Connexions du client VPN AnyConnect

Cette section décrit comment configurer les connexions client VPN AnyConnect.

À propos du client VPN Secure Client (services client sécurisés)

Le Secure Client (services client sécurisés) fournit aux utilisateurs distants des connexions SSL et IPsec/IKEv2 sécurisées vers l'ASA. Sans client déjà installé, les utilisateurs distants saisissent dans leur navigateur l'adresse IP d'une interface configurée pour accepter les connexions VPN SSL ou IPsec/IKEv2. À moins que l'ASA ne soit configuré pour rediriger les requêtes http:// vers https://, les utilisateurs doivent saisir l'URL sous la forme https://*adresse*.

Une fois que l'utilisateur a saisi l'URL, le navigateur se connecte à cette interface et affiche l'écran de connexion. Si l'utilisateur satisfait aux exigences de connexion et d'authentification, et que l'ASA détermine que cet utilisateur a besoin du client, il télécharge le client correspondant au système d'exploitation de l'ordinateur distant. Après le téléchargement, le client s'installe et se configure, établit une connexion sécurisée SSL ou IPsec/IKEv2, puis soit demeure installé, soit se désinstalle, selon la configuration, lorsque la connexion se termine.

Dans le cas d'un client déjà installé, lorsque l'utilisateur s'authentifie, l'ASA vérifie la version du client et le met à niveau au besoin.

Lorsque le client négocie une connexion VPN SSL avec l'ASA, il se connecte en utilisant le protocole Transport Layer Security (TLS) et, éventuellement, Datagram Transport Layer Security (DTLS). L'utilisation de DTLS évite les problèmes de latence et de bande passante associés à certaines connexions SSL et améliore la performance des applications en temps réel sensibles aux retards de paquets.

Le Secure Client (services client sécurisés) peut être téléchargé depuis l'ASA, ou installé manuellement sur le PC distant par l'administrateur système. Pour plus d'informations sur l'installation manuelle du client, consultez la version appropriée du Guide de configuration de la solution de mobilité sécurisée Cisco AnyConnect .

L'ASA télécharge le client en fonction de la stratégie de groupe ou des attributs de nom d'utilisateur de l'utilisateur établissant la connexion. Vous pouvez configurer l'ASA pour télécharger automatiquement le client, ou pour demander à l'utilisateur distant s'il souhaite télécharger le client. Dans ce dernier cas, si l'utilisateur ne répond pas, vous pouvez configurer l'ASA pour télécharger le client après un délai d'expiration ou présenter la page de connexion.

Exigences pour Secure Client (services client sécurisés)

Pour les exigences des ordinateurs terminaux exécutant Secure Client (services client sécurisés), consultez la version appropriée des notes de version de solution de mobilité sécurisée Cisco AnyConnect.

Lignes directrices et limites pour Secure Client (services client sécurisés)

- L'ASA ne vérifie pas les certificats HTTPS distants.
- Pris en charge en mode contexte unique ou multiple. Une licence AnyConnect Apex est requise pour le VPN d'accès à distance en mode multi-contexte. Bien que l'ASA ne reconnaisse pas expressément une licence AnyConnect Apex, il applique les caractéristiques d'une licence Apex, comme AnyConnect Premium sous licence jusqu'à la limite de la plateforme, Secure Client (services client sécurisés) pour les périphériques mobiles, Secure Client (services client sécurisés) pour le téléphone VPN Cisco et pour l'évaluation avancée des postes clients. Les licences partagées, AnyConnect Essentials, l'agrégation de licences de basculement et les licences flex ou à durée déterminée ne sont pas prises en charge.
- L'émission de commandes telles que **curl** sur la tête de réseau du VPN d'accès à distance n'est pas directement prise en charge et pourrait ne pas donner les résultats souhaitables. Par exemple, la tête de réseau ne répond pas aux requêtes HTTP HEAD.
- Lorsque des téléphones VPN matériels, comme ceux de la série Cisco 88xx, utilisent Secure Client (services client sécurisés), ils peuvent subir une reconnexion malgré l'activation de DTLS et la configuration de Dead Peer Detection (DPD).
- Lorsqu'un client se connecte à Secure Client (services client sécurisés), son adresse IP change avant et après la connexion. L'ASA prend en charge ce comportement.

Exigences de licence pour Secure Client (services client sécurisés)

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

Les licences VPN d'accès à distance nécessitent une licence AnyConnect Plus ou Apex, disponible séparément. Consultez les licences pour fonctionnalités de la gamme Cisco ASA pour connaître les valeurs maximales par modèle.

Si vous démarrez une session SSL VPN sans client, puis démarrez la session Secure Client (services client sécurisés) à partir du portail, une session est utilisée au total. Cependant, si vous démarrez d'abord le Secure Client (services client sécurisés) (à partir d'un client autonome, par exemple), puis que vous vous connectez au portail SSL VPN sans client, deux sessions sont utilisées.

Configurer les connexions pour Secure Client (services client sécurisés)

Cette section décrit les conditions préalables, les restrictions et les tâches détaillées pour configurer l'ASA afin qu'il accepte les connexions des clients VPN AnyConnect.

Configurer l'ASA pour déployer le client via le Web

Cette section décrit les étapes permettant de configurer l'ASA pour le déploiement Web de Secure Client (services client sécurisés).

Avant de commencer

Copiez le paquet d'image client dans l'ASA à l'aide de TFTP ou d'une autre méthode.

Remarque Même si la fonctionnalité VPN sans client est désactivée sur l'ASA, lorsque vous utilisez un navigateur Web pour accéder au déploiement Web d'AnyConnect (https://x.x.x.x<ASA IP address>), la session VPN sur l'ASA est comptabilisée comme une session sans client.

Procédure

Étape 1 Identifiez un fichier sur la mémoire flash comme le fichier de paquet Secure Client (services client sécurisés).

L'ASA décompresse le fichier dans la mémoire cache pour le télécharger sur des PC distants. Si vous avez plusieurs clients, attribuez un ordre aux images client avec l'argument d'ordre.

L'ASA télécharge des parties de chaque client dans l'ordre que vous spécifiez jusqu'à ce qu'il corresponde au système d'exploitation du PC distant. Par conséquent, attribuez le numéro le plus bas à l'image utilisée par le système d'exploitation le plus souvent rencontré.

anyconnect image *filename order*

Exemple :

```
hostname(config-webvpn)# anyconnect image
anyconnect-win-2.3.0254-k9.pkg 1
hostname(config-webvpn)# anyconnect image
anyconnect-macosx-i386-2.3.0254-k9.pkg 2
hostname(config-webvpn)# anyconnect image
anyconnect-linux-2.3.0254-k9.pkg 3
```

Remarque
Vous devez émettre la commande **AnyConnect enable** après avoir configuré les images Secure Client (services client sécurisés) avec la commande **AnyConnect image**. Si vous n'activez pas Secure Client (services client sécurisés), il ne fonctionnera pas comme prévu, et la commande **show webvpn anyconnect** considérera le client VPN SSL comme non activé au lieu de répertorier les paquets Secure Client (services client sécurisés) installés.

Étape 2 Activez SSL sur une interface pour les connexions sans client ou Secure Client (services client sécurisés) SSL.

enable *interface*

Exemple :

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

Étape 3 Sans l'exécution de cette commande, Secure Client (services client sécurisés) ne fonctionne pas comme prévu, et une commande **show webvpn anyconnect** renvoie que « le VPN SSL n'est pas activé » au lieu de répertorier les paquets Secure Client (services client sécurisés) installés.

anyconnect enable

Étape 4 (Facultatif) Créez un ensemble d'adresses IP. Vous pouvez utiliser une autre méthode d'affectation d'adresses, telle que DHCP et/ou l'adressage attribué par l'utilisateur.

ip local pool *poolname startaddr-endaddr* **mask** *mask*

Exemple :

```
hostname(config)# ip local pool vpn_users 209.165.200.225-209.165.200.254
mask 255.255.255.224
```

Étape 5 Attribuez un ensemble d'adresses à un groupe de tunnels.

address-pool *poolname*

Exemple :

```
hostname(config)# tunnel-group telecommuters general-attributes
hostname(config-tunnel-general)# address-pool vpn_users
```

Étape 6 Attribuez une stratégie de groupe par défaut au groupe de tunnels.

default-group-policy *name*

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

Étape 7 Activez l'affichage de la liste des groupes de tunnels sur le portail sans client et la page de connexion de l'interface graphique Secure Client (services client sécurisés). La liste des alias est définie par la commande *group-alias name enable*.

group-alias *name* **enable**

Exemple :

```
hostname(config)# tunnel-group telecommuters webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias sales_department enable
```

Étape 8 Précisez Secure Client (services client sécurisés) comme protocole de tunnelisation VPN autorisé pour le groupe ou l'utilisateur.

tunnel-group-list enable

Exemple :

```
hostname(config)# webvpn
hostname(config-webvpn)# tunnel-group-list enable
```

Étape 9 Précisez SSL comme protocole de tunnelisation VPN autorisé pour le groupe ou l'utilisateur. Vous pouvez également spécifier des protocoles supplémentaires. Pour de plus amples informations, consultez la commande vpn-tunnel-protocol dans la référence de commande.

vpn-tunnel-protocol

Exemple :

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

Prochaine étape

Pour en savoir plus sur l'affectation d'utilisateurs aux stratégies de groupe, consultez le chapitre 6, Configuration des profils de connexion, des stratégies de groupe et des utilisateurs.

