que l'attribut d'intervalle d'alerte du délai d'expiration de la session VPN sera hérité de la stratégie de groupe par défaut :

  ```
  hostname(config-webvpn)# no vpn-session-timeout alert-interval
  ```

- Le **vpn-session-timeout alert-interval none** indique que les utilisateurs ne recevront pas d'alerte.

Préciser un délai d'inactivité de session VPN pour une stratégie de groupe

Procédure

Étape 1 (Facultatif) Pour configurer un délai d'inactivité du VPN, utilisez la commande **vpn-idle-timeout** *minutes* en mode de configuration de stratégie de groupe ou en mode de configuration de nom d'utilisateur.

S'il n'y a aucune activité de communication sur la connexion pendant cette période, l'ASA arrête la connexion. La durée minimale est de 1 minute, la durée maximale est de 35 791 394 minutes et la valeur par défaut est de 30 minutes.

L'exemple suivant montre comment définir un délai d'inactivité VPN de 15 minutes pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
hostname(config-group-policy)#
```

Autres actions utilisant la commande [**no**] **vpn-idle-timeout** {*minutes* | **none**} :

- Saisissez **vpn-idle-timeout none** pour désactiver le délai d'inactivité du VPN et empêcher l'héritage d'une valeur de délai d'expiration.

  ```
  hostname(config)# group-policy FirstGroup attributes
  hostname(config-group-policy)# vpn-idle-timeout none
  hostname(config-group-policy)#
  ```

  Il en résulte Secure Client (services client sécurisés) (SSL et IPsec/IKEv2) et un VPN sans client utilisant la valeur globale **default-idle-timeout** *secondes* webvpn. Cette commande est saisie en mode webvpn-config, par exemple : `hostnamee(config-webvpn)# default-idle-timeout 300`. La valeur par défaut est de 1800 secondes (30 min), la plage est comprise entre 60 et 86400 secondes.

  Pour toutes les connexions webvpn, la valeur **default-idle-timeout** est appliquée uniquement si **vpn-idle-timeout none** est défini dans l'attribut de stratégie de groupe/de nom d'utilisateur. Une valeur de délai d'inactivité non nulle est requise par l'ASA pour toutes les connexions Secure Client (services client sécurisés).

  Pour les VPN de site à site (IKEv1, IKEv2) et VPN d'accès à distance IKEv1, nous vous recommandons de désactiver le délai d'expiration et d'autoriser une période d'inactivité illimitée.

- Pour désactiver le délai d'inactivité pour cette stratégie de groupe ou cette politique d'utilisateur, saisissez **no vpn-idle-timeout**. La valeur sera héritée.
- Si vous ne définissez pas du tout **vpn-idle-timeout**, de toute façon, la valeur est héritée, qui est par défaut de 30 minutes.

Remarque
vpn-idle-timeout contrôle uniquement la durée maximale d'une session parente. Les sessions enfants (SSL/DTLS) sont terminées de manière dynamique beaucoup plus tôt par un délai d'inactivité TCP de 5 minutes codé en dur ou en cas d'échec de la vérification Dead Peer Detection (DPD) (3 tentatives). Pour plus de détails, consultez la note dans Configurer la détection d'homologue mort. Pour plus de détails sur les attributs DPD, keepalive et de temporisation, consultez Answer AnyConnect FAQ - Tunnels, DPD et minuterie d'inactivité.

Étape 2 (Facultatif) Vous pouvez éventuellement configurer l'heure à laquelle un message d'alerte de délai d'inactivité s'affiche à l'utilisateur à l'aide de la commande **vpn-idle-timeout alert-interval** {*minutes*} .

Ce message d'alerte indique aux utilisateurs le nombre de minutes qu'il leur reste jusqu'à ce que leur session VPN soit déconnectée pour cause d'inactivité. L'intervalle d'alerte par défaut est d'une minute.

L'exemple suivant montre comment définir un intervalle d'alerte de délai d'inactivité du VPN de 3 minutes pour l'utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout alert-interval 3
hostname(config-username)#
```

Autres actions utilisant la commande [**no**] **vpn-idle-timeout alert-interval** {*minutes* | **none**} :

- Le paramètre **none** indique que les utilisateurs ne recevront pas d'alerte.

  ```
  hostname(config)# username anyuser attributes
  hostname(config-username)# vpn-idle-timeout none
  hostname(config-username)#
  ```

- Pour supprimer l'intervalle d'alerte de cette stratégie de groupe ou d'utilisateur, saisissez **no vpn-idle-timeout alert-interval**. La valeur sera héritée.
- Si vous ne définissez pas ce paramètre du tout, l'intervalle d'alerte par défaut est d'une minute.

Configurer les serveurs WINS et DNS pour une stratégie de groupe

Vous pouvez spécifier des serveurs WINS et des serveurs DNS principaux et secondaires. La valeur par défaut dans chaque cas est aucune. Pour spécifier ces serveurs, procédez comme suit :

Procédure

Étape 1 Précisez les serveurs WINS principal et secondaire :

```
hostname(config-group-policy)# wins-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

La première adresse IP spécifiée est celle du serveur WINS principal. La deuxième adresse IP (facultative) est celle du serveur WINS secondaire. La spécification du mot-clé **none** au lieu d'une adresse IP définit les serveurs WINS à une valeur nulle, ce qui n'autorise aucun serveur WINS et empêche d'hériter d'une valeur d'une stratégie de groupe par défaut ou d'une stratégie de groupe spécifiée.

Chaque fois que vous saisissez la commande **wins-server**, vous remplacez le paramètre existant. Par exemple, si vous configurez le serveur WINS x.x.x.x, puis le serveur WINS y.y.y.y, la deuxième commande remplace la première, et y.y.y.y devient le seul serveur WINS. La même chose est vraie pour plusieurs serveurs. Pour ajouter un serveur WINS plutôt que de remplacer les serveurs précédemment configurés, incluez les adresses IP de tous les serveurs WINS lorsque vous entrez cette commande.

L'exemple suivant montre comment configurer les serveurs WINS avec les adresses IP 10.10.10.15 et 10.10.10.30 pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30
hostname(config-group-policy)#
```

Étape 2 Précisez les serveurs DNS principal et secondaire :

```
hostname(config-group-policy)# dns-server value {ip_address [ip_address] | none}
hostname(config-group-policy)#
```

La première adresse IP spécifiée est celle du serveur DNS principal. La deuxième adresse IP (facultative) est celle du serveur DNS secondaire. La spécification du mot-clé **none** au lieu d'une adresse IP définit les serveurs DNS à une valeur nulle, ce qui n'autorise aucun serveur DNS et empêche d'hériter d'une valeur d'une politique par défaut ou d'un groupe spécifié. Vous pouvez spécifier jusqu'à quatre adresses de serveur DNS : jusqu'à deux adresses IPv4 et deux adresses IPv6.

Chaque fois que vous saisissez la commande **dns-server**, vous remplacez le paramètre existant. Par exemple, si vous configurez le serveur DNS x.x.x.x, puis le serveur DNS y.y.y.y, la deuxième commande remplace la première, et y.y.y.y devient le seul serveur DNS. La même chose est vraie pour plusieurs serveurs. Pour ajouter un serveur DNS plutôt que de remplacer les serveurs précédemment configurés, incluez les adresses IP de tous les serveurs DNS lorsque vous entrez cette commande.

L'exemple suivant montre comment configurer les serveurs DNS avec les adresses IP 10.10.10.15, 10.10.10.30, 2001:DB8::1 et 2001:DB8::2 pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dns-server value 10.10.10.15 10.10.10.30
2001:DB8::1 2001:DB8::2
hostname(config-group-policy)#
```

Étape 3 Si aucun nom de domaine par défaut n'est spécifié dans le groupe de serveurs **DNS DefaultDNS**, vous devez spécifier un domaine par défaut. Utilisez le nom de domaine et le domaine de premier niveau, par exemple **example.com**.

```
asa4(config)# group-policy FirstGroup attributes
asa4(config-group-policy)# default-domain value example.com
asa4(config-group-policy)#
```

Étape 4 (Facultatif) Configurez la portée du réseau DHCP :

dhcp-network-scope {*ip_address* | **none**}

Si vous configurez des serveurs DHCP pour l'ensemble d'adresses dans le profil de connexion, la portée de DHCP identifie les sous-réseaux à utiliser pour le regroupement pour ce groupe. Le serveur DHCP doit également avoir des adresses dans le même sous-réseau identifié par la portée. La portée vous permet de sélectionner un sous-ensemble des ensembles d'adresses définis dans le serveur DHCP à utiliser pour ce groupe précis.

Si vous ne définissez pas de portée réseau, le serveur DHCP attribue les adresses IP dans l'ordre des ensembles d'adresses configurés. Il parcourt les ensembles jusqu'à ce qu'il identifie une adresse non attribuée.

Pour spécifier une portée, saisissez une adresse routable sur le même sous-réseau que l'ensemble souhaité, mais en dehors de cet ensemble. Le serveur DHCP détermine à quel sous-réseau cette adresse IP appartient et attribue une adresse IP de cet ensemble d'adresses.

Nous vous recommandons d'utiliser l'adresse IP d'une interface chaque fois que cela est possible à des fins de routage. Par exemple, si l'ensemble d'adresses est 10.100.10.2-10.100.10.254 et que l'adresse d'interface est 10.100.10.1/24, utilisez 10.100.10.1 comme portée DHCP. N'utilisez pas le numéro de réseau. Vous ne pouvez utiliser DHCP que pour l'adressage IPv4. Si l'adresse que vous choisissez n'est pas une adresse d'interface, vous devrez peut-être créer une voie de routage statique pour l'adresse de portée.

La spécification de **none** empêche l'affectation d'adresses DHCP, par exemple, à partir d'une stratégie de groupe par défaut ou d'un système hérité.

Exemple :

L'exemple suivant passe en mode de configuration d'attributs pour FirstGroup et définit la portée DHCP à 10.100.10.1.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.100.10.1
```

Définir la politique de tunnellisation fractionnée

Définissez les règles de tunnellisation du trafic en précisant la politique de tunnellisation fractionnée pour le trafic IPv4 :

split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

no split-tunnel-policy

Définissez les règles de tunnellisation du trafic en précisant la politique de tunnellisation fractionnée pour le trafic IPv6 :

ipv6-split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

no ipv6-split-tunnel-policy

Les options de politique sont les suivantes :

- **tunnelspecified** : tunnelise tout le trafic vers ou depuis les réseaux précisés dans la liste de réseaux à travers le tunnel. Les données destinées à toutes les autres adresses circulent en clair et sont acheminées par le fournisseur de services Internet de l'utilisateur distant.

  Pour les versions de l'ASA 9.1.4 et ultérieures, lorsque vous précisez une liste d'inclusion, vous pouvez également préciser une liste d'exclusion pour un sous-réseau situé dans la plage d'inclusion. Les adresses du sous-réseau exclu ne seront pas tunnelisées, mais le reste de la liste d'inclusion le sera. Les réseaux dans la liste d'exclusion ne seront pas envoyés sur le tunnel. La liste d'exclusion est précisée à l'aide d'entrées deny, et la liste d'inclusion à l'aide d'entrées permit.

- **excludespecified** : ne tunnelise pas le trafic vers ou depuis les réseaux précisés dans la liste de réseaux. Le trafic de ou vers toutes les autres adresses est tunnelisé. . Le profil du client VPN actif sur le client doit avoir l'option Local LAN Access activée. Cette option fonctionne uniquement avec les Secure Client (services client sécurisés).

Remarque Les réseaux dans la liste d'exclusion qui ne sont pas un sous-ensemble de la liste d'inclusion sont ignorés par le client.

- **tunnelall —**Précise que tout le trafic passe par le tunnel. Cette politique désactive la tunnellisation fractionnée. Les utilisateurs distants ont accès au réseau de l'entreprise, mais ils n'ont pas accès aux réseaux locaux. Il s'agit de l'option par défaut.

Remarque La 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.

Exemple

L'exemple suivant montre comment définir, pour la stratégie de groupe nommée FirstGroup, une politique de tunnellisation fractionnée limitant le tunnel aux seuls réseaux spécifiés pour IPv4 et IPv6 :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified

hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
```

Préciser une liste de réseaux pour la tunnellisation fractionnée

Dans la tunnellisation fractionnée, les listes de réseau déterminent quel trafic réseau passe par le tunnel. Secure Client (services client sécurisés) prend les décisions de tunnellisation fractionnée en fonction d'une liste de réseaux, qui est une ACL.

```
hostname(config-group-policy)# split-tunnel-network-list {value access-list_name | none}
hostname(config-group-policy)# no split-tunnel-network-list value [access-list_name]
```

- **value** nom de liste d'accès : identifie une ACL qui énumère les réseaux à tunneliser ou à ne pas tunneliser. L'ACL peut être une ACL unifiée avec des ACE qui précisent à la fois des adresses IPv4 et IPv6.
- **none** : indique qu'il n'y a pas de liste de réseaux pour la tunnelisation fractionnée ; l'ASA tunnelise tout le trafic. Le fait de préciser le mot-clé **none** définit une liste de réseaux de tunnellisation fractionnée avec une valeur nulle, ce qui interdit la tunnellisation fractionnée. Cela empêche également l'héritage d'une liste de réseaux de tunnellisation fractionnée par défaut à partir d'une stratégie de groupe par défaut ou précisée.

Pour supprimer une liste de réseaux, saisissez la forme **no** de cette commande. Pour supprimer toutes les listes de réseaux de tunnellisation fractionnée, entrez la commande **no split-tunnel-network-list** sans arguments. Cette commande supprime toutes les listes de réseaux configurées, y compris une liste nulle si vous en avez créé une en saisissant le mot-clé **none**.

Lorsqu'il n'y a aucune liste de réseaux de tunnellisation fractionnée, les utilisateurs héritent de toute liste de réseaux présente dans la stratégie de groupe par défaut ou précisée. Pour empêcher les utilisateurs d'hériter de telles listes de réseaux, saisissez la commande **split-tunnel-network-list none**.

Exemple

L'exemple suivant montre comment créer une liste de réseaux nommée FirstList et l'ajouter à la stratégie de groupe nommée FirstGroup. FirstList est une liste d'exclusion et une liste d'inclusion qui est un sous-réseau de la liste d'exclusion :

```
hostname(config)# split-tunnel-policy tunnelspecified
hostname(config)# access-list FirstList deny ip 10.10.10.0 255.255.255.0 any
hostname(config)# access-list FirstList permit ip 10.0.0.0 255.0.0.0 any

hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list value FirstList
```

L'exemple suivant montre comment créer une liste de réseaux nommée v6 et ajouter la politique de tunnellisation fractionnée v6 à la stratégie de groupe nommée GroupPolicy_ipv6-ikev2. v6 est une liste d'exclusion et une liste d'inclusion qui est un sous-réseau de la liste d'exclusion :

```
hostname(config)# access-list v6 extended permit ip fd90:5000::/32 any6
hostname(config)# access-list v6 extended deny ip fd90:5000:3000:2880::/64 any6

hostname(config)# group-policy GroupPolicy_ipv6-ikev2 internal
hostname(config)# group-policy GroupPolicy_ipv6-ikev2 attributes
hostname(config-group-policy)# vpn-tunnel-protocol ikev2 ssl-client
hostname(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
hostname(config-group-policy)# split-tunnel-network-list value v6
```

Vérifier la configuration de la tunnellisation fractionnée

Exécutez la commande **show runn group-policy attributes** pour vérifier votre configuration. Cet exemple montre que l'administrateur a défini à la fois une politique réseau IPv4 et une politique réseau IPv6, et a utilisé la liste de réseaux (ACL unifiée), **FirstList** pour les deux politiques.

```
hostname(config-group-policy)# show runn group-policy FirstGroup attributes
group-policy FirstGroup attributes
 split-tunnel-policy tunnelspecified
 ipv6-split-tunnel-policy tunnelspecified
 split-tunnel-network-list value FirstList
```

Configurer les attributs de domaine pour la tunnellisation fractionnée

Vous pouvez préciser un nom de domaine par défaut ou une liste de domaines à résoudre au moyen du tunnel fractionné, ce que nous appelons DNS fractionné.

AnyConnect 3.1 prend en charge la véritable fonctionnalité DNS fractionné pour les plateformes Windows et Mac OS X. Si la stratégie de groupe sur l'appareil de sécurité active la tunnelisation fractionnée split-include et précise les noms DNS à tunneliser, AnyConnect tunnelise vers le serveur DNS privé toutes les requêtes DNS qui correspondent à ces noms. Le véritable DNS fractionné permet l'accès par tunnel uniquement aux requêtes DNS correspondant aux domaines transmis au client par l'ASA. Ces demandes ne sont pas envoyées en clair. D'un autre côté, si les requêtes DNS ne correspondent pas aux domaines transmis par l'ASA,

AnyConnect permet au résolveur DNS du système d'exploitation client de soumettre le nom d'hôte en clair pour résolution DNS.

Remarque Le DNS fractionné prend en charge les requêtes standard et les mises à jour (y compris A, AAAA, NS, TXT, MX, SOA, ANY, SRV, PTR et CNAME). Les requêtes PTR correspondant à l'un des réseaux tunnelisés sont autorisées dans le tunnel.

Pour Mac OS X, AnyConnect ne peut utiliser le véritable DNS fractionné pour un protocole IP donné que si l'une des conditions suivantes est remplie :

- Le DNS fractionné est configuré pour un protocole IP, comme IPv4, et Client Bypass Protocol est configuré pour l'autre protocole IP, comme IPv6, dans la stratégie de groupe, sans ensemble d'adresses configuré pour ce dernier protocole IP.
- Le DNS fractionné est configuré pour les deux protocoles IP.

Définition d'un nom de domaine par défaut

L'ASA transmet le nom de domaine par défaut à Secure Client (services client sécurisés). Le client ajoute le nom de domaine aux requêtes DNS qui omettent le champ de domaine. Ce nom de domaine s'applique uniquement aux paquets tunnelisés. Lorsqu'il n'y a pas de nom de domaine par défaut, les utilisateurs héritent du nom de domaine par défaut dans la stratégie de groupe par défaut.

Pour spécifier le nom de domaine par défaut pour les utilisateurs de la stratégie de groupe, entrez la commande **default-domain** en mode de configuration de stratégie de groupe. Pour supprimer un nom de domaine, saisissez la forme **no** de cette commande.

```
hostname(config-group-policy)# default-domain {value domain-name | none}
hostname(config-group-policy)# no default-domain [domain-name]
```

Le paramètre de nom de domaine **value** identifie le nom de domaine par défaut pour le groupe. Pour spécifier qu'il n'y a pas de nom de domaine par défaut, saisissez le mot-clé **none**. Cette commande définit un nom de domaine par défaut avec une valeur nulle, ce qui n'autorise pas un nom de domaine par défaut et empêche d'hériter d'un nom de domaine par défaut d'une stratégie de groupe par défaut ou d'une stratégie de groupe spécifiée.

Pour supprimer tous les noms de domaine par défaut, entrez la commande **no default-domain** sans arguments. Cette commande supprime tous les noms de domaine par défaut configurés, y compris une liste nulle si vous en avez créé une en saisissant la commande **default-domain** avec le mot-clé **none** . La forme **no** permet d'hériter d'un nom de domaine.

L'exemple suivant montre comment définir un nom de domaine par défaut FirstDomain pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

Définir une liste de domaines pour la tunnellisation fractionnée

Saisissez une liste de domaines à résoudre via le tunnel fractionné, en plus du domaine par défaut. Entrez la commande **split-dns** en mode de configuration de la stratégie de groupe. Pour supprimer une liste, saisissez la forme **no** de cette commande.

Lorsqu'il n'existe aucune liste de domaines de tunnellisation fractionnée, les utilisateurs héritent de celles définies dans la stratégie de groupe par défaut. Pour empêcher les utilisateurs d'hériter de telles listes de domaines de tunnellisation fractionnées, entrez la commande **split-dns** avec le mot-clé **none** .

Pour supprimer toutes les listes de domaines de tunnellisation fractionnées, entrez la commande **no split-dns** sans arguments. Cela supprime toutes les listes de domaines de tunnellisation fractionnée configurées, y compris une liste nulle créée en émettant la commande **split-dns** avec le mot-clé **none** .

Le paramètre domain-name **value** fournit un nom de domaine que l'ASA résout via le tunnel fractionné. Le mot-clé **none** indique qu'il n'y a pas de liste DNS fractionnée. Il définit également une liste DNS fractionnée avec une valeur nulle, interdisant ainsi une liste DNS fractionnée, et empêche d'hériter d'une liste DNS fractionnée d'une stratégie de groupe par défaut ou spécifiée. La syntaxe de la commande est la suivante :

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2... domain-nameN]
 | none}
hostname(config-group-policy)# no split-dns [domain-name domain-name2 domain-nameN]
```

Saisissez un espace unique pour séparer chaque entrée dans la liste de domaines. Il n'y a aucune limite au nombre d'entrées, mais la chaîne complète ne peut pas dépasser 492 caractères. Vous ne pouvez utiliser que des caractères alphanumériques, des tirets (-) et des points (.). Si le nom de domaine par défaut doit être résolu par le tunnel, vous devez inclure explicitement ce nom dans cette liste.

L'exemple suivant montre comment configurer les domaines Domain1, Domain2, Domain3 et Domain4 pour qu'ils soient résolus au moyen de la tunnellisation fractionnée pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

Remarque Lors de la configuration d'un DNS fractionné, vérifiez que les serveurs DNS privés spécifiés ne recoupent pas les serveurs DNS configurés pour la plateforme cliente. Si c'est le cas, la résolution de noms ne fonctionne pas correctement et des requêtes peuvent être rejetées.

Configurer l'interception DHCP pour Windows XP et la tunnellisation fractionnée

Une anomalie Microsoft XP entraîne la corruption des noms de domaine si les options de tunnellisation fractionnée dépassent 255 octets. Pour éviter ce problème, l'ASA limite le nombre de routes qu'il envoie à 27 à 40 routes, le nombre de routes dépendant des classes des routes.

DHCP Intercept permet aux clients Microsoft Windows XP d'utiliser la tunnellisation fractionnée avec l'ASA. L'ASA répond directement au message DHCP Inform du client Microsoft Windows XP, en fournissant à ce client le masque de sous-réseau, le nom de domaine et les routes statiques sans classe pour l'adresse IP du tunnel. Pour les clients Windows antérieurs à Windows XP, DHCP Intercept fournit le nom de domaine et le masque de sous-réseau. Cela est utile dans les environnements où l'utilisation d'un serveur DHCP n'est pas avantageuse.

La commande **intercept-dhcp** active ou désactive l'interception DHCP.

```
hostname(config-group-policy)# intercept-dhcp netmask {enable | disable}
hostname(config-group-policy)#
```

La variable *netmask* fournit le masque de sous-réseau pour l'adresse IP du tunnel. La forme **no** de cette commande supprime l'interception DHCP de la configuration :

[**no**] **intercept-dhcp**

L'exemple suivant montre comment définir les interceptions DHCP pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# intercept-dhcp enable
```

Configurer les paramètres du proxy de navigateur pour une utilisation avec les clients d'accès à distance

Suivez ces étapes pour configurer les paramètres du serveur proxy pour un client.

Procédure

Étape 1 Configurez un proxy de navigateur et un port pour un périphérique client en saisissant la commande **msie-proxy server** en mode de configuration de stratégie de groupe :

```
hostname(config-group-policy)# msie-proxy server {value server[:port] | none}
hostname(config-group-policy)#
```

La valeur par défaut est **none**, qui ne spécifie aucun paramètre du proxy de navigateur du périphérique client. Pour supprimer l'attribut de la configuration, utilisez la forme **no** de la commande.

```
hostname(config-group-policy)# no msie-proxy server
hostname(config-group-policy)#
```

La ligne contenant l'adresse IP ou le nom d'hôte du proxy et le numéro de port doit comporter moins de 100 caractères.

L'exemple suivant montre comment configurer l'adresse IP 192.168.10.1 en tant que proxy de navigateur, en utilisant le port 880, pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server value 192.168.21.1:880
hostname(config-group-policy)#
```

Étape 2 Configurez les actions du proxy de navigateur (« méthodes ») pour un périphérique client en saisissant la commande **msie-proxy method** en mode de configuration de stratégie de groupe.

```
hostname(config-group-policy)# msie-proxy method [auto-detect | no-modify |
no-proxy | use-server]
hostname(config-group-policy)#
```

La valeur par défaut est **no-modify**. Pour supprimer l'attribut de la configuration, utilisez la forme **no** de la commande.

```
hostname(config-group-policy)# no msie-proxy method [auto-detect | no-modify |
no-proxy | use-server]
hostname(config-group-policy)#
```

Les méthodes disponibles sont les suivantes :

- **auto-detect** : active la détection automatique du serveur mandataire dans le navigateur du périphérique client.
- **no-modify** : conserve inchangé le paramètre du proxy dans le navigateur HTTP pour ce périphérique client.
- **no-proxy—**Désactive le paramètre du proxy HTTP dans le navigateur pour le périphérique client.
- **use-server—**Définit le paramètre du proxy HTTP dans le navigateur pour utiliser la valeur configurée dans la commande **msie-proxy server** .

La ligne contenant l'adresse IP ou le nom d'hôte du proxy et le numéro de port doit comporter moins de 100 caractères.

L'exemple suivant montre comment configurer la détection automatique en tant que paramètre du proxy de navigateur pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy method auto-detect
hostname(config-group-policy)#
```

L'exemple suivant configure le paramètre proxy de navigateur pour la stratégie de groupe nommée FirstGroup afin d'utiliser le serveur QAserver, port 1001 comme serveur pour le périphérique client :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server QAserver:port 1001
hostname(config-group-policy)# msie-proxy method use-server
hostname(config-group-policy)#
```

Étape 3 Configurez les paramètres de liste d'exceptions du proxy de navigateur pour un contournement local sur le périphérique client en saisissant la commande **msie-proxy except-list** en mode de configuration de stratégie de groupe. Ces adresses ne sont pas accessibles par un proxy. Cette liste correspond à la zone Exceptions dans la boîte de dialogue Paramètres de proxy.

```
hostname(config-group-policy)# msie-proxy except-list {value server[:port] | none}
hostname(config-group-policy)#
```

Pour supprimer l'attribut de la configuration, utilisez la forme **no** de la commande :

```
hostname(config-group-policy)# no msie-proxy except-list
hostname(config-group-policy)#
```

- **value** server:port : spécifie l'adresse IP ou le nom d'un serveur MSIE et le port appliqué à ce périphérique client. Le numéro de port est facultatif.
- **none** :indique qu'il n'y a pas d'adresse IP, de nom d'hôte ni de port et empêche d'hériter d'une liste d'exceptions.