Activer l'installation permanente du client

L'activation de l'installation permanente du client désactive la fonction de désinstallation automatique du client. Le client reste installé sur l'ordinateur distant pour les connexions ultérieures, ce qui réduit le temps de connexion pour l'utilisateur distant.

Pour activer l'installation permanente du client pour un groupe ou un utilisateur spécifique, utilisez la commande anyconnect keep-installer à partir des modes de stratégie de groupe ou de nom d'utilisateur webvpn.

La valeur par défaut est que l'installation permanente du client est activée. Le client reste sur l'ordinateur distant à la fin de la session. L'exemple suivant configure la stratégie de groupe existante *sales* pour supprimer le client sur l'ordinateur distant à la fin de la session :

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-policy)# anyconnect keep-installer installed none
```

Configurer DTLS

Datagram Transport Layer Security (DTLS) permet à Secure Client (services client sécurisés) d'établir une connexion VPN SSL pour utiliser deux tunnels simultanés : un tunnel SSL et un tunnel DTLS. L'utilisation de DTLS évite les problèmes de latence et de bande passante associés aux connexions SSL et améliore la performance des applications en temps réel sensibles aux retards de paquets.

Avant de commencer

Consultez Configurer les paramètres avancés SSL pour configurer DTLS sur cette tête de réseau et quelle version de DTLS est utilisée.

Pour que DTLS passe à une connexion TLS, la détection d'homologue mort (DPD) doit être activée. Si vous n'activez pas DPD et que la connexion DTLS rencontre un problème, la connexion se termine au lieu de revenir à TLS. Pour en savoir plus sur DPD, consultez Configurer, à la page 17.

Procédure

Étape 1 Précisez les options DTLS pour les connexions VPN Secure Client (services client sécurisés) :

a) Activez SSL et DTLS sur l'interface en mode webvpn.

Par défaut, DTLS est activé lorsque l'accès VPN SSL est activé sur une interface.

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

Désactivez DTLS pour tous les utilisateurs Secure Client (services client sécurisés) avec la commande **enable** *interface* **tls-only** en mode de configuration webvpn.

Si vous désactivez DTLS, les connexions VPN SSL se connectent uniquement à l'aide d'un tunnel SSL.

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside tls-only
```

b) Configurez les ports pour SSL et DTLS à l'aide des commandes **port** et **dtls port** .

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
hostname(config-webvpn)# port 555
hostname(config-webvpn)# dtls port 556
```

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

a) Activez DTLS pour des groupes ou des utilisateurs spécifiques avec la commande **anyconnect ssl dtls** en mode de configuration de stratégie de groupe webvpn ou de nom d'utilisateur webvpn.

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect ssl dtls enable
```

b) Si vous le souhaitez, activez la compression DTLS à l'aide de la commande AnyConnect dtls compression.

```
hostname(config-group-webvpn)# anyconnect dtls compression lzs
```

Inviter les utilisateurs distants

Procédure

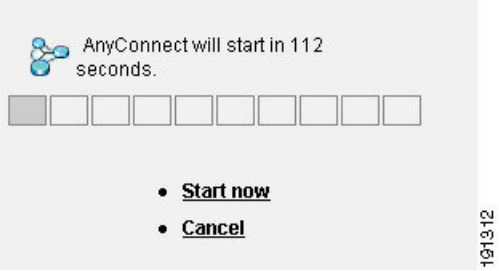
Vous pouvez activer l'ASA afin qu'il invite les utilisateurs distants du client VPN SSL à télécharger le client à l'aide de la commande **anyconnect ask** depuis les modes de configuration webvpn de stratégie de groupe ou de nom d'utilisateur :

[**no**] **anyconnect ask** {**none** | **enable** [**default** {**webvpn** | } **timeout** *value*]}

- **anyconnect enable**invite l'utilisateur distant à télécharger le client ou à accéder à la page du portail sans client et attend indéfiniment la réponse de l'utilisateur.
- **anyconnect ask enable default** télécharge immédiatement le client.
- **anyconnect ask enable default webvpn** passe immédiatement à la page du portail.
- La valeur **anyconnect ask enable default timeout** invite l'utilisateur distant à télécharger le client ou à accéder à la page du portail sans client et attend la durée de *value (valeur)* avant d'entreprendre l'action par défaut : télécharger le client.
- La valeur **anyconnect ask enable default clientless timeout** invite l'utilisateur distant à télécharger le client ou à accéder à la page du portail sans client et attend la durée de *value (valeur)* avant d'entreprendre l'action par défaut : afficher la page du portail sans client.

La figure ci-dessous montre l'invite affichée aux utilisateurs distants lorsque la valeur **default anyconnect timeout** *ou la valeur***default webvpn timeout** est configurée :

Illustration 1 : Invite affichée pour les utilisateurs distants pour le téléchargement du client VPN SSL



Exemple

L'exemple suivant configure l'ASA pour inviter l'utilisateur à télécharger le client ou à se rendre à la page du portail sans client et à attendre *10 secondes pour obtenir une réponse* avant de télécharger le client :

```
hostname(config-group-webvpn)# anyconnect ask enable default anyconnect timeout
 10
```

Activer le téléchargement du profil Secure Client (services client sécurisés)

Vous activez les fonctionnalités Secure Client (services client sécurisés) dans les profils Secure Client (services client sécurisés), fichiers XML qui contiennent les paramètres de configuration pour le client principal avec sa fonctionnalité VPN et pour les modules clients facultatifs. L'ASA déploie les profils pendant l'installation et les mises à jour de Secure Client (services client sécurisés). Les utilisateurs ne peuvent pas gérer ou modifier les profils.

Le fichier téléchargé sur le client est du format : <*profile_name*>.xml.

Vous pouvez configurer un profil à l'aide de l'éditeur de profils Secure Client (services client sécurisés), un outil de configuration graphique pratique lancé par ASDM ou ISE. Le paquet de logiciels Secure Client (services client sécurisés) pour Windows comprend l'éditeur, qui s'active lorsque vous chargez le paquet

client sur le périphérique headend choisi et que vous le spécifiez comme image Secure Client (services client sécurisés).

Nous fournissons également une version autonome de l'éditeur de profils pour Windows que vous pouvez utiliser comme solution de rechange à l'éditeur de profils intégré à ASDM ou ISE. Si vous prédéployez le client, vous pouvez utiliser l'éditeur de profil autonome pour créer des profils pour le service VPN et d'autres modules que vous déployez sur les ordinateurs à l'aide de votre système de gestion de logiciels.

Pour en savoir plus sur Secure Client (services client sécurisés) et son éditeur de profils, consultez la version appropriée du Guide de configuration de la solution de mobilité sécurisée Cisco AnyConnect .

Remarque Le protocole Secure Client (services client sécurisés) est SSL par défaut. Pour activer IPsec IKEv2, vous devez configurer les paramètres IKEv2 sur l'ASA et configurer IKEv2 comme protocole principal dans le profil client. Le profil compatible IKEv2 doit être déployé sur l'ordinateur terminal ; sinon, le client tente de se connecter à l'aide de SSL.

Procédure

Étape 1 Utilisez l'éditeur de profil d'ASDM/ISE ou l'éditeur de profil autonome pour créer un profil.

Étape 2 Chargez le fichier de profil dans la mémoire flash sur l'ASA à l'aide de tftp ou toute autre méthode.

Étape 3 Utilisez la commande **anyconnect profiles** à partir du mode de configuration webvpn pour identifier le fichier en tant que profil client à charger dans la mémoire cache.

Exemple :

L'exemple suivant spécifie les fichiers sales_hosts.xml et engineering_hosts.xml en tant que profils :

```
asa1(config-webvpn)# anyconnect profiles sales
disk0:/sales_hosts.xml
asa1(config-webvpn)# anyconnect profiles engineering
disk0:/engineering_hosts.xml
```

Les profils sont maintenant disponibles pour les stratégies de groupe.

Affichez les profils chargés dans la mémoire cache à l'aide de la commande **dir cache:stc/profiles** :

```
hostname(config-webvpn)# dir cache:/stc/profiles

Directory of cache:stc/profiles/

0      ----  774         11:54:41 Nov 22 2006  engineering.xml
0      ----  774         11:54:29 Nov 22 2006  sales.xml

2428928 bytes total (18219008 bytes free)
hostname(config-webvpn)#
```

Étape 4 Entrez le mode de configuration webvpn de la stratégie de groupe et spécifiez un profil client pour une stratégie de groupe avec la commande **anyconnect profiles** :

Exemple :

Vous pouvez saisir la commande client profiles value suivie d'un point d'interrogation (**?**) pour afficher les profils disponibles. Par exemple :

```
asa1(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages: engineering sales
```

L'exemple suivant configure la stratégie de groupe pour utiliser le profil *sales* avec le type de profil client *vpn* :

```
asa1(config-group-webvpn)# anyconnect profiles value sales type vpn
asa1(config-group-webvpn)#
```

Activer la mise à niveau différée Secure Client (services client sécurisés)

La mise à niveau différée permet à l'utilisateur Secure Client (services client sécurisés) de retarder le téléchargement de la mise à niveau du client. Lorsqu'une mise à jour de client est disponible, Secure Client (services client sécurisés) ouvre une boîte de dialogue demandant à l'utilisateur s'il souhaite effectuer la mise à jour ou reporter la mise à niveau. Cette boîte de dialogue de mise à niveau ne s'affichera pas, sauf si AutoUpdate est défini sur *Enabled* (Activé) dans le paramètre de profil Secure Client (services client sécurisés).