Par défaut, msie-proxy except-list est désactivé.

La ligne contenant l'adresse IP ou le nom d'hôte du proxy et le numéro de port doit comporter moins de 100 caractères.

L'exemple suivant montre comment définir une liste d'exceptions de proxy de navigateur, composée du serveur à l'adresse IP 192.168.20.1, en utilisant le port 880, pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
hostname(config-group-policy)#
```

Étape 4 Activez ou désactivez les paramètres de contournement local du proxy de navigateur pour un périphérique client en saisissant la commande **msie-proxy local-bypass** en mode de configuration de stratégie de groupe.

```
hostname(config-group-policy)# msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

Pour supprimer l'attribut de la configuration, utilisez la forme **no** de la commande.

```
hostname(config-group-policy)# no msie-proxy local-bypass {enable | disable}
hostname(config-group-policy)#
```

Par défaut, le contournement local du proxy est désactivé.

L'exemple suivant montre comment activer le contournement local du proxy de navigateur pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy local-bypass enable
hostname(config-group-policy)#
```

Configurer les attributs de sécurité pour les clients IPsec (IKEv1)

Pour spécifier les paramètres de sécurité pour un groupe, procédez comme suit.

Procédure

Étape 1 Précisez s'il faut autoriser les utilisateurs à enregistrer leurs mots de passe de connexion sur le système client, à l'aide de la commande **password-storage** avec le mot-clé **enable** en mode de configuration de stratégie de

groupe. Pour désactiver le stockage de mot de passe, utilisez la commande **password-storage** avec le mot-clé **disable**.

```
hostname(config-group-policy)# password-storage {enable | disable}
hostname(config-group-policy)#
```

Pour des raisons de sécurité, l'enregistrement des mots de passe est désactivé par défaut. Activez le stockage des mots de passe uniquement sur les systèmes que vous savez se trouver dans des sites sécurisés.

Pour supprimer l'attribut de stockage de mot de passe de la configuration en cours d'exécution, saisissez la forme **no** de cette commande :

```
hostname(config-group-policy)# no password-storage
hostname(config-group-policy)#
```

La spécification de cette forme **no** permet l'héritage d'une valeur de password-storage à partir d'une autre stratégie de groupe.

Cette commande ne s'applique pas à l'authentification interactive des clients matériels ni à l'authentification des utilisateurs individuels pour les clients matériels.

L'exemple suivant montre comment activer le stockage de mot de passe pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
hostname(config-group-policy)#
```

Étape 2 Précisez s'il faut activer la compression IP, qui est désactivée par défaut.

Remarque
La compression IP n'est pas prise en charge pour les connexions IPsec IKEv2.

```
hostname(config-group-policy)# ip-comp {enable | disable}
hostname(config-group-policy)#
```

Pour activer la compression IP LZS, entrez la commande **ip-comp** avec le mot-clé **enable** en mode de configuration de stratégie de groupe. Pour désactiver la compression IP, entrez la commande **ip-comp** avec le mot-clé **disable** .

Pour supprimer l'attribut **ip-comp** de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cela permet l'hérédité d'une valeur d'une autre stratégie de groupe.

```
hostname(config-group-policy)# no ip-comp
hostname(config-group-policy)#
```

L'activation de la compression des données peut accélérer les débits de transmission de données pour les utilisateurs d'appels distants qui se connectent avec des modems.

Astuces
La compression des données augmente les besoins en mémoire et l'utilisation du processeur pour chaque session utilisateur et réduit par conséquent le débit global de l'ASA. Pour cette raison, nous vous recommandons

d'activer la compression des données uniquement pour les utilisateurs distants se connectant avec un modem. Concevez une stratégie de groupe spécifique aux utilisateurs de modem et activez la compression uniquement pour eux.

Étape 3 Précisez s'il faut exiger que les utilisateurs se réauthentifient lors du renouvellement IKE, à l'aide de la commande **re-xauth** avec le mot-clé **enable** en mode de configuration de stratégie de groupe.

Remarque
Le renouvellement IKE n'est pas pris en charge pour les connexions IKEv2.

Si vous activez la réauthentification lors du renouvellement IKE, l'ASA invite l'utilisateur à saisir un nom d'utilisateur et un mot de passe lors de la négociation initiale IKE de phase 1 et lui redemande également de s'authentifier à chaque renouvellement IKE. La réauthentification offre une sécurité supplémentaire.

Si l'intervalle de renouvellement configuré est très court, les utilisateurs peuvent trouver les demandes d'autorisation répétées peu pratiques. Pour éviter les demandes d'autorisation répétées, désactivez la réauthentification. Pour vérifier l'intervalle de renouvellement configuré, en mode de surveillance, saisissez la commande **show crypto ipsec sa** permettant d'afficher la durée de vie de l'association de sécurité en secondes et en kilo-octets de données. Pour désactiver la réauthentification de l'utilisateur lors du renouvellement IKE, saisissez le mot-clé **disable**. La réauthentification sur le renouvellement IKE est désactivée par défaut.

```
hostname(config-group-policy)# re-xauth {enable | disable}
hostname(config-group-policy)#
```

Pour activer l'hérédité d'une valeur de réauthentification sur le renouvellement IKE à partir d'une autre stratégie de groupe, supprimez l'attribut re-xauth de la configuration en cours d'exécution en saisissant la forme **no** de cette commande :

```
hostname(config-group-policy)# no re-xauth
hostname(config-group-policy)#
```

Remarque
La réauthentification échoue s'il n'y a aucun utilisateur à l'autre extrémité de la connexion.

Étape 4 Précisez s'il faut activer la confidentialité de transmission parfaite. Dans les négociations IPsec, la confidentialité de transmission parfaite garantit que chaque nouvelle clé cryptographique n'est liée à aucune clé précédente. Une stratégie de groupe peut hériter d'une valeur de confidentialité de transmission parfaite d'une autre stratégie de groupe. La confidentialité de transmission parfaite est désactivée par défaut. Pour activer la confidentialité de transmission parfaite, utilisez la commande **pfs** avec le mot-clé **enable** en mode de configuration de stratégie de groupe.

```
hostname(config-group-policy)# pfs {enable | disable}
hostname(config-group-policy)#
```

Pour désactiver la confidentialité de transmission parfaite, entrez la commande **pfs** avec le mot-clé **disable** .

Pour supprimer l'attribut de confidentialité de transmission parfaite de la configuration en cours et éviter d'hériter d'une valeur, saisissez la forme **no** de cette commande.

```
hostname(config-group-policy)# no pfs
hostname(config-group-policy)#
```

Configurer les attributs IPsec-UDP pour les clients IKEv1

IPsec sur UDP, parfois appelé IPsec à travers NAT, permet à un client matériel de se connecter par UDP à un ASA qui exécute NAT. Il est désactivé par défaut. IPsec sur UDP est propriétaire ; il s'applique uniquement aux connexions d'accès à distance et nécessite une configuration de mode. L'ASA échange des paramètres de configuration avec le client pendant la négociation des SA. L'utilisation d'IPsec sur UDP peut dégrader légèrement les performances du système.

Pour activer IPsec sur UDP, configurez la commande **ipsec-udp** avec le mot-clé **enable** approprié en mode de configuration de stratégie de groupe, comme suit :

```
hostname(config-group-policy)# ipsec-udp {enable | disable}
hostname(config-group-policy)# no ipsec-udp
```

Pour utiliser IPsec sur UDP, vous devez également configurer la commande **ipsec-udp-port**, comme décrit dans cette section.

Pour désactiver IPsec sur UDP, saisissez le mot-clé **disable** . Pour supprimer l'attribut IPsec sur UDP de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cela permet l'hérédité d'une valeur pour IPsec sur UDP provenant d'une autre stratégie de groupe.

L'exemple suivant montre comment définir IPsec sur UDP pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp enable
```

Si vous avez activé IPsec sur UDP, vous devez également configurer la commande **ipsec-udp-port** en mode de configuration de stratégie de groupe. Cette commande définit un numéro de port UDP pour IPsec sur UDP. Pendant les négociations IPsec, l'ASA écoute sur le port configuré et transfère le trafic UDP pour ce port même si d'autres règles de filtrage abandonnent le trafic UDP. Les numéros de port peuvent être compris entre 4001 et 49151. La valeur par défaut est 10000.

Pour désactiver le port UDP, saisissez la forme **no** de cette commande. Cela permet d'hériter d'une valeur pour le port IPsec sur UDP provenant d'une autre stratégie de groupe.

```
hostname(config-group-policy)# ipsec-udp-port port
```

L'exemple suivant montre comment définir un port UDP IPsec au port 4025 pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```

Configurer les attributs pour les clients de matériel VPN

Procédure

Étape 1 (Facultatif) Configurez le mode d'extension du réseau avec la commande suivante :

[**no**] **nem** [**enable** | **disable**]

Le mode d'extension du réseau permet aux clients matériels de présenter un réseau unique routable au réseau privé distant via le tunnel VPN. La PAT ne s'applique pas. Par conséquent, les périphériques derrière le serveur Easy VPN ont un accès direct aux périphériques du réseau privé derrière le client Easy VPN distant sur le tunnel et uniquement sur le tunnel, et vice versa. Le client matériel doit lancer le tunnel, mais une fois que le tunnel est opérationnel, l'un ou l'autre des côtés peut lancer l'échange de données.

Exemple :

L'exemple suivant montre comment définir NEM pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
```

Pour désactiver le protocole NEM, saisissez le mot-clé **disable** . Pour supprimer l'attribut NEM de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cette option permet l'hérédité d'une valeur d'une autre stratégie de groupe.

Étape 2 (Facultatif) Configurez l'authentification de l'unité sécurisée avec la commande suivante :

[**no**] **secure-unit-authentication** [**enable** | **disable**]

L'authentification par unité sécurisée offre une sécurité supplémentaire en obligeant les clients de matériel VPN à s'authentifier à l'aide d'un nom d'utilisateur et d'un mot de passe chaque fois que le client amorce un tunnel. Avec cette fonctionnalité activée, le client matériel n'utilise pas le nom d'utilisateur et le mot de passe enregistrés. L'authentification par unité sécurisée est désactivée par défaut.

L'authentification par unité sécurisée nécessite que vous ayez un groupe de serveurs d'authentification configuré pour le profil de connexion utilisé par le ou les clients matériels. Si vous avez besoin d'une authentification par unité sécurisée sur l'appareil de sécurité adaptable Cisco principal, veillez à la configurer sur tous les serveurs de sauvegarde.

Remarque
Avec cette fonctionnalité activée, pour établir un tunnel VPN, un utilisateur doit être présent pour saisir le nom d'utilisateur et le mot de passe.

Exemple :

L'exemple suivant montre comment activer l'authentification par unité sécurisée pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)#group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-authentication enable
```

Pour désactiver l'authentification par unité sécurisée, saisissez le mot-clé **disable** . Pour supprimer l'attribut d'authentification par unité sécurisée de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cette option permet l'hérédité d'une valeur pour l'authentification par unité sécurisée d'une autre stratégie de groupe.

Étape 3 (Facultatif) Configurez l'authentification des utilisateurs avec la commande suivante :

[**no**] **user-authentication** [**enable** | **disable**]

Lorsque cette option est activée, l'authentification des utilisateurs exige que les utilisateurs individuels derrière un client matériel s'authentifient pour obtenir l'accès au réseau via le tunnel. Les utilisateurs individuels s'authentifient en fonction de l'ordre des serveurs d'authentification que vous configurez. L'authentification des utilisateurs est désactivée par défaut.

Si vous avez besoin de l'authentification des utilisateurs sur l'appareil de sécurité adaptable Cisco principal, veillez à la configurer sur tous les serveurs de sauvegarde.

Exemple :

L'exemple suivant montre comment activer l'authentification des utilisateurs pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
```

Pour désactiver l'authentification de l'utilisateur, saisissez le mot-clé **disable** . Pour supprimer l'attribut d'authentification de l'utilisateur de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cette option permet l'hérédité d'une valeur pour l'authentification des utilisateurs d'une autre stratégie de groupe.

Étape 4 Définissez un délai d'inactivité pour les utilisateurs individuels qui se sont authentifiés avec la commande suivante :

[**no**] **user-authentication-idle-timeout** *minutes* | **none**]

Le paramètre *minutes* spécifie le nombre de minutes dans la période d'inactivité. Le minimum est de 1 minute, la valeur par défaut est de 30 minutes et le maximum est de 35 791 394 minutes.

S'il n'y a aucune activité de communication par un utilisateur derrière un client matériel pendant la période d'inactivité, l'ASA met fin à l'accès du client. Cette minuterie met fin uniquement à l'accès du client par le tunnel VPN, et non au tunnel VPN lui-même.