La mise à niveau différée est activée en ajoutant des types d'attributs personnalisés et des valeurs nommées à l'ASA ; ensuite, référencez et configurez ces attributs dans une stratégie de groupe.

Les attributs personnalisés suivants prennent en charge la mise à niveau différée :

Tableau 1 : Attributs personnalisés pour la mise à niveau différée

Type d'attribut personnalisé	Valeurs valides :	Valeur par défaut	Notes
DeferredUpdateAllowed	true false	faux	La valeur true active la mise à jour différée. Si la mise à jour différée est désactivée (false), les paramètres ci-dessous sont ignorés.
DeferredUpdateMinimumVersion	x.y.z	0.0.0	Version minimale de Secure Client (services client sécurisés) à installer pour que les mises à jour soient reportables. La vérification de version minimale s'applique à tous les modules activés sur la tête de réseau. Si un module activé (y compris le VPN) n'est pas installé ou ne répond pas à la version minimale, la connexion n'est pas admissible pour une mise à jour retardée. Si cet attribut n'est pas spécifié, une invite de report s'affiche (ou est rejetée automatiquement), quelle que soit la version installée sur le terminal.

Type d'attribut personnalisé	Valeurs valides :	Valeur par défaut	Notes
DeferredUpdateDismissTimeout	0-300 (secondes)	none (Aucun) (désactivé)	Nombre de secondes pendant lesquelles l'invite de mise à niveau retardée s'affiche avant d'être rejetée automatiquement. Cet attribut s'applique uniquement lorsqu'une invite de mise à jour retardée doit s'afficher (l'attribut de version minimale est évalué en premier). Si cet attribut est manquant, la fonctionnalité de suppression automatique est désactivée et une boîte de dialogue s'affiche (le cas échéant) jusqu'à ce que l'utilisateur réponde. La définition de cet attribut à zéro permet de forcer le report ou la mise à niveau automatique en fonction des éléments suivants : • La version installée et la valeur de DeferredUpdateMinimumVersion. • La valeur de DeferredUpdateDismissResponse.
DeferredUpdateDismissResponse	mise à jour reportée	mettre à jour	Action à effectuer lorsque DeferredUpdateDismissTimeout se produit.

Procédure

Étape 1 Créez les types d'attributs personnalisés avec la commande **anyconnnect-custom-attr** en mode de configuration webvpn :

[**no**] **AnyConnect-custom-attr** *attr-type* [**description** *description*]

Exemple :

L'exemple suivant montre comment ajouter les types d'attributs personnalisés DeferredUpdateAllowed et DeferredUpdateDismissTimeout :

```
hostame(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed
description Indicates if the deferred update feature is enabled or not
hostame(config-webvpn)# anyconnect-custom-attr DeferredUpdateDismissTimeout
```

Étape 2 Ajoutez des valeurs nommées pour les attributs personnalisés avec la commande **anyconnect-custom-data** en mode de configuration globale. Pour les attributs avec des valeurs longues, vous pouvez fournir une entrée en double qui permet la concaténation. Cependant, avec une entrée de configuration en double, la boîte de dialogue de mise à niveau ne s'affiche pas, et un utilisateur ne peut pas reporter la mise à niveau ; au lieu de cela, la mise à niveau se produit automatiquement.

[**no**] **AnyConnect-custom-data** *attr-type attr-name attr-value*

Exemple :

L'exemple suivant montre comment ajouter une valeur nommée pour le type d'attribut personnalisé DeferredUpdateDismissTimeout et pour l'activation de DeferredUpdateAllowed :

```
hostname(config)# anyconnect-custom-data DeferredUpdateDismissTimeout
def-timeout 150
hostname(config)# anyconnect-custom-data DeferredUpdateAllowed
def-allowed true
```

Étape 3 Ajoutez ou supprimez les valeurs nommées d'attribut personnalisé à une stratégie de groupe à l'aide de la commande **anyconnect-custom** :

- **anyconnect-custom** *attr-type* **value** *attr-name*
- **anyconnect-custom** *attr-type* **none**
- **no anyconnect-custom** *attr-type*

Exemple :

L'exemple suivant montre comment activer la mise à jour retardée pour la stratégie de groupe nommée sales et définir le délai d'expiration à 150 secondes :

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# anyconnect-custom DeferredUpdateAllowed
value def-allowed
hostname(config-group-policy)# anyconnect-custom DeferredUpdateDismissTimeout
value def-timeout
```

Activer la conservation DSCP

En définissant un autre attribut personnalisé, vous pouvez contrôler le point de code de services différenciés (DSCP) sur les plateformes Windows ou OS X pour les connexions DTLS uniquement. L'activation de la conservation DSCP permet aux périphériques de hiérarchiser le trafic sensible à la latence ; le routeur tient compte de ce paramètre et marque le trafic prioritaire afin d'améliorer la qualité de la connexion sortante.

Procédure

Étape 1 Créez les types d'attributs personnalisés avec la commande **anyconnect-custom-attr** en mode de configuration webvpn :

[no] anyconnect-custom-attr DSCPPreservationAllowed description Définir le contrôle du point de code de services différenciés (DSCP) sur les plateformes Windows ou OS X pour les connexions DTLS uniquement.

Étape 2 Ajoutez des valeurs nommées pour les attributs personnalisés avec la commande **anyconnect-custom-data** en mode de configuration globale :

[no] anyconnect-custom-data DSCPPreservationAllowed true

Remarque

Par défaut, Secure Client (services client sécurisés) effectue la conservation DSCP (true). Pour le désactiver, définissez l'attribut personnalisé sur false au niveau de la tête de réseau, puis relancez la connexion.

Activer les fonctionnalités Secure Client (services client sécurisés) supplémentaires

Pour minimiser le temps de téléchargement, le client ne demande les téléchargements (à partir de l'ASA ou de l'ISE) que des modules principaux dont il a besoin. À mesure que des fonctionnalités supplémentaires deviennent disponibles pour le Secure Client (services client sécurisés), vous devez mettre à jour les clients distants pour qu'ils utilisent les fonctionnalités.

Pour activer de nouvelles fonctionnalités, vous devez spécifier les nouveaux noms de module à l'aide de la commande **anyconnect modules** à partir du mode de configuration de la stratégie de groupe webvpn ou du nom d'utilisateur webvpn :

[**no**]**anyconnect modules** {**none** | **value** *string*}

Séparez plusieurs chaînes par des virgules.

Activer le démarrage avant la connexion

Le démarrage avant la connexion (SBL) permet l'exécution de scripts d'ouverture de session, la mise en cache des mots de passe, le mappage des lecteurs, et plus encore, pour le Secure Client (services client sécurisés) installé sur un PC Windows. Pour SBL, vous devez activer l'ASA afin qu'il télécharge le module qui permet l'identification et l'authentification graphiques (GINA) pour le Secure Client (services client sécurisés). La procédure suivante montre comment activer SBL :

Procédure

Étape 1 Activez l'ASA afin qu'il télécharge le module GINA pour la connexion VPN vers des groupes ou des utilisateurs précis au moyen de la commande **anyconnect modules** *vpngina* à partir des modes de configuration webvpn de la stratégie de groupe ou du nom d'utilisateur.

Exemple :

Dans l'exemple suivant, l'utilisateur entre dans le mode d'attributs de stratégie de groupe pour la stratégie de groupe *telecommuters*, entre dans le mode de configuration webvpn pour cette stratégie de groupe et précise la chaîne *vpngina* :

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)#anyconnect modules value vpngina
```

Étape 2 Récupérez une copie du fichier de profils clients (AnyConnectProfile.tmpl).

Étape 3 Modifiez le fichier de profils pour préciser que SBL est activé. L'exemple ci-dessous montre la partie pertinente du fichier de profils (AnyConnectProfile.tmpl) pour Windows :

```
<Configuration>
    <ClientInitialization>
        <UseStartBeforeLogon>false</UseStartBeforeLogon>
```

```
    </ClientInitialization>
```

La balise <UseStartBeforeLogon> détermine si le client utilise SBL. Pour activer SBL, remplacez *false* par *true*. L'exemple ci-dessous montre la balise avec SBL activé :

```
<ClientInitialization>
        <UseStartBeforeLogon>true</UseStartBeforeLogon>
    </ClientInitialization>
```

Étape 4 Enregistrez les modifications apportées à AnyConnectProfile.tmpl et mettez à jour le fichier de profil du groupe ou de l'utilisateur sur l'ASA au moyen de la commande **profile** du mode de configuration webvpn. Par exemple :

```
asa1(config-webvpn)#anyconnect profiles sales disk0:/sales_hosts.xml
```

Traduction des langues pour les messages utilisateur Secure Client (services client sécurisés)

L'ASA fournit la traduction linguistique du portail et des écrans affichés aux utilisateurs qui amorcent des connexions VPN SSL sans client basées sur un navigateur, ainsi que l'interface affichée pour les utilisateurs du client VPN Cisco AnyConnect.

Cette section décrit comment configurer l'ASA pour traduire ces messages utilisateur.

Comprendre la traduction linguistique

Les zones fonctionnelles et leurs messages visibles pour les utilisateurs distants sont organisés en domaines de traduction. Tous les messages affichés dans l'interface utilisateur de Cisco AnyConnect VPN Client se trouvent dans le domaine Secure Client (services client sécurisés).