Exemple :

L'exemple suivant montre comment définir une valeur de délai d'inactivité de 45 minutes pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
hostname(config-group-policy)#user-authentication-idle-timeout 45
```

Pour supprimer la valeur de délai d'inactivité, saisissez la forme **no** de cette commande. Cette option permet l'hérédité d'une valeur de délai d'inactivité d'une autre stratégie de groupe. Pour éviter d'hériter d'une valeur de délai d'inactivité, entrez la commande **user-authentication-idle-timeout** avec le mot-clé **none** . Cette commande définit le délai d'inactivité avec une valeur nulle, ce qui désactive le délai d'inactivité et empêche l'hérédité d'une valeur de délai d'inactivité d'authentification d'utilisateur à partir d'une politique par défaut ou d'un groupe spécifié.

Remarque
Le délai d'inactivité indiqué en réponse à la commande **show uauth** est toujours la valeur du délai d'inactivité de l'utilisateur qui a authentifié le tunnel sur le périphérique distant du VPN Cisco Easy.

Étape 5 Configurez le contournement des téléphones IP avec la commande suivante :

ip-phone-bypass enable

Le contournement du téléphone IP permet aux téléphones IP derrière les clients matériels de se connecter sans subir les processus d'authentification des utilisateurs. Le contournement du téléphone IP est désactivé par défaut. Cela s'applique uniquement lorsque l'IUA est activée.

Remarque
Vous devez également configurer l'exemption d'adresse MAC sur le client pour exempter ces clients de l'authentification.

Pour désactiver le contournement du téléphone IP, saisissez le mot-clé **disable** . Pour supprimer l'attribut de contournement du téléphone IP de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cette option permet l'héritage d'une valeur pour le contournement du téléphone IP d'une autre stratégie de groupe.

Étape 6 Configurez le contournement LEAP avec la commande suivante :

leap-bypass enable

Le contournement LEAP s'applique uniquement lorsque **user-authentication** est activée. Cette commande permet aux paquets LEAP des périphériques de point d'accès sans fil Cisco d'établir l'authentification LEAP, puis de s'authentifier à nouveau par authentification de l'utilisateur. Le contournement LEAP est désactivé par défaut.

Les utilisateurs LEAP derrière un client matériel ont un dilemme circulaire : ils ne peuvent pas négocier l'authentification LEAP, car ils ne peuvent pas envoyer leurs informations d'authentification au serveur RADIUS derrière le périphérique de site central sur le tunnel. La raison pour laquelle ils ne peuvent pas envoyer leurs informations d'authentification sur le tunnel est qu'ils ne se sont pas authentifiés sur le réseau sans fil. Pour résoudre ce problème, le contournement LEAP permet aux paquets LEAP, et uniquement aux paquets LEAP, de traverser le tunnel pour authentifier la connexion sans fil avec un serveur RADIUS avant que les utilisateurs individuels ne s'authentifient. Les utilisateurs procèdent ensuite à l'authentification individuelle des utilisateurs.

Le contournement LEAP fonctionne correctement dans les conditions suivantes :

- **secure-unit-authentication** doit être désactivé. Si l'authentification de l'unité interactive est activée, un périphérique non LEAP (filaire) doit authentifier le client matériel avant que les périphériques LEAP puissent se connecter en utilisant ce tunnel.
- **user-authentication** est activé. Sinon, le contournement LEAP ne s'applique pas.
- Les points d'accès dans l'environnement sans fil doivent être des points d'accès Cisco Aironet exécutant le protocole de découverte Cisco (CDP). Les cartes réseau (NIC) sans fil pour PC peuvent être d'autres marques.

Exemple :

L'exemple suivant montre comment définir le contournement LEAP pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
hostname(config-group-policy)# leap-bypass enable
```

Pour désactiver le contournement LEAP, saisissez le mot-clé **disable** . Pour supprimer l'attribut de contournement LEAP de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cette option permet l'héritage d'une valeur pour le contournement LEAP d'une autre stratégie de groupe :

Configurer les attributs de stratégie de groupe pour les connexions Secure Client (services client sécurisés)

Après avoir activé les connexions Secure Client (services client sécurisés) comme décrit dans Connexions du client VPN AnyConnect, vous pouvez activer ou exiger les fonctionnalités Secure Client (services client sécurisés) pour une stratégie de groupe. Suivez ces étapes en mode de configuration webvpn de stratégie de groupe :

Procédure

Étape 1 Entrez le mode de configuration webvpn de stratégie de groupe. Par exemple :

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
```

Étape 2 Pour désactiver l'installation permanente du Secure Client (services client sécurisés) sur l'ordinateur terminal, utilisez la commande AnyConnect keep-installer avec le mot-clé **none**. Par exemple :

```
hostname(config-group-webvpn)# anyconnect keep-installer none
hostname(config-group-webvpn)#
```

La valeur par défaut est que l'installation permanente du client est activée. Le client reste installé sur le point terminal à la fin de la session Secure Client (services client sécurisés).

Étape 3 Pour activer la compression des données HTTP sur la connexion SSL Secure Client (services client sécurisés) pour la stratégie de groupe, saisissez la commande AnyConnect ssl compression. Par défaut, la compression est définie sur **none** (désactivé). Pour activer la compression, utilisez le mot-clé **deflate** . Par exemple :

```
hostname(config-group-webvpn)# anyconnect compression deflate
hostname(config-group-webvpn)#
```

Étape 4 Configurer

Étape 5 Vous pouvez vous assurer que la connexion Secure Client (services client sécurisés) par l'intermédiaire d'un proxy, d'un pare-feu ou d'un périphérique NAT reste ouverte, même si le périphérique limite la durée pendant laquelle la connexion peut être inactive, en ajustant la fréquence des messages keepalive à l'aide de la commande **anyconnect ssl keepalive command:**

anyconnect ssl keepalive {none | *seconds***}**

Le réglage de keepalives garantit également que Secure Client (services client sécurisés) ne se déconnecte pas et ne se reconnecte pas lorsque l'utilisateur distant n'exécute pas activement une application basée sur des sockets, comme Microsoft Outlook ou Microsoft Internet Explorer.

L'exemple suivant configure l'appareil de sécurité pour activer Secure Client (services client sécurisés) afin d'envoyer des messages keepalive, avec une fréquence de 300 secondes (5 minutes) :

```
hostname(config-group-webvpn)# anyconnect ssl keepalive 300
hostname(config-group-webvpn)#
```

Étape 6 Pour permettre à Secure Client (services client sécurisés) d'effectuer un renouvellement sur une session SSL, utilisez la commande AnyConnect ssl rekey :

AnyConnect ssl rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}}

Par défaut, le renouvellement est désactivé.

La définition de la méthode en tant que new-tunnel spécifie que Secure Client (services client sécurisés) établit un nouveau tunnel pendant le renouvellement SSL. La spécification de la méthode comme aucune désactive le renouvellement. La définition de la méthode en tant que SSL indique que la renégociation SSL a lieu pendant le renouvellement. Au lieu de préciser la méthode, vous pouvez préciser l'heure : c'est-à-dire le nombre de minutes entre le début de la session et le renouvellement, de 1 à 10 080 (1 semaine).

L'exemple suivant configure Secure Client (services client sécurisés) pour renégocier avec SSL pendant le renouvellement et configure le renouvellement pour qu'il se produise 30 minutes après le début de la session :

```
hostname(config-group-webvpn)# anyconnect ssl rekey method ssl
hostname(config-group-webvpn)# anyconnect ssl rekey time 30
hostname(config-group-webvpn)#
```

Étape 7 La fonctionnalité Client Protocol Bypass vous permet de configurer la façon dont Secure Client (services client sécurisés) gère le trafic IPv4 lorsque l'ASA s'attend uniquement à du trafic IPv6 ou comment il gère le trafic IPv6 lorsqu'il s'attend uniquement à du trafic IPv4.

Lorsque Secure Client (services client sécurisés) établit une connexion VPN avec l'ASA, l'ASA peut lui attribuer une adresse IPv4, IPv6 ou à la fois une adresse IPv4 et IPv6. Si l'ASA attribue à la connexion Secure Client (services client sécurisés) uniquement une adresse IPv4 ou uniquement une adresse IPv6, vous pouvez maintenant configurer le protocole de contournement du client pour rejeter le trafic réseau pour lequel l'ASA n'a pas attribué d'adresse IP, ou permettre à ce trafic de contourner l'ASA et d'être envoyé par le client non chiffré ou « en clair ».

Par exemple, supposons que l'ASA attribue uniquement une adresse IPv4 à la connexion Secure Client (services client sécurisés) et que le point terminal soit en double pile. Lorsque le point terminal tente d'atteindre une adresse IPv6, si le protocole de contournement des clients est désactivé, le trafic IPv6 est abandonné; cependant, si le protocole de contournement client est activé, le trafic IPv6 est envoyé par le client en clair.

Si vous établissez un tunnel IPsec (par opposition à une connexion SSL), l'ASA n'est pas informé si IPv6 est activé ou non sur le client, donc l'ASA applique toujours le paramètre du protocole de contournement du client.

Utilisez la commande client-bypass-protocol pour activer ou désactiver la fonctionnalité du protocole de contournement du client. Voici la syntaxe de la commande :

client-bypass-protocol {enable | disable}

L'exemple suivant active le protocole de contournement du client :

```
hostname(config-group-policy)# client-bypass-protocol enable
hostname(config-group-policy)#
```

L'exemple suivant désactive le protocole de contournement du client :

```
hostname(config-group-policy)# client-bypass-protocol disable
hostname(config-group-policy)#
```

L'exemple suivant supprime un paramètre de protocole de contournement du client activé ou désactivé :

```
hostname(config-group-policy)# no client-bypass-protocol enable
hostname(config-group-policy)#
```

Étape 8 Si vous avez configuré l'équilibrage de charge entre vos périphériques ASA, spécifiez le FQDN de l'ASA afin de résoudre l'adresse IP de l'ASA utilisée pour rétablir la session VPN. Ce paramètre est essentiel pour prendre en charge l'itinérance des clients entre les réseaux de différents protocoles IP (comme IPv4 à IPv6).

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

Si le nom de domaine complet du périphérique n'est pas transmis au client, le client tentera de se reconnecter à l'adresse IP que le tunnel avait précédemment établie. Afin de prendre en charge l'itinérance entre les réseaux de différents protocoles IP (de IPv4 à IPv6), Secure Client (services client sécurisés) doit effectuer la résolution de nom du FQDN du périphérique après l'itinérance, afin de pouvoir déterminer quelle adresse ASA utiliser pour rétablir le tunnel. Le client utilise le nom de domaine complet ASA présent dans son profil lors de la connexion initiale. Lors des reconnexions de session ultérieures, il utilise toujours le nom de domaine complet du périphérique transmis par l'ASA (et configuré par l'administrateur dans la stratégie de groupe), le cas échéant. Si le nom de domaine complet n'est pas configuré, l'ASA détermine le nom de domaine complet du périphérique (et l'envoie au client) de tout ce qui est défini sous Configuration > Device Setup (Configuration du périphérique) > Device Name/Password and Domain Name (Nom du périphérique/mot de passe et nom de domaine).

Si le nom de domaine complet du périphérique n'est pas poussé par l'ASA, le client ne peut pas rétablir la session VPN après avoir effectué l'itinérance entre les réseaux de protocoles IP différents.

Utilisez la commande gateway-fqdn pour configurer le nom de domaine complet de l'ASA. Voici la syntaxe de la commande :

gateway-fqdn { **value** *FQDN_Name* | **none**} or **no gateway-fqdn**

L'exemple suivant définit le nom de domaine complet de l'ASA comme ASAName.example.cisco.com

```
hostname(config-group-policy)# gateway-fqdn value ASAName.example.cisco.com
hostname(config-group-policy)#
```

L'exemple suivant supprime le nom de domaine complet de l'ASA de la stratégie de groupe. La stratégie de groupe hérite ensuite de cette valeur de la stratégie de groupe par défaut.

```
hostname(config-group-policy)# no gateway-fqdn
hostname(config-group-policy)#
```

L'exemple suivant définit le nom de domaine complet comme une valeur vide. Le nom de domaine complet configuré à l'aide des commandes hostname et domain-name sera utilisé s'il est disponible.

```
hostname(config-group-policy)# gateway-fqdn none
```

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

Configurer les attributs du serveur de sauvegarde

Configurez les serveurs de sauvegarde si vous prévoyez de les utiliser. Les serveurs de sauvegarde IPsec permettent à un client VPN de se connecter au site central lorsque l'ASA principal n'est pas disponible. Lorsque vous configurez les serveurs de sauvegarde, l'ASA transmet la liste des serveurs au client pendant l'établissement du tunnel IPsec. Les serveurs de sauvegarde n'existent pas tant que vous ne les avez pas configurés, que ce soit sur le client ou sur l'ASA principal.

Configurez les serveurs de sauvegarde sur le client ou sur l'ASA principal. Si vous configurez des serveurs de sauvegarde sur l'ASA, l'ASA transmet la liste des serveurs au clien vers les clients du groupe, en remplacement de la liste de serveurs de sauvegarde sur le client si elle est configurée.

Remarque Si vous utilisez des noms d'hôte, il est conseillé d'avoir des serveurs DNS et WINS de secours sur un réseau distinct de celui des serveurs DNS et WINS principaux. Sinon, si les clients derrière un client matériel obtiennent des informations DNS et WINS du client matériel par DHCP, et que la connexion au serveur principal est perdue, et que les serveurs de secours utilisent des informations DNS et WINS différentes, les clients ne peuvent pas être mis à jour tant que le bail DHCP n'expire pas. En outre, si vous utilisez des noms d'hôte et que le serveur DNS n'est pas disponible, des retards importants peuvent se produire.

Pour configurer les serveurs de sauvegarde, saisissez la commande **backup-servers** en mode de configuration de stratégie de groupe :

```
hostname(config-group-policy)# backup-servers {server1 server2... server10 |
clear-client-config | keep-client-config}
```

Pour supprimer un serveur de sauvegarde, saisissez la forme **no** de cette commande avec le serveur de sauvegarde spécifié. Pour supprimer l'attribut backup-servers de la configuration en cours d'exécution et activer l'hérédité d'une valeur pour backup-servers d'une autre stratégie de groupe, saisissez la forme **no** de cette commande sans arguments.