Le progiciel pour l'ASA comprend un modèle de table de traduction pour le domaine Secure Client (services client sécurisés). Vous pouvez exporter le modèle, ce qui crée un fichier XML du modèle à l'URL que vous indiquez. Les champs de message de ce fichier sont vides. Vous pouvez modifier les messages et importer le modèle pour créer un nouvel objet de table de traduction qui réside dans la mémoire flash.

Vous pouvez également exporter une table de traduction existante. Le fichier XML créé affiche les messages que vous avez précédemment modifiés. La réimportation de ce fichier XML avec le même nom de langue crée une nouvelle version de l'objet de table de traduction, qui remplace les messages précédents. Les modifications apportées à la table de traduction du domaine Secure Client (services client sécurisés) sont immédiatement visibles par les utilisateurs Secure Client (services client sécurisés).

Création de tableaux de traduction

La procédure suivante décrit comment créer des tables de traduction pour le domaine Secure Client (services client sécurisés) :

Procédure

Étape 1 Exportez un modèle de tableau de traduction vers un ordinateur avec la commande **export webvpn translation-table** à partir du mode d'exécution privilégié.

Dans l'exemple suivant, la commande **show import webvpn translation-table** affiche les modèles de tableau de traduction et les tableaux disponibles.

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect

PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
```

L'utilisateur exporte ensuite la table de traduction pour le domaine de traduction Secure Client (services client sécurisés). Le nom de fichier du fichier XML créé est nommé *client* et contient des champs de message vides :

```
hostname# export webvpn translation-table AnyConnect
template tftp://209.165.200.225/client
```

Dans l'exemple suivant, l'utilisateur exporte une table de traduction nommée *zh*, qui a été précédemment importée d'un modèle. zh est l'abréviation par Microsoft Internet Explorer pour la langue chinoise.

```
hostname# export webvpn translation-table customization
language zh tftp://209.165.200.225/chinese_client
```

Étape 2 Modifier le fichier XML du tableau de traduction. L'exemple suivant montre une partie du modèle Secure Client (services client sécurisés). La fin de cette sortie comprend un champ d'ID de message (msgid) et un champ de chaîne de message (msgstr) pour le message *Connected*, qui s'affiche dans l'interface graphique Secure Client (services client sécurisés) lorsque le client établit une connexion VPN. Le modèle complet contient plusieurs paires de champs de message :

```
# SOME DESCRIPTIVE TITLE.
# Copyright (C) YEAR THE PACKAGE'S COPYRIGHT HOLDER
# This file is distributed under the same license as the PACKAGE package.
# FIRST AUTHOR <EMAIL@ADDRESS>, YEAR.
#
#, fuzzy
msgid ""
msgstr ""
"Project-Id-Version: PACKAGE VERSION\n"
"Report-Msgid-Bugs-To: \n"
"POT-Creation-Date: 2006-11-01 16:39-0700\n"
"PO-Revision-Date: YEAR-MO-DA HO:MI+ZONE\n"
```

```
"Last-Translator: FULL NAME <EMAIL@ADDRESS>\n"
"Language-Team: LANGUAGE <LL@li.org>\n"
"MIME-Version: 1.0\n"
"Content-Type: text/plain; charset=CHARSET\n"
"Content-Transfer-Encoding: 8bit\n"

#: C:\cygwin\home\<user>\cvc\main\Api\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\check\AgentIfc.cpp:22
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp:23
#: C:\cygwin\home\<user>\cvc\main\Api\save\AgentIfc.cpp~:20
#: C:\cygwin\home\<user>\cvc\main\Api\save\older\AgentIfc.cpp:22
msgid "Connected"
msgstr ""
```

Le msgid contient la traduction par défaut. Le msgstr qui suit msgid fournit la traduction. Pour créer une traduction, saisissez le texte traduit entre les guillemets de la chaîne msgstr. Par exemple, pour traduire le message « Connected » par une traduction en Espagnol, insérez le texte en Espagnol entre les guillemets :

```
msgid "Connected"
msgstr "Conectado"
```

Assurez-vous de sauvegarder le fichier.

Étape 3 Importez la table de traduction à l'aide de la commande **import webvpn translation-table** à partir du mode d'exécution privilégié. Assurez-vous de préciser le nom de la nouvelle table de traduction avec l'abréviation de la langue compatible avec le navigateur.

Dans l'exemple suivant, le fichier XML est importé *es-us*, l'abréviation utilisée par Microsoft Internet Explorer pour l'Espagnol Parlé aux États-Unis.

```
hostname# import webvpn translation-table AnyConnect
language es-us tftp://209.165.200.225/client
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
hostname# show import webvpn translation-table
Translation Tables' Templates:
AnyConnect
PortForwarder

customization
keepout
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin

Translation Tables:
es-us AnyConnect
```

Supprimer les tableaux de traduction

Si vous n'avez plus besoin d'un tableau de traduction, vous pouvez le supprimer.

Procédure

Étape 1 Répertoriez les tableaux de traduction existants.

Dans l'exemple suivant, la commande **show import webvpn translation-table** affiche les modèles de tableau de traduction et les tableaux disponibles. Plusieurs tableaux sont disponibles pour le français (fr), le japonais (ja) et le russe (ru).

```
hostname# show import webvpn translation-table
Translation Tables' Templates:
  AnyConnect
  PortForwarder
  banners
  csd
  customization
  url-list
  webvpn
Translation Tables:
  fr                    PortForwarder
  fr                    AnyConnect
  fr                    customization
  fr                    webvpn
  ja                    PortForwarder
  ja                    AnyConnect
  ja                    customization
  ja                    webvpn
  ru                    PortForwarder
  ru                    customization
  ru                    webvpn
```

Étape 2 Supprimez le tableau de traduction indésirable.

revert webvpn translation-table *translationdomain* **language** *language*

Où *translationdomain* correspond au domaine indiqué à droite dans la liste des tableaux de traduction ci-dessus, et *language* est le nom de langue à 2 caractères.

Vous devez supprimer chaque tableau individuellement. Vous ne pouvez pas supprimer tous les tableaux d'une langue donnée avec une seule commande.

Par exemple, pour supprimer le tableau de traduction française pour Secure Client (services client sécurisés):

```
ciscoasa# revert webvpn translation-table anyconnect language fr
ciscoasa#
```

Configuration des fonctionnalités SSL avancées Secure Client (services client sécurisés)

La section suivante décrit les fonctionnalités avancées qui affinent les connexions VPN SSL Secure Client (services client sécurisés) :

Activer le renouvellement

Lorsque l'ASA et le Secure Client (services client sécurisés) effectuent un renouvellement sur une connexion VPN SSL, ils renégocient les clés de chiffrement et les vecteurs d'initialisation, augmentant ainsi la sécurité de la connexion.

Pour permettre au client d'effectuer un renouvellement sur une connexion VPN SSL pour un groupe ou un utilisateur spécifique, utilisez la commande **AnyConnect ssl** rekey à partir des modes de stratégie de groupe ou de nom d'utilisateur webvpn.

[no]AnyConnect ssl rekey {**method** {**new-tunnel** | **none** | **ssl**} | **time** *minutes*}

- **method new-tunnel** spécifie que le client établit un nouveau tunnel pendant le renouvellement.
- **method ssl** spécifie que le client établit un nouveau tunnel pendant le renouvellement.
- **method none** désactive le renouvellement.
- **time** *minutes* spécifie le nombre de minutes à partir du début de la session ou du dernier renouvellement, jusqu'à ce que le renouvellement ait lieu, de 1 à 10080 (1 semaine).

Remarque La configuration de la méthode de renouvellement comme **ssl** ou **new-tunnel** spécifie que le client établit un nouveau tunnel pendant le renouvellement au lieu que la renégociation SSL ait lieu pendant le renouvellement. Consultez la référence de commande pour obtenir l'historique de la commande **AnyConnect ssl rekey**.

Dans l'exemple suivant, le client est configuré pour renégocier avec SSL pendant le renouvellement, qui a lieu 30 minutes après le début de la session, pour la stratégie de groupe existante *sales* :

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

Configurer

La détection d'homologue mort (DPD) garantit que la passerelle ASA ou le client peut rapidement détecter une condition où l'homologue ne répond pas et que la connexion a échoué. Pour activer la détection d'homologue mort (DPD) et définir la fréquence à laquelle le Secure Client (services client sécurisés) ou la passerelle ASA exécute le DPD.

Remarque Lorsque la connexion est interrompue du côté client, l'ASA n'abandonne pas la session Secure Client (services client sécurisés) en raison de DPD ou de keepalive sans condition. DPD n'est déclenché par l'ASA que lorsqu'il y a un flux de données entre l'ASA et le client. Une fois que DPD est déclenché, il effectue trois tentatives pour chaque session enfant (SSL/DTLS) avant de les supprimer.

S'il n'y a pas de flux de données, le DPD n'est pas déclenché. L'ASA dispose d'un délai d'inactivité TCP codé en dur de 5 minutes qui ferme automatiquement les connexions de tunnel SSL/DTLS lorsqu'aucune donnée ni aucun paquet Keepalive ne circule pendant exactement 5 minutes, quel que soit le paramètre configuré de délai d'inactivité du VPN. Après la suppression des sessions enfants, la commande **vpn-idle-timeout** est uniquement responsable du contrôle de la durée maximale d'une session parente. Pour plus de détails sur les attributs DPD, keepalive et de temporisation, consultez la FAQ AnyConnect – Tunnels, DPD et minuterie d'inactivité.

Avant de commencer

- Cette fonctionnalité s'applique uniquement à la connectivité entre la passerelle ASA et le client SSL VPN Secure Client (services client sécurisés). Il ne fonctionne pas avec IPsec, car DPD est basé sur l'implémentation des normes qui ne permet pas le remplissage.
- Si vous activez DTLS, activez également la détection d'homologue mort (DPD). DPD permet à une connexion DTLS défaillante de revenir à TLS. Dans le cas contraire, la connexion se termine.
- Lorsque DPD est activé sur l'ASA, vous pouvez utiliser la fonction de MTU optimale (OMTU) pour trouver la plus grande MTU de point terminal à laquelle le client peut transmettre avec succès les paquets DTLS. Mettez en œuvre OMTU en envoyant un paquet DPD rempli jusqu'à la MTU maximale. Si un écho correct de la charge utile est reçu de la tête de réseau, la taille de la MTU est acceptée. Sinon, la MTU est réduite et la sonde est de nouveau envoyée jusqu'à ce que la MTU minimale autorisée pour le protocole soit atteinte.

Procédure

Étape 1 Accédez à la stratégie de groupe souhaitée.

Entrez le mode de stratégie de groupe ou de nom d'utilisateur webvpn :

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

Ou