```
hostname(config-group-policy)# no backup-servers [server1 server2... server10 |
clear-client-config | keep-client-config]
```

Le mot-clé **clear-client-config** spécifie que le client n'utilise aucun serveur de sauvegarde. L'ASA transmet une liste de serveurs vide.

Le mot-clé **keep-client-config** spécifie que l'ASA n'envoie aucune information sur les serveurs de sauvegarde. Le client utilise sa propre liste de serveurs de sauvegarde, le cas échéant. Il s'agit du paramètre par défaut.

La liste de paramètres *server1 server 2.... server10* est une liste de serveurs délimités par des espaces et ordonnés par priorité pour le client VPN à utiliser lorsque l'ASA principal n'est pas disponible. Cette liste identifie les serveurs par adresse IP ou nom d'hôte. La liste peut comporter 500 caractères et contenir jusqu'à 10 entrées.

L'exemple suivant montre comment configurer les serveurs de sauvegarde avec les adresses IP 10.10.10.1 et 192.168.10.14, pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

Configurer les paramètres du contrôle d'admission au réseau

Les commandes NAC de stratégie de groupe dans cette section ont toutes des valeurs par défaut. Sauf si vous avez une bonne raison de les modifier, acceptez les valeurs par défaut pour ces paramètres.

L'ASA utilise la messagerie EAP (Extensible Authentication Protocol) sur UDP (EAPoUDP) pour valider la posture des hôtes distants. La validation de posture consiste à vérifier qu'un hôte distant est conforme aux exigences de sécurité avant l'attribution d'une politique d'accès réseau. Un serveur de contrôle d'accès doit être configuré pour le contrôle d'admission au réseau avant de configurer la NAC sur l'appareil de sécurité.

Le serveur de contrôle d'accès télécharge le jeton de posture, une chaîne de texte d'information configurable sur l'ACS, vers le périphérique de sécurité afin d'aider à la surveillance du système, au reporting, au débogage et à la journalisation. Un jeton de posture typique est Healthy (En bonne santé), Checkup (Contrôle), Quarantine (Quarantaine), Infected (Infecté) ou Unknown (Inconnu). Après la validation de la posture ou l'authentification sans client, l'ACS télécharge la politique d'accès de la session sur l'appareil de sécurité.

Pour configurer les paramètres de contrôle d'admission au réseau pour la stratégie de groupe par défaut ou une autre stratégie de groupe, procédez comme suit.

Procédure

Étape 1 (Facultatif) Configurez la période de la minuterie de requête d'état. l'appareil de sécurité démarre la minuterie de requête d'état après chaque validation de posture et réponse à la requête d'état réussies. L'expiration de cette minuterie déclenche une requête pour les modifications de la posture de l'hôte, appelée requête d'état. Saisissez le nombre de secondes dans une plage de 30 à 1 800. Le paramètre par défaut est 300.

Pour préciser l'intervalle entre chaque validation de posture réussie dans une session de contrôle d'admission du réseau et la prochaine requête pour modifications de la posture d'hôte, utilisez la commande **nac-sq-period** en mode de configuration de stratégie de groupe :

```
hostname(config-group-policy)# nac-sq-period seconds
hostname(config-group-policy)#
```

Pour hériter de la valeur du minuteur de requête d'état depuis la stratégie de groupe par défaut, accédez à l'autre stratégie de groupe depuis laquelle vous souhaitez hériter, puis utilisez la forme **no** de cette commande :

```
hostname(config-group-policy)# no nac-sq-period [seconds]
hostname(config-group-policy
```

L'exemple suivant modifie la valeur de la minuterie de requête d'état à 1 800 secondes :

```
hostname(config-group-policy)# nac-sq-period 1800
hostname(config-group-policy)#
```

L'exemple suivant hérite de la valeur du minuteur de requête d'état depuis la stratégie de groupe par défaut :

```
hostname(config-group-policy)# no nac-sq-period
```

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

Étape 2 (Facultatif) Configurez la période de revalidation de la NAC. l'appareil de sécurité démarre la minuterie de revalidation après chaque validation de posture réussie. L'expiration de cette minuterie déclenche la prochaine validation de posture inconditionnelle. l'appareil de sécurité conserve la validation de la posture pendant la revalidation. La stratégie de groupe par défaut entre en vigueur si le serveur de contrôle d'accès n'est pas disponible pendant la validation ou la revalidation de la posture. Saisissez l'intervalle en secondes entre chaque validation de posture réussie. La plage est de 300 à 86 400. Le paramètre par défaut est 36 000.

Pour préciser l'intervalle entre chaque validation de posture réussie dans une session de contrôle d'admission du réseau, utilisez la commande **nac-reval-period** en mode de configuration de stratégie de groupe :

```
hostname(config-group-policy)# nac-reval-period seconds
hostname(config-group-policy)#
```

Pour hériter de la valeur du minuteur de revalidation depuis la stratégie de groupe par défaut, accédez à l'autre stratégie de groupe depuis laquelle vous souhaitez hériter, puis utilisez la forme **no** de cette commande :

```
hostname(config-group-policy)# no nac-reval-period [seconds]
hostname(config-group-policy)#
```

L'exemple suivant modifie la minuterie de revalidation à 86 400 secondes :

```
hostname(config-group-policy)# nac-reval-period 86400
hostname(config-group-policy)
```

L'exemple suivant hérite de la valeur du délai de revalidation de la stratégie de groupe par défaut :

```
hostname(config-group-policy)# no nac-reval-period
hostname(config-group-policy)#
```

Étape 3 (Facultatif) Configurez l'ACL par défaut pour la NAC. l'appareil de sécurité applique la politique de sécurité associée à l'ACL sélectionnée si la validation de la posture échoue. Spécifiez **none** ou une liste de contrôle d'accès étendue. Le paramètre par défaut est **none**. Si le paramètre est **none** et que la validation de la posture échoue, l'appareil de sécurité applique la stratégie de groupe par défaut.

Pour spécifier la liste de contrôle d'accès à utiliser comme liste de contrôle d'accès par défaut pour les sessions de contrôle d'admission au réseau qui échouent à la validation de la posture, utilisez la commande **nac-default-acl** en mode de configuration de stratégie de groupe :

```
hostname(config-group-policy)# nac-default-acl {acl-name | none}
hostname(config-group-policy)#
```

Pour hériter de l'ACL de la stratégie de groupe par défaut, accédez à l'autre stratégie de groupe à partir de laquelle l'hériter, puis utilisez la forme **no** de cette commande :

```
hostname(config-group-policy)# no nac-default-acl [acl-name | none]
hostname(config-group-policy)#
```

Les éléments de cette commande sont les suivants :

- *acl-name :* spécifie le nom du groupe de serveurs de validation de posture, tel qu'il est configuré sur l'ASA à l'aide de la commande **aaa-server host**. Le nom doit correspondre à la variable de balise de serveur spécifiée dans cette commande.
- **none** : désactive l'hérédité de l'ACL de la stratégie de groupe par défaut et n'applique pas d'ACL aux sessions de la NAC qui échouent la validation de la posture.

Comme la NAC est désactivée par défaut, le trafic VPN traversant l'ASA n'est pas soumis à l'ACL par défaut de la NAC tant que la NAC n'est pas activée.

L'exemple suivant identifie acl-1 comme liste de contrôle d'accès à appliquer lorsque la validation de la posture échoue :

```
hostname(config-group-policy)# nac-default-acl acl-1
hostname(config-group-policy)#
```

L'exemple suivant hérite de l'ACL de la stratégie de groupe par défaut :

```
hostname(config-group-policy)# no nac-default-acl
hostname(config-group-policy)#
```

L'exemple suivant désactive l'hérédité de l'ACL de la stratégie de groupe par défaut et n'applique pas d'ACL aux sessions de la NAC qui échouent la validation de la posture :

```
hostname(config-group-policy)# nac-default-acl none
hostname(config-group-policy)#
```

Étape 4 Configurer des exemptions NAC pour le VPN Par défaut, la liste d'exemptions est vide. La valeur par défaut de l'attribut de filtre est **none**. Saisissez la **commande vpn-nac-exempt** une fois pour chaque système d'exploitation (et liste de contrôle d'accès) à mettre en correspondance afin d'exempter les hôtes distants de la validation de la posture.

Pour ajouter une entrée à la liste des types d'ordinateurs distants qui sont exemptés de la validation de la posture, utilisez la commande **vpn-nac-exempt** en mode de configuration de stratégie de groupe :

```
hostname(config-group-policy)# vpn-nac-exempt os "os name" [filter {acl-name | none}]
[disable]
hostname(config-group-policy)#
```

Pour désactiver l'hérédité et préciser que tous les hôtes sont soumis à la validation de la posture, utilisez le mot-clé **none** immédiatement après **vpn-nac-exempt** :

```
hostname(config-group-policy)# vpn-nac-exempt none
hostname(config-group-policy)#
```

Pour supprimer une entrée de la liste d'exemptions, utilisez la forme **no** de cette commande et nommez le système d'exploitation (et l'ACL) dans l'entrée à supprimer :

```
hostname(config-group-policy)# no vpn-nac-exempt [os "os name"] [filter {acl-name | none}]
 [disable]
hostname(config-group-policy)#
```

Pour supprimer toutes les entrées de la liste d'exemptions associée à cette stratégie de groupe et hériter de la liste de la stratégie de groupe par défaut, utilisez la forme **no** de cette commande sans préciser de mots-clés supplémentaires :

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)#
```

Les éléments de syntaxe de ces commandes sont les suivants :

- *acl-name :*nom de l'ACL présente dans la configuration ASA.
- disable : désactive l'entrée dans la liste d'exemptions sans la supprimer de la liste.
- **filter** : (facultatif) Appliquez une ACL pour filtrer le trafic si l'ordinateur correspond au nom du système d'exploitation.
- **none** : lorsqu'il est saisi immédiatement après **vpn-nac-exempt**, ce mot-clé désactive l'hérédité et spécifie que tous les hôtes sont soumis à la validation de la posture. Lorsqu'il est saisi immédiatement après **le filtre**, ce mot-clé indique que l'entrée ne spécifie pas d'ACL.
- **OS**(système d'exploitation**) :**exempte un système d'exploitation de la validation de la posture.
- *os name :* nom du système d'exploitation. Les guillemets sont requis uniquement si le nom comprend un espace (par exemple, « Windows XP »).

L'exemple suivant désactive l'hérédité et spécifie que tous les hôtes seront soumis à la validation de la posture :

```
hostname(config-group-policy)# no vpn-nac-exempt none
hostname(config-group-policy)
```

L'exemple suivant supprime toutes les entrées de la liste d'exemptions :

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)
```

Étape 5 Activez ou désactivez le contrôle d'admission au réseau en entrant la commande suivante :

```
hostname(config-group-policy)# nac {enable | disable}
hostname(config-group-policy)#
```

Pour hériter du paramètre NAC de la stratégie de groupe par défaut, accédez à l'autre stratégie de groupe à partir de laquelle l'hériter, puis utilisez la forme **no** de cette commande :

```
hostname(config-group-policy)# no nac [enable | disable]
hostname(config-group-policy)#
```

Par défaut, la NAC est désactivée. L'activation de la NAC nécessite une validation de la posture pour l'accès à distance. Si l'ordinateur distant réussit les vérifications de validation, le serveur ACS télécharge la politique d'accès pour que l'ASA l'applique. La NAC est désactivée par défaut.

Un serveur de contrôle d'accès doit être présent sur le réseau.

L'exemple suivant active la NAC pour la stratégie de groupe :