```
hostname# username username attributes
hostname(config-username)# webvpn
hostname (config-username-webvpn #
```

Étape 2 Définir la détection côté passerelle.

Utilisez la commande [**no**] **anyconnect dpd-interval** {[**gateway** {*secondes* | **none**}]} .

La passerelle fait référence à l'ASA. Vous activez DPD et spécifiez l'intervalle auquel l'ASA attend tout paquet du client sur une plage comprise entre 30 (par défaut) et 3 600 secondes (1 heure). Une valeur de 300 est conseillée. Si aucun paquet n'est reçu dans cet intervalle, l'ASA effectue le test DPD avec trois tentatives au même intervalle. Si l'ASA ne reçoit pas de réponse du client, il interrompt le tunnel TLS/DTLS.

Remarque
La spécification **none** désactive les tests DPD effectués par l'ASA. Utilisez **no AnyConnect dpd-interval** pour supprimer cette commande de la configuration.

La spécification de **none** désactive le test DPD effectué par l'ASA. Utilisez la commande **no anyconnect dpd-interval** pour supprimer cette commande de la configuration.

Étape 3 Définir la détection côté client.

Utilisez la commande [**no**] **anyconnect dpd-interval** {[**client** {*seconds* | **none**}]} .

Le client fait référence à Secure Client (services client sécurisés). Vous activez DPD et spécifiez la fréquence à laquelle le client effectue le test DPD sur une plage de 30 (par défaut) à 3 600 secondes (1 heure). Une valeur de 30 secondes est conseillée.

La spécification de **client none** désactive le DPD effectué par le client. Utilisez la commande **no anyconnect dpd-interval** pour supprimer cette commande de la configuration.

Exemple

L'exemple suivant définit la fréquence du DPD effectué par l'ASA à 30 secondes et celle du DPD effectué par le client à 10 secondes pour la stratégie de groupe existante *sales* :

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect dpd-interval gateway 30
hostname(config-group-webvpn)# anyconnect dpd-interval client 10
```

Activer les messages keepalive

Vous pouvez ajuster la fréquence des messages keepalive pour vous assurer qu'une connexion VPN SSL à travers un proxy, un pare-feu ou un périphérique NAT demeure ouverte, même si ce périphérique limite la durée pendant laquelle la connexion peut rester inactive. L'ajustement de la fréquence garantit également que le client ne se déconnecte pas puis ne se reconnecte pas lorsque l'utilisateur distant n'exécute pas activement une application fondée sur des sockets, comme Microsoft Outlook ou Microsoft Internet Explorer.

Les messages keepalive sont activés par défaut. Si vous désactivez les messages keepalive, en cas de basculement, les sessions client VPN SSL ne sont pas transférées vers le périphérique en veille.

Pour définir la fréquence des messages keepalive, utilisez la commande **keepalive** à partir du mode de configuration de stratégie de groupe webvpn ou nom d'utilisateur webvpn : utilisez la forme **no** de la commande pour la supprimer de la configuration et faire hériter la valeur :

[**no**] **anyconnect ssl keepalive** {**none** | *secondes*}

- **none** Désactive les messages keepalive des clients.
- *secondes* permet au client d'envoyer des messages keepalive et précise la fréquence des messages dans une plage de 15 à 600 secondes.

Dans l'exemple suivant : l'ASA est configuré pour permettre au client d'envoyer des messages keepalive avec une fréquence de 300 secondes, soit 5 minutes, pour la stratégie de groupe existante *sales* :

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

Utiliser la compression

La compression augmente les performances des communications entre l'ASA et le client en réduisant la taille des paquets transférés pour les connexions à faible bande passante. Par défaut, la compression de toutes les connexions VPN SSL est activée sur l'ASA, à la fois au niveau global et pour des groupes ou des utilisateurs spécifiques.

Remarque Lors de la mise en œuvre de la compression sur les connexions à large bande, vous devez prendre en compte le fait que la compression repose sur une connectivité sans perte. C'est la principale raison pour laquelle elle n'est pas activée par défaut sur les connexions à large bande.

La compression doit être activée globalement à l'aide de la commande **compression** en mode de configuration globale, puis elle peut être définie pour des groupes ou des utilisateurs spécifiques avec la commande **anyconnect ssl compression** en mode group-policy webvpn ou username webvpn.

Modification globale de la compression

Pour modifier les paramètres globaux de compression, utilisez la commande AnyConnect ssl **compression** à partir du mode de configuration globale. Pour supprimer la commande de la configuration, utilisez la forme **no** de la commande.

Dans l'exemple suivant, la compression est désactivée globalement pour toutes les connexions VPN SSL :

```
hostname(config)# no compression
```

Modification de la compression pour les groupes et les utilisateurs

Pour modifier la compression pour un groupe ou un utilisateur particulier, utilisez la commande AnyConnect ssl compression en mode group-policy webvpn ou username webvpn :

[**no**] **anyconnect ssl compression** {**deflate** | **none**}

Par défaut, pour les groupes et les utilisateurs, la compression SSL est définie sur *deflate* (activée).

Pour supprimer la commande **AnyConnect ssl compression** de la configuration et faire hériter la valeur du paramètre global, utilisez la forme **no** de la commande :

Dans l'exemple suivant, la compression est désactivée pour la stratégie de groupe sales :

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no anyconnect ssl compression none
```

Ajuster la taille de la MTU

Vous pouvez ajuster la taille de la MTU, de 576 à 1 406 octets, pour les connexions VPN SSL établies par le client au moyen de la commande **anyconnect mtu**, en mode de configuration group-policy webvpn ou username webvpn. :

[**no**] **anyconnect mtu** *size*

Cette commande affecte uniquement Secure Client (services client sécurisés). L'ancien client VPN SSL de Cisco () n'est pas en mesure de s'ajuster à différentes tailles de MTU. De plus, cette commande a une incidence sur les connexions client établies en SSL et sur celles établies en SSL avec DTLS.

La valeur par défaut pour cette commande dans la stratégie de groupe par défaut est **no anyconnect mtu**. La taille de la MTU est ajustée automatiquement en fonction de la MTU de l'interface utilisée par la connexion, moins le surdébit IP/UDP/DTLS.

Vous pouvez recevoir le message « Configuration MTU envoyée par la passerelle sécurisée trop petite », par exemple lors de l'exécution du module AnyConnect ISE Posture. Si vous saisissez **AnyConnect mtu 1200** avec **AnyConnect ssl df-bit-ignore disable**, vous pouvez éviter ces erreurs d'analyse du système.

Exemple

L'exemple suivant configure la taille de la MTU à 1 200 octets pour la stratégie de groupe télétravailleurs :

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect mtu 1200
```

Mettre à jour les images Secure Client (services client sécurisés)

Vous pouvez mettre à jour les images des clients sur l'ASA à tout moment en suivant cette procédure.

Remarque Pour une sécurité, une performance et une gestion optimales de votre infrastructure VPN, nous vous recommandons de supprimer régulièrement les images Secure Client (services client sécurisés) obsolètes de votre pare-feu, en ne conservant que les dernières versions requises pour éviter les conflits de configuration.

Procédure

Étape 1 Copiez les nouvelles images client dans l'ASA à l'aide de la commande **copy** du mode d'exécution privilégié ou à l'aide d'une autre méthode.

Étape 2 Si les nouveaux fichiers image client portent les mêmes noms de fichier que les fichiers déjà chargés, entrez de nouveau la commande **anyconnect image** qui se trouve dans la configuration. Si les nouveaux noms de fichiers sont différents, désinstallez les anciens fichiers à l'aide de la commande d'image [**no**]**anyconnect image**. Utilisez ensuite la commande **anyconnect image** pour attribuer un ordre aux images et faire en sorte que l'ASA charge les nouvelles images.

Activer l'accès VPN IPv6

Si vous souhaitez configurer l'accès IPv6, vous devez utiliser l'interface de ligne de commande. La version 9.0(x) de l'ASA ajoute la prise en charge des connexions VPN IPv6 à son interface externe à l'aide des protocoles SSL et IKEv2/IPsec.