```
hostname(config-group-policy)# nac enable
hostname(config-group-policy)#
```

Configurer les politiques de pare-feu des clients VPN

Un pare-feu isole et protège un ordinateur contre Internet en inspectant chaque paquet de données entrant et sortant pour déterminer s'il faut l'autoriser à passer par le pare-feu ou l'abandonner. Les pare-feu offrent une sécurité supplémentaire si les utilisateurs distants d'un groupe ont configuré la tunnellisation fractionnée. Dans ce cas, le pare-feu protège l'ordinateur de l'utilisateur, et, par conséquent, le réseau d'entreprise, contre les intrusions par Internet ou le réseau local (LAN) de l'utilisateur. Les utilisateurs distants se connectant à l'ASA avec le client VPN peuvent choisir l'option de pare-feu appropriée.

Définissez les politiques de pare-feu personnelles que l'ASA transmet au client VPN lors de la négociation du tunnel IKE à l'aide de la commande **client-firewall** en mode de configuration de stratégie de groupe. Pour supprimer une politique de pare-feu, entrez la forme **no** de cette commande.

Pour supprimer toutes les politiques de pare-feu, entrez la commande **no client-firewall** sans arguments. Cette commande supprime toutes les politiques de pare-feu configurées, y compris une politique nulle si vous en avez créé une en saisissant la commande **client-firewall** avec le mot-clé **none** .

En l'absence de politiques de pare-feu, les utilisateurs héritent de celles qui existent dans la politique par défaut ou dans une autre stratégie de groupe. Pour empêcher les utilisateurs d'hériter de ces politiques de pare-feu, entrez la commande **client-firewall** avec le mot-clé **none** .

La boîte de dialogue Ajouter ou Modifier une stratégie de groupe sous l'onglet Pare-feu client vous permet de configurer les paramètres de pare-feu pour les clients VPN pour la stratégie de groupe en cours d'ajout ou de modification.

Remarque Seuls les clients VPN exécutant Microsoft Windows peuvent utiliser ces paramètres de pare-feu. Ils ne sont actuellement pas disponibles pour les clients matériels ou autres clients logiciels (non Windows).

Dans le premier scénario, un utilisateur distant dispose d'un pare-feu personnel installé sur le PC. Le client VPN applique la politique de pare-feu définie sur le pare-feu local et il surveille ce pare-feu pour s'assurer qu'il est en cours d'exécution. Si le pare-feu arrête de s'exécuter, le client VPN abandonne la connexion à l'ASA. (Ce mécanisme d'application du pare-feu est appelé Are You There (AYT), car le client VPN surveille le pare-feu en lui envoyant périodiquement des messages « are you there? » ; si aucune réponse n'est reçue, le client VPN sait que le pare-feu est hors service et met fin à sa connexion à l'ASA.) L'administrateur réseau peut configurer ces pare-feu de PC à l'origine, mais avec cette approche, chaque utilisateur peut personnaliser sa propre configuration.

Dans le deuxième scénario, vous pourriez préférer appliquer une politique de pare-feu centralisée pour les pare-feu personnels sur les PC clients VPN. Un exemple courant serait de bloquer le trafic Internet vers les PC distants d'un groupe à l'aide de la 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.

Configurer les politiques de pare-feu pour Secure Client (services client sécurisés)

Les règles de pare-feu pour Secure Client (services client sécurisés) peuvent préciser des adresses IPv4 et IPv6.

Avant de commencer

Vous avez créé des règles d'accès unifiées avec des adresses IPv6 spécifiées.

Procédure

Étape 1 Entrez en mode de configuration de stratégie de groupe webvpn.

webvpn

Exemple :

```
hostname(config)# group-policy ac-client-group attributes
hostname(config-group-policy)# webvpn
```

Étape 2 Précisez une règle de contrôle d'accès pour la règle de réseau privé ou public. La règle de réseau privé est la règle appliquée à l'interface d'adaptateur virtuel VPN sur le client.

AnyConnect firewall-rule client-interface {private | public} value *[RuleName]*

```
hostname(config-group-webvpn)# anyconnect firewall-rule client-interface private value
ClientFWRule
```

Étape 3 Affichez les attributs de la stratégie de groupe ainsi que l'attribut de politique webvpn pour la stratégie de groupe.

show runn group-policy [value]

Exemple :

```
hostname(config-group-webvpn)# show run group-policy FirstGroup
group-policy FirstGroup internal
group-policy FirstGroup attributes
webvpn
  anyconnect firewall-rule client-interface private value ClientFWRule
```

Étape 4 Supprimez la règle de pare-feu client de la règle de réseau privé.

no anyconnect firewall-rule client-interface private value [*RuleName*]

Exemple :

```
hostname(config-group-webvpn)# no anyconnect firewall-rule client-interface private value
hostname(config-group-webvpn)#
```

Utiliser un serveur Zone Labs Integrity.

Cette section présente le serveur Zone Labs Integrity, également appelé serveur Check Point Integrity, et fournit un exemple de procédure de configuration de l'ASA pour prendre en charge le serveur Zone Labs Integrity. Le serveur Integrity est un poste de gestion centralisé pour la configuration et l'application des politiques de sécurité sur les ordinateurs distants. Si un PC distant ne se conforme pas à la politique de sécurité dictée par le serveur Integrity, il ne peut pas accéder au réseau privé protégé par le serveur Integrity et l'ASA.

Le logiciel client VPN et le logiciel client Integrity résident sur le même ordinateur distant. Les étapes suivantes résument les actions du PC distant, de l'ASA et du serveur Integrity dans l'établissement d'une session entre le PC et le réseau privé d'entreprise :

1. Le logiciel client VPN (résidant sur le même ordinateur distant que le logiciel client Integrity) se connecte à l'ASA et indique à ce dernier de quel type de client de pare-feu il s'agit.
2. Une fois que l'ASA a approuvé le type de pare-feu du client, l'ASA transmet les informations d'adresse du serveur Integrity au client Integrity.
3. Lorsque l'ASA agit comme proxy, le client Integrity établit une connexion restreinte avec le serveur Integrity. Une connexion restreinte existe uniquement entre le client Integrity et le serveur Integrity.
4. Le serveur Integrity détermine si le client Integrity est conforme aux politiques de sécurité obligatoires. Si le client Integrity est conforme aux politiques de sécurité, le serveur Integrity demande à l'ASA d'ouvrir la connexion et de fournir au client Integrity les détails de la connexion.
5. Sur le PC distant, le client VPN transmet les détails de la connexion au client Integrity et signale que l'application de la politique doit commencer immédiatement et que le client Integrity peut accéder au réseau privé.
6. Une fois la connexion VPN établie, le serveur Integrity continue de surveiller l'état du client Integrity à l'aide de messages de pulsation du client.

Remarque La version actuelle de l'ASA prend en charge un seul serveur Integrity à la fois, même si les interfaces utilisateur permettent de configurer jusqu'à cinq serveurs Integrity. Si le serveur Integrity actif tombe en panne, configurez-en un autre sur l'ASA, puis rétablissez la session client VPN.

Pour configurer le serveur Integrity, procédez comme suit :

Procédure

Étape 1 Configurez un serveur Integrity en utilisant l'adresse IP 10.0.0.5.

```
zonelabs-Integrity server-address {hostname1 | ip-address1}
```

Exemple :

```
hostname(config)# zonelabs-Integrity server-address 10.0.0.5
```

Étape 2 Précisez le port 300 (le port par défaut est 5054).

zonelabs-integrity port port-number

Exemple :

```
hostname(config)# zonelabs-integrity port 300
```

Étape 3 Précisez l'interface interne pour les communications avec le serveur Integrity.

zonelabs-integrity interface interface

Exemple :

```
hostname(config)# zonelabs-integrity interface inside
```

Étape 4 Assurez-vous que l'ASA attend 12 secondes une réponse du serveur Integrity actif ou de secours avant de déclarer le serveur Integrity défaillant et de fermer les connexions des clients VPN.

Remarque
Si la connexion entre l'ASA et le serveur Integrity échoue, les connexions du client VPN restent ouvertes par défaut afin que le VPN d'entreprise ne soit pas interrompu par la défaillance d'un serveur Integrity. Cependant, vous pourriez vouloir fermer les connexions VPN si le serveur Zone Labs Integrity tombe en panne.

zonelabs-integrity fail-timeout timeout

Exemple :

```
hostname(config)# zonelabs-integrity fail-timeout 12
```

Étape 5 Configurez l'ASA de sorte que les connexions aux clients VPN se terminent lorsque la connexion entre l'ASA et le serveur Zone Labs Integrity échoue.

zonelabs-integrity fail-close

Exemple :

```
hostname(config)# zonelabs-integrity fail-close
```

Étape 6 Rétablissez l'état d'échec configuré de la connexion des clients VPN à sa valeur par défaut et assurez-vous que les connexions des clients restent ouvertes.

zonelabs-integrity fail-open

Exemple :

```
hostname(config)# zonelabs-integrity fail-open
```

Étape 7 Précisez que le serveur Integrity se connecte au port 300 (la valeur par défaut est le port 80) de l'ASA pour demander le certificat SSL du serveur.

zonelabs-integrity ssl-certificate-port cert-port-number

Exemple :

```
hostname(config)# zonelabs-integrity ssl-certificate-port 300
```

Étape 8 Alors que le certificat SSL du serveur est toujours authentifié, spécifiez que le certificat SSL client du serveur Integrity doit être authentifié.

zonelabs-integrity ssl-client-authentication {enable | disable}

Exemple :

```
hostname(config)# zonelabs-integrity ssl-client-authentication enable
```

Définir le type de client de pare-feu sur Zone Labs

Procédure

	Commande ou action	Objectif
Étape 1	Pour définir le type de client pare-feu sur le type Zone Labs Integrity, saisissez la commande suivante : **Exemple :** `hostname(config)# client-firewall req zonelabs-integrity`	**client-firewall {opt | req} zonelabs-integrity**

Prochaine étape

Pour obtenir plus de renseignements, consultez Configurer les politiques de pare-feu des clients VPN, à la page 75. Les arguments de commande qui précisent les stratégies de pare-feu ne sont pas utilisés lorsque le type de pare-feu est **zonelabs-integrity**, car le serveur Integrity détermine ces stratégies.

Définir les paramètres de pare-feu client

Saisissez les commandes suivantes pour définir les paramètres de pare-feu client appropriés. Vous ne pouvez configurer qu'une seule instance de chaque commande. Pour obtenir plus de renseignements, consultez Configurer les politiques de pare-feu des clients VPN, à la page 75.

- Cisco Integrated Firewall

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-integrated
acl-in ACL acl-out ACL
```

- Cisco Security Agent

```
hostname(config-group-policy)# client-firewall {opt | req} cisco-security-agent
```

- Aucun pare-feu

```
hostname(config-group-policy)# client-firewall none
```

- Pare-feu personnalisé

```
hostname(config-group-policy)# client-firewall {opt | req} custom vendor-id num product-id
 num policy {AYT | CPP acl-in ACL acl-out ACL} [description string]
```

- Pare-feu de Zone Labs

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-integrity
```

Remarque Lorsque le type de pare-feu est **zonelabs-integrity**, n'incluez pas d'arguments. Le serveur d'intégrité de Zone Labs détermine les politiques.

```
hostname(config-group-policy)# client-firewall {opt | req} zonelabs-zonealarm
 policy {AYT | CPP acl-in ACL acl-out ACL}

hostname(config-group-policy)# client-firewall {opt | req}
zonelabs-zonealarmorpro policy {AYT | CPP acl-in ACL acl-out ACL}

client-firewall {opt | req} zonelabs-zonealarmpro policy {AYT | CPP acl-in
 ACL acl-out ACL}
```

- Pare-feu personnels Sygate

```
hostname(config-group-policy)# client-firewall {opt | req} sygate-personal

hostname(config-group-policy)# client-firewall {opt | req} sygate-personal-pro

hostname(config-group-policy)# client-firewall {opt | req} sygate-security-agent
```

- Network Ice, Black Ice Firewall

```
hostname(config-group-policy)# client-firewall {opt | req} networkice-blackice
```

Tableau 2 : Mots-clés et variables de commande client-firewall

Paramètre	Description
acl-in ACL	Fournit la politique utilisée par le client pour le trafic entrant.
acl-out ACL	Fournit la politique utilisée par le client pour le trafic sortant.
AYT	Spécifie que l'application de pare-feu du PC client contrôle la politique de pare-feu. L'ASA vérifie que le pare-feu est en cours d'exécution. Il demande : « Êtes-vous là ? ». S'il n'y a pas de réponse, l'ASA met fin au tunnel.
cisco-integrated	Spécifie le type de pare-feu intégré Cisco.
cisco-security-agent	Spécifie le type de pare-feu Cisco Intrusion Prevention Security Agent.
CPP	Spécifie la politique poussée comme source de la politique de pare-feu du client VPN.
custom	Spécifie le type de pare-feu personnalisé.
description string	Décrit le pare-feu.
networkice-blackice	Spécifie le type de pare-feu Network ICE Black ICE.

none (aucun)	Indique qu'il n'y a pas de politique de pare-feu client. Définit une politique de pare-feu avec une valeur nulle, interdisant ainsi une politique de pare-feu. Empêche d'hériter d'une politique de pare-feu d'une politique par défaut ou d'une stratégie de groupe précisée.
opt	Indique un type de pare-feu facultatif.
product-id	Identifie le produit de pare-feu.
req	Indique un type de pare-feu requis.
sygate-personal	Spécifie le type de pare-feu Sygate Personal.
sygate-personal-pro	Spécifie le type de pare-feu Sygate Personal Pro.
sygate-security-agent	Spécifie le type de pare-feu Sygate Security Agent.
vendor-id	Identifie le fournisseur de pare-feu.
zonelabs-integrity	Spécifie le type de pare-feu du serveur d'intégrité de Zone Labs Integrity.
zonelabs-zonealarm	Spécifie le type de pare-feu Zone Labs Zone Alarm.
zonelabs-zonealarmorpro policy	Spécifie le type de pare-feu Zone Labs Zone Alarm ou Pro.
zonelabs-zonealarmpro policy	Spécifie le type de pare-feu Zone Labs Zone Alarm Pro.

L'exemple suivant montre comment définir une politique de pare-feu client qui nécessite Cisco Intrusion Prevention Security Agent pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
hostname(config-group-policy)#
```

Configurer les règles d'accès client

Configurez des règles qui limitent les types et les versions de clients d'accès à distance pouvant se connecter par IPsec à travers l'ASA, à l'aide de la commande **client-access-rule** en mode de configuration group-policy. Élaborez les règles selon les lignes directrices suivantes :

- Si vous ne définissez aucune règle, l'ASA autorise tous les types de connexion.
- Lorsqu'un client ne correspond à aucune des règles, l'ASA refuse la connexion. Si vous définissez une règle de refus, vous devez également définir au moins une règle d'autorisation ; dans le cas contraire, l'ASA refuse toutes les connexions.
- Pour les clients logiciels comme matériels, le type et la version doivent correspondre exactement à ce qui apparaît dans l'affichage **show vpn-sessiondb remote**.
- Le caractère ***** est un caractère générique, que vous pouvez saisir plusieurs fois dans chaque règle. Par exemple, **client-access rule 3 deny type * version 3.*** crée une règle d'accès client de priorité 3 qui refuse tous les types de clients exécutant une version 3.x du logiciel.
- Vous pouvez élaborer un maximum de 25 règles par stratégie de groupe.