Vous activez l'accès IPv6 à l'aide de la commande **ipv6 enable** dans le cadre de l'activation des connexions VPN SSL. Voici un exemple de connexion IPv6 qui active IPv6 sur l'interface externe :

```
hostname(config)# interface GigabitEthernet0/0
hostname(config-if)# ipv6 enable
```

Pour activer le VPN SSL IPv6, effectuez les actions générales suivantes :

1. Activez IPv6 sur l'interface externe.
2. Activez IPv6 et une adresse IPv6 sur l'interface interne.
3. Configurez un ensemble local d'adresses IPv6 pour les adresses IP attribuées aux clients.

4. Configurez une passerelle par défaut de tunnel IPv6.

Procédure

Étape 1 Configurez les interfaces :

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 192.168.0.1 255.255.255.0
 ipv6 enable      ; Needed for IPv6.
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.0.1 255.255.0.0
 ipv6 address 2001:DB8::1/32        ; Needed for IPv6.
 ipv6 enable      ; Needed for IPv6.
```

Étape 2 Configurez un « ensemble local ipv6 » (utilisé pour l'affectation d'adresses IPv6) :

```
ipv6 local pool ipv6pool 2001:DB8:1:1::5/32 100     ; Use your IPv6 prefix here
```

Remarque
Vous pouvez configurer l'ASA pour attribuer une adresse IPv4, une adresse IPv6 ou à la fois une adresse IPv4 et une adresse IPv6 à Secure Client (services client sécurisés) en créant des regroupements internes d'adresses sur l'ASA ou en attribuant une adresse dédiée à un utilisateur local sur l'ASA.

Étape 3 Ajoutez l'ensemble d'adresses IPv6 à votre stratégie de groupe de tunnels (ou stratégie de groupe) :

```
tunnel-group YourTunGrp1 general-attributes  ipv6-address-pool ipv6pool
```

Remarque
Vous devez également configurer un ensemble d'adresses IPv4 ici (à l'aide de la commande « address-ensemble »).

Étape 4 Configurez une passerelle par défaut de tunnel IPv6 :