- Il y a une limite de 255 caractères pour un ensemble complet de règles.
- Vous pouvez saisir n/a pour les clients qui n'envoient ni type de client ni version.

Pour supprimer une règle, saisissez la forme **no** de cette commande. Cette commande équivaut à la commande suivante :

```
hostname(config-group-policy)# client-access-rule 1 deny type "Cisco VPN Client" version
4.0
```

Pour supprimer toutes les règles, saisissez **no client-access-rule command** sans arguments. Cela supprime toutes les règles configurées, y compris une règle nulle si vous en avez créé une en exécutant la commande **client-access-rule** avec le mot-clé **none** .

Par défaut, il n'y a aucune règle d'accès. En l'absence de règle d'accès client, les utilisateurs héritent de toutes les règles qui existent dans la stratégie de groupe par défaut.

Pour empêcher les utilisateurs d'hériter des règles d'accès client, entrez la commande **client-access-rule** avec le mot-clé **none** . Le résultat de cette commande est que tous les types et versions de clients peuvent se connecter.

```
hostname(config-group-policy)# client-access rule priority {permit | deny} type
type version {version | none}
```

```
hostname(config-group-policy)# no client-access rule [priority {permit | deny} type
 type version version]
```

Le tableau ci-dessous explique la signification des mots-clés et des paramètres dans ces commandes.

Tableau 3 : Mots-clés et variables de commande client-access rules

Paramètre	Description
deny	Refuse les connexions pour les périphériques d'un type et/ou d'une version particuliers.
none	N'autorise aucune restriction d'accès client. Définit la règle d'accès client à une valeur nulle, de sorte qu'aucune restriction n'est appliquée. Empêche d'hériter d'une valeur provenant d'une stratégie de groupe par défaut ou précisée.
permit	Autorise les connexions pour des périphériques d'un type ou d'une version particuliers.
priority	Détermine la priorité de la règle. La règle dont l'entier est le plus faible a la priorité la plus élevée. Par conséquent, la règle dont l'entier est le plus faible et qui correspond à un type ou à une version de client est celle qui s'applique. Si une règle de priorité inférieure est contradictoire, l'ASA l'ignore.
type *type*	Identifie les types de périphériques au moyen de chaînes de forme libre. La chaîne doit correspondre exactement à ce qui apparaît dans l'affichage **show vpn-sessiondb remote**, sauf que vous pouvez saisir le caractère * comme caractère générique.

Paramètre	Description
version version	Identifie la version du périphérique au moyen de chaînes de forme libre, par exemple 7.0. Une chaîne doit correspondre exactement à ce qui apparaît dans l'affichage **show vpn-sessiondb remote**, sauf que vous pouvez saisir le caractère * comme caractère générique.

L'exemple suivant montre comment créer des règles d'accès client pour la stratégie de groupe nommée FirstGroup. Ces règles autorisent les clients VPN Cisco exécutant la version 4.x du logiciel, tout en refusant tous les clients Windows NT :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 deny type WinNT version *
hostname(config-group-policy)# client-access-rule 2 permit "Cisco VPN Client"
version 4.*
```

Remarque Le champ « type » est une chaîne de forme libre qui accepte n'importe quelle valeur, mais cette valeur doit correspondre à la valeur fixe que le client envoie à l'ASA au moment de la connexion.

Configurer les attributs d'utilisateur

Cette section décrit les attributs d'utilisateur et comment les configurer.

Par défaut, les utilisateurs héritent de tous les attributs utilisateur de la stratégie de groupe attribuée. L'ASA vous permet également d'attribuer des attributs individuels au niveau de l'utilisateur, en remplaçant les valeurs de la stratégie de groupe qui s'applique à cet utilisateur. Par exemple, vous pouvez préciser une stratégie de groupe qui donne à tous les utilisateurs l'accès pendant les heures ouvrables, mais accorder à un utilisateur précis un accès 24 heures sur 24.

Afficher la configuration du nom d'utilisateur

Pour afficher la configuration pour tous les noms d'utilisateurs, y compris les valeurs par défaut héritées de la stratégie de groupe, saisissez le mot-clé **all** avec la commande **show running-config username**, comme suit :

```
hostname# show running-config all username
hostname#
```

Cette commande affiche le mot de passe chiffré et le niveau de privilège pour tous les utilisateurs ou, si vous fournissez un nom d'utilisateur, pour cet utilisateur précis. Si vous omettez le mot-clé **all** (tout), seules les valeurs explicitement configurées s'affichent dans cette liste. L'exemple suivant montre le résultat de cette commande pour l'utilisateur nommé testuser :

```
hostname# show running-config all username testuse
username testuser password 12RsxXQnphyr/I9Z encrypted privilege 15
```

Configurer les attributs pour les utilisateurs individuels

Pour configurer des utilisateurs spécifiques, vous attribuez un mot de passe (ou aucun mot de passe) et des attributs à un utilisateur à l'aide de la commande **username**, qui passe en mode nom d'utilisateur. Tous les attributs que vous ne spécifiez pas sont hérités de la stratégie de groupe.

La base de données d'authentification des utilisateurs internes est composée des utilisateurs saisis avec la commande **username**. La commande **login** utilise cette base de données pour l'authentification. Pour ajouter un utilisateur à la base de données ASA, saisissez la commande **username** en mode de configuration globale. Pour supprimer un utilisateur, utilisez la version **no** de cette commande avec le nom d'utilisateur que vous souhaitez supprimer. Pour supprimer tous les noms d'utilisateurs, utilisez la commande **clear configure username** sans ajouter de nom d'utilisateur.

Définir un mot de passe d'utilisateur et un niveau de privilège

Entrez la commande **username** pour attribuer un mot de passe et un niveau de privilège à un utilisateur. Vous pouvez saisir le mot-clé **nopassword** pour préciser que cet utilisateur ne nécessite pas de mot de passe. Si vous spécifiez un mot de passe, vous pouvez préciser si ce mot de passe est stocké sous une forme chiffrée.

Le mot-clé facultatif **privilege** vous permet de définir un niveau de privilège pour cet utilisateur. Les niveaux de privilège vont de 0 (le plus bas) à 15. Les administrateurs système ont généralement le niveau de privilège le plus élevé. La valeur par défaut est 2.

```
hostname(config)# username name {nopassword | password password [encrypted]}
[privilege priv_level]}
```

```
hostname(config)# no username [name]
```

Le tableau ci-dessous décrit la signification des mots-clés et des variables utilisés dans cette commande.

Mots-clés et variables de la commande username

Mot clé/variable	Signification
encrypted	Indique que le mot de passe est chiffré.
Nom	Nom de l'utilisateur.
nopassword	Indique que cet utilisateur n'a pas besoin de mot de passe.
password password	Indique que cet utilisateur possède un mot de passe et spécifie le mot de passe.
niveau de privilège	Définit le niveau de privilège pour cet utilisateur La plage est comprise entre 0 et 15, les nombres inférieurs ayant moins de capacité à utiliser des commandes et à gérer l'ASA. Le niveau de privilège par défaut est 2. Le niveau de privilège typique d'un administrateur système est de 15.

Par défaut, les utilisateurs VPN que vous ajoutez avec cette commande n'ont aucun attribut ni association de stratégie de groupe. Vous devez configurer toutes les valeurs explicitement.

L'exemple suivant montre comment configurer un utilisateur nommé anyuser avec un mot de passe chiffré de pw_12345678 et un niveau de privilège 12 :

```
hostname(config)# username anyuser password pw_12345678 encrypted privilege
```

```
 12
hostname(config)#
```

Configurer les attributs d'utilisateur

Après avoir configuré le mot de passe de l'utilisateur (le cas échéant) et le niveau de privilège de l'utilisateur, vous définissez les autres attributs. Celles-ci peuvent être dans n'importe quel ordre. Pour supprimer une paire attribut-valeur, saisissez la forme **no** de la commande.

Entrez en mode nom d'utilisateur en entrant la commande **username** avec le mot-clé **attributes** :

```
hostname(config)# username name attributes
hostname(config-username)#
```

L'invite change pour indiquer le nouveau mode. Vous pouvez maintenant configurer les attributs.

Configurer les attributs d'utilisateur VPN

Les attributs d'utilisateur VPN définissent des valeurs spécifiques aux connexions VPN, comme décrit dans les sections suivantes.

Configurer l'héritage

Vous pouvez permettre aux utilisateurs d'hériter de la stratégie de groupe des valeurs d'attributs que vous n'avez pas configurés au niveau du nom d'utilisateur. Pour préciser le nom de la stratégie de groupe dont cet utilisateur hérite les attributs, saisissez la commande **vpn-group-policy**. Par défaut, les utilisateurs VPN n'ont aucune association à une stratégie de groupe :

```
hostname(config-username)# vpn-group-policy group-policy-name
hostname(config-username)# no vpn-group-policy group-policy-name
```

Pour un attribut disponible en mode nom d'utilisateur, vous pouvez remplacer la valeur d'un attribut dans une stratégie de groupe pour un utilisateur particulier en le configurant en mode nom d'utilisateur.

L'exemple suivant montre comment configurer un utilisateur nommé anyuser pour utiliser les attributs de la stratégie de groupe nommée FirstGroup :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
hostname(config-username)#
```

Configurer les heures d'accès

Associez les heures pendant lesquelles cet utilisateur est autorisé à accéder au système en précisant le nom d'une politique de plage temporelle configurée :

Pour supprimer l'attribut de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cette option permet l'hérédité d'une valeur de plage temporelle d'une autre stratégie de groupe. Pour éviter d'hériter d'une valeur, entrez la commande **vpn-access-hours none**. La valeur par défaut est un accès non restreint.

```
hostname(config-username)# vpn-access-hours value {time-range | none}
```

```
hostname(config-username)# vpn-access-hours value none
hostname(config)#
```

L'exemple suivant montre comment associer l'utilisateur nommé anyuser à une politique de plage temporelle appelée 824 :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-access-hours 824
hostname(config-username)#
```

Configurer le nombre maximal de connexions simultanées

Simultaneous Logins Per User (connexions simultanées par utilisateur) : précise le nombre maximal de connexions simultanées autorisées pour cet utilisateur. La plage est comprise entre 0 et 2147483647. La valeur par défaut est de 3 connexions simultanées. Pour supprimer l'attribut de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Saisissez 0 pour désactiver la connexion et empêcher l'accès de l'utilisateur.

```
hostname(config-username)# vpn-simultaneous-logins integer
hostname(config-username)# no vpn-simultaneous-logins
hostname(config-username)# vpn-session-timeout alert-interval none
```

Remarque Bien que la limite maximale du nombre de connexions simultanées soit très élevée, en autoriser plusieurs peut compromettre la sécurité et affecter les performances.

L'exemple suivant montre comment autoriser un maximum de 4 connexions simultanées pour l'utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-simultaneous-logins 4
hostname(config-username)#
```

Configurer le délai d'inactivité

Procédure

Étape 1 (Facultatif) Pour configurer un délai d'inactivité du VPN, utilisez la commande **vpn-idle-timeout** *minutes* en mode de configuration de stratégie de groupe ou en mode de configuration de nom d'utilisateur.

S'il n'y a aucune activité de communication sur la connexion pendant cette période, l'ASA arrête la connexion. La durée minimale est de 1 minute, la durée maximale est de 35 791 394 minutes et la valeur par défaut est de 30 minutes.

L'exemple suivant montre comment définir un délai d'inactivité VPN de 15 minutes pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 15
```

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

Autres actions utilisant la commande [**no**] **vpn-idle-timeout** {*minutes* | **none**} :

- Saisissez **vpn-idle-timeout none** pour désactiver le délai d'inactivité du VPN et empêcher l'héritage d'une valeur de délai d'expiration.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout none
hostname(config-group-policy)#
```

  Il en résulte Secure Client (services client sécurisés) (SSL et IPsec/IKEv2) et un VPN sans client utilisant la valeur globale **default-idle-timeout** *secondes* webvpn. Cette commande est saisie en mode webvpn-config, par exemple : `hostnamee(config-webvpn)# default-idle-timeout 300`. La valeur par défaut est de 1800 secondes (30 min), la plage est comprise entre 60 et 86400 secondes.

  Pour toutes les connexions webvpn, la valeur **default-idle-timeout** est appliquée uniquement si **vpn-idle-timeout none** est défini dans l'attribut de stratégie de groupe/de nom d'utilisateur. Une valeur de délai d'inactivité non nulle est requise par l'ASA pour toutes les connexions Secure Client (services client sécurisés).

  Pour les VPN de site à site (IKEv1, IKEv2) et VPN d'accès à distance IKEv1, nous vous recommandons de désactiver le délai d'expiration et d'autoriser une période d'inactivité illimitée.