```
ipv6 route inside ::/0 X:X:X:X::X tunneled
```

SAML 2.0

L'ASA prend en charge SAML 2.0 afin que les utilisateurs VPN puissent saisir leurs informations d'authentification une seule fois lorsqu'ils accèdent à différentes applications SaaS en dehors du réseau privé.

Par exemple, une entreprise cliente a activé PingIdentity comme fournisseur d'identité (IdP) SAML et possède des comptes sur Rally, Salesforce, Oracle OEM, Microsoft ADFS, OneLogin ou Dropbox, pour lesquels l'authentification unique SAML 2.0 a été activée. Lorsque vous configurez l'ASA pour prendre en charge

SAML 2.0 SSO en tant que fournisseur de services (SP), les utilisateurs finaux peuvent se connecter une seule fois et avoir accès à tous ces services.

La prise en charge de SAML par AnyConnect a été ajoutée afin de permettre à un client AnyConnect 4.4 d'accéder à des applications basées sur SaaS au moyen de SAML 2.0. AnyConnect 4.6 a introduit une version améliorée de l'intégration SAML avec un navigateur intégré, qui a remplacé l'intégration au navigateur natif (externe) des versions précédentes. La nouvelle version améliorée avec navigateur intégré exigeait une mise à niveau vers AnyConnect 4.6 (ou version ultérieure) et ASA 9.7.1.24 (ou version ultérieure), 9.8.2.28 (ou version ultérieure) ou 9.9.2.1 (ou version ultérieure).

La version 9.17.1 d'ASA / version 7.17.1 d'ASDM a introduit la prise en charge du navigateur externe SAML pour AnyConnect VPN avec AnyConnect 4.10.04065 (ou version ultérieure). Lorsque vous utilisez SAML comme méthode d'authentification principale pour le profil de connexion VPN AnyConnect, vous pouvez choisir que le client Secure Client (services client sécurisés) utilise un navigateur local, au lieu du navigateur intégré à Secure Client (services client sécurisés) pour effectuer l'authentification Web. Grâce à cette fonctionnalité, Secure Client (services client sécurisés) prend en charge WebAuthN et toutes les autres options d'authentification Web basées sur SAML, telles que l'authentification unique, l'authentification biométrique ou d'autres méthodes améliorées qui ne sont pas offertes avec le navigateur intégré. Pour utiliser le navigateur externe SAML, vous devez effectuer la configuration décrite ici : Configurer le navigateur du système d'exploitation par défaut pour l'authentification SAML, à la page 29.

L'ASA agit comme SP lorsque SAML est configuré comme méthode d'authentification pour un groupe de tunnels, qu'il s'agisse du groupe de tunnels par défaut ou de tout autre groupe. L'utilisateur VPN lance la connexion unique en accédant à un ASA activé ou au fournisseur d'identité de SAML. Chacun de ces scénarios est décrit ci-dessous.

Authentification unique initiée par le SP SAML

Lorsque l'utilisateur final initie la connexion en accédant à l'ASA, le processus d'authentification se déroule comme suit :

1. Lorsque l'utilisateur VPN accède à un groupe de tunnels activé pour SAML ou le sélectionne, l'utilisateur final est redirigé vers le fournisseur d'identité SAML pour l'authentification. L'utilisateur est invité à s'authentifier, sauf s'il accède directement à l'URL de groupe, auquel cas la redirection est silencieuse.

   L'ASA génère une demande d'authentification SAML, que le navigateur redirige vers le fournisseur d'identité de SAML.

2. Le fournisseur d'identité invite l'utilisateur final à saisir ses informations d'authentification, puis l'utilisateur final se connecte. Les informations d'authentification saisies doivent satisfaire à la configuration d'authentification du fournisseur d'identité.

3. La réponse du fournisseur d'identité est renvoyée au navigateur et publiée sur l'URL de connexion de l'ASA. L'ASA vérifie la réponse pour terminer la connexion.

SSL initié par le fournisseur d'identité SAML

Lorsque l'utilisateur initie la connexion en accédant au fournisseur d'identité, le processus d'authentification se déroule comme suit :

1. Un utilisateur final accède au fournisseur d'identité. Le fournisseur d'identité invite l'utilisateur final à saisir ses informations d'authentification conformément à sa configuration d'authentification. L'utilisateur final envoie ses informations d'authentification et se connecte au fournisseur d'identité.

2. En général, l'utilisateur final obtient une liste des services compatibles avec SAML qui ont été configurés avec le fournisseur d'identité. L'utilisateur final choisit l'ASA.
3. Une réponse SAML est renvoyée au navigateur et publiée sur l'URL de connexion de l'ASA. L'ASA vérifie la réponse pour terminer la connexion.

Cercle de confiance

La relation de confiance entre l'ASA et le fournisseur d'identité SAML est établie au moyen de certificats configurés (points de confiance ASA).

La relation de confiance entre l'utilisateur final et le fournisseur d'identité SAML est établie par l'authentification configurée sur le fournisseur d'identité.

Délai d'expiration SAML

Dans l'assertion SAML, il existe NotBefore et NotOnOrAfter comme suit :<saml:Conditions NotBefore="2015-03-10T19:47:41Z" NotOnOrAfter="2015-03-10T20:47:41Z">

Un délai d'expiration SAML configuré sur l'ASA remplacera NotOnOrAfter si la somme de NotBefore et du délai d'expiration est antérieure à NotOnOrAfter. Si NotBefore + le délai d'expiration est postérieur à NotOnOrAfter, NotOnOrAfter prend effet.

Le délai d'expiration doit être très court pour éviter que l'assertion ne soit réutilisée après l'expiration du délai. Vous devez synchroniser le serveur NTP (Network Time Protocol) de votre ASA avec le serveur NTP du fournisseur d'identité pour utiliser la fonctionnalité SAML.

Prise en charge dans le réseau privé

L'identifiant du fournisseur de services basé sur SAML 2.0 est pris en charge dans un réseau privé. Lorsque le fournisseur d'identité SAML est déployé dans le nuage privé, l'ASA et les autres services compatibles avec SAML sont en position d'homologues et se trouvent tous dans le réseau privé. Avec l'ASA comme passerelle entre l'utilisateur et les services, l'authentification sur l'IdP est gérée avec une session webvpn anonyme restreinte, et tout le trafic entre l'IdP et l'utilisateur est traduit. Lorsque l'utilisateur se connecte, l'ASA modifie la session avec les attributs correspondants et stocke les sessions du fournisseur d'identité. Vous pouvez ensuite utiliser le fournisseur de services sur le réseau privé sans avoir à saisir de nouveau vos informations d'authentification.

L'attribut *NameID* du fournisseur d'identité SAML détermine le nom d'utilisateur et est utilisé pour l'autorisation, la comptabilité et la base de données des sessions VPN.

Remarque Vous ne pouvez pas échanger d'informations d'authentification entre les réseaux privé et public. Si vous utilisez le même fournisseur d'identité pour les fournisseurs de services internes et externes, vous devez vous authentifier séparément. Le fournisseur d'identité interne uniquement ne peut pas être utilisé avec des services externes : le fournisseur d'identité externe uniquement ne peut pas être utilisé avec les fournisseurs de services dans le réseau privé.

Directives et limites relatives à SAML 2.0

- ASA prend en charge les signatures suivantes pour l'authentification SAML :

  - SHA1 avec RSA et HMAC
  - SHA2 avec RSA et HMAC

- ASA prend en charge la liaison Redirect-POST SAML 2.0, qui est prise en charge par tous les fournisseurs d'identité SAML.
- L'ASA fonctionne uniquement comme fournisseur de service SAML. Il ne peut pas servir de fournisseur d'identité en mode passerelle ou en mode homologue.
- Cette fonctionnalité SAML SSO SP est une méthode d'authentification d'exclusion mutuelle. Elle ne peut pas être utilisée conjointement avec AAA et le certificat.
- Les fonctionnalités basées sur l'authentification par nom d'utilisateur/mot de passe, l'authentification de certificats et le KCD ne sont pas prises en charge. Par exemple, la fonction de préremplissage du nom d'utilisateur et du mot de passe, la connexion automatique basée sur un formulaire, la connexion automatique basée sur la substitution de macros, KCD SSO, etc.
- L'ASA prend en charge l'équilibrage de charges VPN avec l'authentification SAML AnyConnect.
- Lorsque vous utilisez Safari pour l'authentification SAML, assurez-vous de disposer de la mise à jour de Safari 14.1.2 ou ultérieure.
- Les administrateurs ASA doivent assurer la synchronisation de l'horloge entre l'ASA et le fournisseur d'identité SAML pour une gestion appropriée des déclarations d'authentification et un comportement correct du délai d'expiration.
- Les administrateurs ASA ont la responsabilité de maintenir un certificat de signature valide sur l'ASA et sur le fournisseur d'identité en tenant compte des éléments suivants :
  - Le certificat de signature du fournisseur d'identité est obligatoire lors de la configuration d'un fournisseur d'identité sur l'ASA.
  - L'ASA n'effectue pas de vérification de révocation sur le certificat de signature reçu du fournisseur d'identité.
- Dans les assertions SAML, il existe des conditions NotBefore et NotOnOrAfter . Le **délai d'expiration** configuré pour la SAML interagit avec ces conditions comme suit :
  - Le délai d'expiration remplace NotOnOrAfter si la somme de NotBefore et du délai d'expiration est antérieure à NotOnOrAfter.
  - Si NotBefore + le délai d'expiration est postérieur à NotOnOrWith, NotOnOrAfter prend effet.
  - Si l'attribut NotBefore est absent, l'ASA refuse la demande de connexion. Si l'attribut NotOnOrAfter est absent et que le délai d'expiration SAML n'est pas défini, l'ASA refuse la demande de connexion.
- L'ASA ne fonctionne pas avec Duo dans un déploiement utilisant SAML interne, ce qui oblige l'ASA à passer par le proxy pour que le client s'authentifie, en raison du changement de nom de domaine complet qui se produit lors de la demande/réponse pour l'authentification à deux facteurs (push, code, mot de passe).
- Les certificats de serveur non fiable ne sont pas autorisés dans le navigateur intégré.
- L'intégration SAML au navigateur intégré n'est pas prise en charge en modes CLI ou SBL.

- L'authentification SAML établie dans un navigateur Web n'est pas partagée avec AnyConnect, et inversement.
- Selon la configuration, diverses méthodes sont utilisées lors de la connexion à la tête de réseau avec le navigateur intégré. Par exemple, alors qu'AnyConnect peut préférer une connexion IPv4 à une connexion IPv6, le navigateur intégré peut préférer IPv6, ou inversement. De même, AnyConnect peut avoir recours à l'absence de proxy après avoir essayé de passer par un proxy et obtenu un échec, tandis que le navigateur intégré peut arrêter la navigation après avoir essayé de passer par un mandataire et obtenu un échec.
- Vous devez synchroniser le serveur NTP (Protocole de temps réseau) de votre ASA avec le serveur NTP du fournisseur d'identité pour utiliser la fonctionnalité SAML.
- L'assistant VPN sur ASDM ne prend actuellement pas en charge les configurations SAML.
- Vous ne pouvez pas accéder aux serveurs internes avec la SSO après vous être connecté à l'aide d'un fournisseur d'identité interne.
- L'attribut NameID du fournisseur d'identité SAML détermine le nom d'utilisateur de l'utilisateur et est utilisé pour l'autorisation, la comptabilité et la base de données des sessions VPN.
- SAML n'est pas pris en charge en mode multicontexte.
- Plusieurs attributs reçus avec une validation SAML ne sont pas pris en charge.
- Les Chromebook ne prennent pas en charge Secure Client SAML avec l'authentification par navigateur externe.
- Assurez-vous que le fournisseur d'identité comprend le paramètre d'état de relais dans la réponse SAML, tel qu'il a été reçu dans la demande SAML correspondante.

Configurer un fournisseur d'identité (IdP) SAML 2.0

Avant de commencer

Obtenez les URL de connexion et de déconnexion pour votre fournisseur SAML (IdP). Vous pouvez obtenir les URL sur le site Web du fournisseur, ou ils peuvent fournir ces informations dans un fichier de métadonnées.

Procédure

Étape 1 Créez un fournisseur d'identité SAML en mode de configuration webvpn et passez en sous-mode saml-idp sous webvpn.

[**no**] **saml idp** *idp-entityID*

idp-entityID : l'ID d'entité du fournisseur d'identité de SAML doit contenir de 4 à 128 caractères.

Pour supprimer un fournisseur d'identité de SAML, utilisez la forme **no** de cette commande.

Étape 2 Configurez les URL du fournisseur d'identité.

url [**sign-in** | **sign-out**] *value*

value : Il s'agit de l'URL pour la connexion au fournisseur d'identité ou de l'URL de redirection lors de la déconnexion du fournisseur d'identité. L'URL **sign-in** est requise, l'URL **sign-out** est facultative. La valeur de l'URL doit contenir de 4 à 500 caractères.

Étape 3 (Facultatif) Configure l'URL de base du fournisseur de services SAML pour l'authentification VPN. Cette URL est utilisée dans les métadonnées SAML, qui sont fournies aux fournisseurs d'identité tiers, afin que les fournisseurs d'identité puissent rediriger les utilisateurs de points terminaux vers l'ASA.

base-url *URL*

Cette URL est fournie à des fournisseurs d'identité tiers pour rediriger les utilisateurs finaux vers l'ASA.

Lorsque base-url est configuré, nous l'utilisons comme URL de base pour les attributs AssertionConsumerService et SingleLogoutService dans **show saml metadata**.

Lorsque l'URL de base n'est pas configurée, l'URL est déterminée par le nom d'hôte et le nom de domaine de l'ASA. Par exemple, nous utilisons `https://ssl-vpn.cisco.com` lorsque le nom d'hôte est `ssl-vpn` et que le nom de domaine est `cisco.com`.

Une erreur se produit si ni l'URL de base ni le nom d'hôte/nom de domaine ne sont configurés lors de la saisie de **show saml metadata**.

Étape 4 Configurez les trustpoints entre le fournisseur d'identité et le fournisseur (ASA).

trustpoint [**idp** | **sp**] *trustpoint-name*

idp : spécifie le trustpoint qui contient le certificat du fournisseur d'identité pour que l'ASA vérifie les assertions SAML.

sp : spécifie le trustpoint qui contient le certificat de l'ASA (SP) pour que le fournisseur d'identité vérifie la signature de l'ASA ou l'assertion SAML chiffrée.

trustpoint-name : doit être un trustpoint configuré précédemment.

Étape 5 (Facultatif) Configurez le délai d'expiration SAML.

timeout assertion *timeout-in-seconds*

Si ce paramètre est spécifié, cette configuration remplace NotOnOrAfter si la somme de NotBefore et de timeout-in-seconds est antérieure à NotOnOrAfter.

Si ce paramètre n'est pas spécifié, NotBefore et NotOnOrAfter dans l'assertion sont utilisés pour déterminer la validité.

Remarque
Pour un groupe de tunnels avec un fournisseur d'identité SAML existant configuré, toutes les modifications apportées à l'interface de ligne de commande saml idp sous webvpn ne sont appliquées qu'au groupe de tunnels lorsque SAML est réactivé pour ce groupe de tunnels particulier. Après avoir configuré le délai d'expiration, le délai d'expiration mis à jour ne prend effet qu'après la réémission de l'interface de ligne de commande du fournisseur d'identité saml dans les attributs webvpn du groupe de tunnels.

Étape 6 (Facultatif) Activez ou désactivez (paramètre par défaut) la signature dans la requête SAML.

signature <value>

Remarque
Avec la mise à niveau vers SSO 2.5.1, la méthode de signature par défaut passe de SHA1 à SHA256, et vous pouvez configurer la méthode de signature que vous préférez en entrant la *valeur* rsa-sha1, rsa-sha256, rsa-sha384 ou rsa-sha512.

Étape 7 (Facultatif) Pour définir l'indicateur déterminant que le fournisseur d'identité est un réseau interne, utilisez la commande **internal**. L'ASA fonctionnera ensuite en mode de passerelle.

Étape 8 Utilisez **show webvpn saml idp** pour afficher la configuration.

Étape 9 Utilisez **force re-authentication** pour que le fournisseur d'identité s'authentifie directement plutôt que de dépendre d'un contexte de sécurité précédent lorsqu'une demande d'authentification SAML se produit. Il s'agit du paramètre par défaut ; donc, pour désactiver, utilisez **no force re-authentication**.

Exemple

L'exemple suivant configure un fournisseur d'identité nommé salesforce_idp et utilise des points de confiance préconfigurés :

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)#saml idp salesforce_idp

ciscoasa(config-webvpn-saml-idp)#url sign-in
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
ciscoasa(config-webvpn-saml-idp)#url sign-out
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect

ciscoasa(config-webvpn-saml-idp)#trustpoint idp salesforce_trustpoint
ciscoasa(config-webvpn-saml-idp)#trustpoint sp asa_trustpoint

ciscoasa(config)#show webvpn saml idp
saml idp salesforce_idp
url sign-in https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
url sign-out https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
trustpoint idp salesforce_trustpoint
trustpoint  sp asa_trustpoint
```

La page Web suivante montre un exemple de la manière d'obtenir les URL pour OneLogin

https://onelogin.zendesk.com/hc/en-us/articles/202767260-Configuring-SAML-for-Clarizen

La page Web suivante est un exemple d'utilisation des métadonnées pour trouver les URL à partir de OneLogin.

http://onlinehelp.tableau.com/current/online/en-us/saml_config_onelogin.htm

Prochaine étape

Appliquez l'authentification SAML aux profils de connexion, comme décrit dans Configurer l'ASA en tant que fournisseur de services SAML 2.0, à la page 28.