- Pour désactiver le délai d'inactivité pour cette stratégie de groupe ou cette politique d'utilisateur, saisissez **no vpn-idle-timeout**. La valeur sera héritée.
- Si vous ne définissez pas du tout **vpn-idle-timeout**, de toute façon, la valeur est héritée, qui est par défaut de 30 minutes.

Remarque
vpn-idle-timeout contrôle uniquement la durée maximale d'une session parente. Les sessions enfants (SSL/DTLS) sont terminées de manière dynamique beaucoup plus tôt par un délai d'inactivité TCP de 5 minutes codé en dur ou en cas d'échec de la vérification Dead Peer Detection (DPD) (3 tentatives). Pour plus de détails, consultez la note dans Configurer la détection d'homologue mort. Pour plus de détails sur les attributs DPD, keepalive et de temporisation, consultez Answer AnyConnect FAQ - Tunnels, DPD et minuterie d'inactivité.

Étape 2 (Facultatif) Vous pouvez éventuellement configurer l'heure à laquelle un message d'alerte de délai d'inactivité s'affiche à l'utilisateur à l'aide de la commande **vpn-idle-timeout alert-interval** {*minutes*} .

Ce message d'alerte indique aux utilisateurs le nombre de minutes qu'il leur reste jusqu'à ce que leur session VPN soit déconnectée pour cause d'inactivité. L'intervalle d'alerte par défaut est d'une minute.

L'exemple suivant montre comment définir un intervalle d'alerte de délai d'inactivité du VPN de 3 minutes pour l'utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout alert-interval 3
hostname(config-username)#
```

Autres actions utilisant la commande [**no**] **vpn-idle-timeout alert-interval** {*minutes* | **none**} :

- Le paramètre **none** indique que les utilisateurs ne recevront pas d'alerte.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-idle-timeout none
hostname(config-username)#
```

- Pour supprimer l'intervalle d'alerte de cette stratégie de groupe ou d'utilisateur, saisissez **no vpn-idle-timeout alert-interval**. La valeur sera héritée.
- Si vous ne définissez pas ce paramètre du tout, l'intervalle d'alerte par défaut est d'une minute.

Configurer la durée maximale de connexion

Procédure

Étape 1 (Facultatif) Configurez une durée maximale pour les connexions VPN en utilisant la commande **vpn-session-timeout** {*minutes* dans le mode de configuration de stratégie de groupe ou dans le mode de configuration du nom d'utilisateur.

La durée minimale est de 1 minute et la durée maximale est de 35 791 394 minutes. Il n'y a pas de valeur par défaut. À la fin de cette période, l'ASA met fin à la connexion.

L'exemple suivant montre comment définir un délai d'expiration de session VPN de 180 minutes pour la stratégie de groupe nommée FirstGroup :

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
hostname(config-group-policy)#
```

L'exemple suivant montre comment définir un délai d'expiration de session VPN de 180 minutes pour l'utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-session-timeout 180
hostname(config-username)#
```

Autres actions utilisant la commande [**no**] **vpn-session-timeout** {*minutes* | **none**} :

- Pour supprimer l'attribut de cette stratégie et autoriser l'héritage, saisissez la forme **no vpn-session-timeout** de cette commande.
- Pour autoriser un délai d'expiration illimité et ainsi empêcher l'héritage d'une valeur de délai d'expiration, saisissez **vpn-session-timeout none**.

Étape 2 Configurez le moment où un message d'alerte d'expiration de session s'affiche à l'utilisateur au moyen de la commande **vpn-session-timeout alert-interval** {*minutes* | } .

Ce message d'alerte indique aux utilisateurs le nombre de minutes restantes avant la déconnexion automatique de leur session VPN. L'exemple suivant montre comment spécifier que les utilisateurs seront informés 20 minutes avant la déconnexion de leur session VPN. Vous pouvez spécifier une plage de 1 à 30 minutes.

```
hostname(config-webvpn)# vpn-session-timeout alert-interval 20
```

Autres actions utilisant la commande [**no**] **vpn-session-timeout alert-interval** {*minutes* | **none**} :

- Utilisez la forme no de la commande pour indiquer que l'attribut d'intervalle d'alerte du délai d'expiration de la session VPN sera hérité de la stratégie de groupe par défaut :

```
hostname(config-webvpn)# no vpn-session-timeout alert-interval
```

- Le **vpn-session-timeout alert-interval none** indique que les utilisateurs ne recevront pas d'alerte.

Appliquer un filtre ACL

Précisez le nom d'une liste de contrôle d'accès spécifique à l'utilisateur configurée précédemment à utiliser comme filtre pour les connexions VPN. Pour ignorer une liste de contrôle d'accès et empêcher d'hériter d'une liste de contrôle d'accès de la stratégie de groupe, saisissez la commande **vpn-filter** avec le mot-clé none. Pour supprimer la liste de contrôle d'accès, y compris une valeur nulle créée en saisissant la commande **vpn-filter none**, utilisez la forme **no** de cette commande. L'option **no** permet l'héritage d'une valeur à partir de la stratégie de groupe. Il n'y a pas de comportement ou de valeur par défaut pour cette commande.

Vous configurez les listes de contrôle d'accès pour autoriser ou refuser différents types de trafic pour cet utilisateur. Notez que le filtre VPN s'applique aux connexions initiales uniquement. Il ne s'applique pas aux connexions secondaires, comme une connexion de support SIP, qui sont ouvertes en raison de l'action de l'inspection d'application. Vous utilisez ensuite la commande **vpn-filter** pour appliquer ces listes de contrôle d'accès.

```
hostname(config-username)# vpn-filter {value ACL_name | none}
hostname(config-username)# no vpn-filter
hostname(config-username)#
```

Remarque Le VPN SSL sans client n'utilise pas les listes de contrôle d'accès définies dans la commande **vpn-filter**.

L'exemple suivant montre comment définir un filtre qui invoque une liste de contrôle d'accès nommée acl_vpn pour l'utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-filter value acl_vpn
hostname(config-username)#
```

Préciser l'adresse IPv4 et le masque réseau

Précisez l'adresse IP et le masque réseau à affecter à un utilisateur particulier. Pour supprimer l'adresse IP, saisissez la forme **no** de cette commande.

```
hostname(config-username)# vpn-framed-ip-address {ip_address}
hostname(config-username)# no vpn-framed-ip-address
hostname(config-username)
```

L'exemple suivant montre comment définir l'adresse IP 10.92.166.7 pour un utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-address 10.92.166.7
hostname(config-username)
```

Précisez le masque réseau à utiliser avec l'adresse IP spécifiée à l'étape précédente. Si vous avez utilisé la commande **no vpn-framed-ip-address**, ne spécifiez pas de masque réseau. Pour supprimer le masque de sous-réseau, saisissez la forme **no** de cette commande. Aucun comportement ni valeur par défaut.

```
hostname(config-username)# vpn-framed-ip-netmask {netmask}
hostname(config-username)# no vpn-framed-ip-netmask
hostname(config-username)
```

L'exemple suivant montre comment définir un masque de sous-réseau de 255.255.255. 254 pour un utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-netmask 255.255.255.254
hostname(config-username)
```

Préciser l'adresse IPv6 et le masque réseau

Précisez l'adresse IPv6 et le masque de sous-réseau à attribuer à un utilisateur particulier. Pour supprimer l'adresse IP, saisissez la forme **no** de cette commande.

```
hostname(config-username)# vpn-framed-ipv6-address {ip_address}
hostname(config-username)# no vpn-framed-ipv6-address
hostname(config-username)
```

L'exemple suivant montre comment définir l'adresse IP et le masque de sous-réseau 2001::3000:1000:2000:1/64 pour un utilisateur nommé anyuser. Cette adresse indique une valeur de préfixe de 2001:0000:0000:0000 et un ID d'interface 3000:1000:2000:1.

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ipv6-address 2001::3000:1000:2000:1/64
hostname(config-username)
```

Préciser le protocole de tunnel

Précisez les types de tunnels VPN (IPsec ou VPN SSL sans client) que cet utilisateur peut utiliser. La valeur par défaut est extraite de la stratégie de groupe par défaut, dont la valeur par défaut est IPsec. Pour supprimer l'attribut de la configuration en cours d'exécution, saisissez la forme **no** de cette commande.

```
hostname(config-username)# vpn-tunnel-protocol {webvpn | IPsec}
hostname(config-username)# no vpn-tunnel-protocol [webvpn | IPsec]
hostname(config-username)
```

Les valeurs des paramètres pour cette commande sont les suivantes :

- **IPsec—**Négocie un tunnel IPsec entre deux homologues (un client d'accès à distance ou une autre passerelle sécurisée). Crée des associations de sécurité qui régissent l'authentification, le chiffrement, l'encapsulation et la gestion des clés.
- **webvpn—**Fournit un accès VPN SSL sans client aux utilisateurs distants par l'intermédiaire d'un navigateur Web compatible avec le protocole HTTPS et ne nécessite pas de client.

Entrez cette commande pour configurer un ou plusieurs modes de tunnelisation. Au moins un mode de tunnelisation doit être configuré pour que les utilisateurs puissent se connecter sur un tunnel VPN.

L'exemple suivant montre comment configurer les modes de tunnelisation VPN SSL et IPsec sans client pour l'utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-tunnel-protocol webvpn
hostname(config-username)# vpn-tunnel-protocol IPsec
hostname(config-username)
```

Restreindre l'accès des utilisateurs distants

Configurez cet attribut **group-lock** avec le mot-clé **value** afin de restreindre les utilisateurs distants à un accès uniquement par le profil de connexion préexistant spécifié. Le verrouillage de groupe restreint les utilisateurs en vérifiant si le groupe configuré dans le client VPN est le même que le profil de connexion auquel l'utilisateur est affecté. Si ce n'est pas le cas, l'ASA empêche l'utilisateur de se connecter. Si vous ne configurez pas group-lock, l'ASA authentifie les utilisateurs sans tenir compte du groupe attribué.

Pour supprimer l'attribut **group-lock** de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cette option permet l'héritage d'une valeur à partir de la stratégie de groupe. Pour désactiver le verrouillage de groupe et pour éviter d'hériter d'une valeur de verrouillage de groupe d'une stratégie de groupe par défaut ou d'une stratégie de groupe spécifiée, saisissez la commande **group-lock** avec le mot-clé **none** .

```
hostname(config-username)# group-lock {value tunnel-grp-name | none}
hostname(config-username)# no group-lock
hostname(config-username)
```

L'exemple suivant montre comment définir le verrouillage de groupe pour l'utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# group-lock value tunnel-group-name
hostname(config-username)
```

Activer le stockage des mots de passe pour les utilisateurs de clients logiciels

Précisez s'il faut autoriser les utilisateurs à stocker leurs mots de passe de connexion sur le système client. Le stockage de mot de passe est désactivé par défaut. Activez le stockage des mots de passe uniquement sur les systèmes que vous savez se trouver dans des sites sécurisés. Pour désactiver le stockage de mot de passe, entrez la commande **password-storage** avec le mot-clé **disable** . Pour supprimer l'attribut de stockage de mot de passe de la configuration en cours d'exécution, saisissez la forme **no** de cette commande. Cela permet l'héritage d'une valeur pour le stockage de mots de passe de la stratégie de groupe.

```
hostname(config-username)# password-storage {enable | disable}
hostname(config-username)# no password-storage
hostname(config-username)
```

Cette commande n'a aucune incidence sur l'authentification client matériel interactive ou l'authentification d'utilisateur individuel pour les clients de matériel.

L'exemple suivant montre comment activer le stockage de mot de passe pour l'utilisateur nommé anyuser :

```
hostname(config)# username anyuser attributes
hostname(config-username)# password-storage enable
```

```
hostname(config-username)
```

Bonnes pratiques pour la configuration et l'ajustement de l'ACL du filtre de VPN

Cette section présente les bonnes pratiques à suivre lors de la mise à jour d'une liste de contrôle d'accès de filtre de VPN existante sans interrompre le trafic.

Mise à jour d'une liste de contrôle d'accès de filtre VPN existante

Suivez ces étapes lorsque vous souhaitez mettre à jour une liste de contrôle d'accès de filtre vpn appliquée sur l'périphérique ASA :

1. Créez une nouvelle liste de contrôle d'accès vpn-filter sur votre système (exemple : *new_acl.txt*).
2. Téléchargez l'ACL vpn-filter actuelle à partir du périphérique (exemple : *old_acl.txt*).
3. Créez des instructions de modification pour l'ACL :

```
* Add update in-progress to ACL remark
echo ?access-list <name> line 1 ACL update in-progress? > push.txt
* Delete old rules
sed ?s/^/no /g? old.acl >> push.txt
 * Add new rules
cat new.acl >> push.txt
 * Remove update in-progress to ACL remark
echo ?no access-list <name> ACL update in-progress? >> push.txt
```

4. Chargez le fichier push.txt sur l'périphérique.

Remplacement d'une liste de contrôle d'accès de filtre VPN existante par une nouvelle

Suivez les étapes suivantes pour remplacer la liste de contrôle d'accès vpn-filter appliquée sur l'périphérique ASA :

1. Créez une nouvelle liste de contrôle d'accès vpn-filter chaque fois que vous souhaitez en remplacer une existante.
2. Mettez à jour la stratégie de groupe avec l'ACL vpn-filter.
3. Supprimez l'ancienne liste de contrôle d'accès vpn-filter appliquée sur le périphérique.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.