Configurer l'ASA en tant que fournisseur de services SAML 2.0

Avant de commencer

Le fournisseur d'identité doit avoir été configuré précédemment. Consultez Configurer un fournisseur d'identité (IdP) SAML 2.0, à la page 26.

Procédure

Étape 1 En sous-mode webvpn de groupe de tunnels, utilisez la commande saml identity-provider pour attribuer un fournisseur d'identité.

saml identity-provider *idp-entityID*

idp-entityID : doit être l'un des fournisseurs d'identité existants configurés précédemment.

Pour désactiver SAML SP, utilisez la forme **no** de cette commande.

Étape 2 Activez la méthode d'authentification SAML.

authentication saml

Exemple

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

Configurer le navigateur du système d'exploitation par défaut pour l'authentification SAML

Précisez si AnyConnect doit gérer ou non le processus d'authentification SSO à l'aide du navigateur natif de la plateforme (le navigateur par défaut du système d'exploitation) ou à l'aide du navigateur intégré dans AnyConnect.

Vous devez télécharger le progiciel de navigateur externe AnyConnect (par exemple, *external-sso-4.10.04065-webdeploy-k9.pkg*) et le charger sur ASA. Vous pouvez ensuite choisir la méthode de connexion SAML (le navigateur intégré d'AnyConnect ou le navigateur par défaut du système d'exploitation) pour l'authentification SAML. Cet ensemble est un script qui permet au client VPN de lancer le navigateur Web du système d'exploitation par défaut à des fins d'authentification, et est indépendant du système d'exploitation, du navigateur et de la version du client VPN. Tant que la fonctionnalité est activée, la version du client VPN et le fichier de version du paquet de navigateur externe n'ont pas besoin de correspondre.

Choisir le navigateur du système d'exploitation par défaut active la connexion unique (SSO) entre votre authentification VPN et d'autres connexions d'entreprise. Choisissez cette option si vous souhaitez prendre en charge des méthodes d'authentification web, telles que l'authentification biométrique, qui ne peuvent pas être exécutées dans le navigateur intégré. Avant de sélectionner le navigateur du système d'exploitation, vous devez charger un paquet qui peut être exécuté dans le navigateur pour activer l'authentification Web.

Procédure

Étape 1 En sous-mode webvpn, utilisez la commande AnyConnect external-browser-pkg pour activer l'authentification SAML AnyConnect à l'aide du navigateur par défaut du système d'exploitation.

anyconnect external-browser-pkg *path*

Pour désactiver le navigateur par défaut du système d'exploitation pour l'authentification SAML, utilisez la forme **no** de cette commande.

Étape 2 En sous-mode webvpn de groupe de tunnels, utilisez la commande external-browser pour activer l'authentification SAML AnyConnect à l'aide du navigateur par défaut du système d'exploitation.

external-browser enable *idp-entityID*

Pour désactiver le navigateur par défaut du système d'exploitation pour l'authentification SAML, utilisez la forme **no** de cette commande.

Exemple

Cet exemple sélectionne le chemin d'accès au paquet de navigateur externe AnyConnect et active un navigateur externe (le navigateur par défaut du système d'exploitation) pour l'authentification SAML.

```
asa(config-webvpn)# anyconnect external-browser-pkg flashshow :
asa(config)# tunnel-group SAML webvpn-attributes
asa(config-tunnel-webvpn)# external-browser enable
asa(config-tunnel-webvpn)#
```

Configurer l'authentification par certificat et SAML

Vous pouvez configurer l'authentification par certificat et l'authentification SAML pour les profils de connexion basés sur SAML afin de valider les ressources du client sans profilage pour une clé de fichier ou de registre particulière. Les authentifications basées sur SAML peuvent être liées à des ressources ou à des utilisateurs autorisés. Vous pouvez utiliser un seul certificat ou plusieurs certificats avec SAML pour l'authentification.

Lorsque Secure Client (services client sécurisés) amorce une connexion, l'ASA ou le FTD demandera et authentifie un ou plusieurs certificats du point terminal avant que l'authentification SAML ne soit effectuée.

Une fois l'authentification SAML terminée, le nom d'utilisateur de SAML et du certificat peut être

Une fois l'authentification SAML terminée, le nom d'utilisateur de SAML et du certificat peut être comparé avant de passer à la phase d'autorisation.

Avant de commencer

Assurez-vous de configurer les paramètres SAML requis avant la configuration de l'authentification par certificat et SAML :

- Obtenez les URL de connexion et de déconnexion pour votre fournisseur SAML (IdP). Vous pouvez obtenir les URL sur le site Web du fournisseur, ou ils peuvent fournir ces informations dans un fichier de métadonnées.
- Configurez les paramètres du fournisseur d'identité SAML et du point de confiance. Voir la section Configurer l'authentification par certificat et SAML, à la page 30.

Procédure

Étape 1 Pour configurer le certificat et l'authentification SAML, passez en mode d'attributs webvpn-attributes de groupe de tunnels en saisissant la commande suivante. L'invite change pour indiquer le changement de mode :

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

Étape 2 Pour préciser la méthode d'authentification à utiliser, entrez la commande suivante :

```
hostname(config-tunnel-webvpn)#authentication authentication_method
```

Par exemple : la commande suivante permet l'authentification SAML et par certificat :

```
hostname(config-tunnel-webvpn)#authentication saml certificate
```

La commande suivante permet l'authentification par certificat et SAML :

```
hostname(config-tunnel-webvpn)#authentication certificate saml
```

La commande suivante permet l'authentification par certificats multiples et SAML :

```
hostname(config-tunnel-webvpn)#authentication multiple-certificate saml
```

Étape 3 Ajoutez ou modifiez un profil de connexion, puis sélectionnez les paramètres d'attributs du profil de connexion dans **Basic (De base).**.

Étape 4 Pour préciser la méthode d'authentification pour l'authentification par certificat et SAML, sélectionnez SAML et certificat ou Plusieurs certificats et SAML dans la liste déroulante.

Exemple

L'exemple suivant configure plusieurs certificats et l'authentification SAML pour le profil de connexion sales_group :

```
ciscoasa(config)# tunnel-group sales_group webvpn
ciscoasa(config-tunnel-webvpn)#authentication multiple-certificate saml
```

Exemple de SAML 2.0 et OneLogin

Suivez cet exemple en utilisant votre fournisseur d'identité SAML 2.0 tiers à la place des informations et de la dénomination Onelogin.

1. Définissez la synchronisation de l'horloge entre le fournisseur d'identité et l'ASA (SP).

```
ciscoasa(config)# ntp server 209.244.0.4
```

2. Obtenez les métadonnées SAML du fournisseur d'identité en suivant les procédures fournies par votre fournisseur d'identité tiers.

3. Importez le certificat de signature du fournisseur d'identité dans un point de confiance.

```
ciscoasa(config)# crypto ca trustpoint onelogin
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# no ca-check
ciscoasa(config-ca-trustpoint)# crypto ca authenticate onelogin
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
quit
INFO: Certificate has the following attributes:
Fingerprint:     85de3781 07388f5b d92d9d14 1e22a549
Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

4. Importez le certificat de signature PKCS12 du SP (ASA) dans un point de confiance

```
ciscoasa(config)# crypto ca import asa_saml_sp pkcs12 password
Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
quit
INFO: Import PKCS12 operation completed successfully
```

5. Ajoutez un fournisseur d'identité de SAML :

```
ciscoasa(config-webvpn)# saml idp https://app.onelogin.com/saml/metadata/462950
```

6. Configurez les attributs en sous-mode saml-idp :

   Configurez l'URL de connexion et l'URL de déconnexion du fournisseur d'identité :

```
ciscoasa(config-webvpn-saml-idp)# url sign-in
https://ross.onelogin.com/trust/saml2/http-post/sso/462950
ciscoasa(config-webvpn-saml-idp)# url sign-out
https://ross.onelogin.com/trust/saml2/http-redirect/slo/462950
```

   Configurez le point de confiance du fournisseur d'identité et le point de confiance du fournisseur de services (SP)

```
ciscoasa(config-webvpn-saml-idp)# trustpoint idp onelogin
ciscoasa(config-webvpn-saml-idp)# trustpoint sp asa_saml_sp
```

   Configurez l'URL de base du VPN sans client, la signature de requête SAML et le délai d'expiration (timeout) de l'assertion SAML :

```
ciscoasa(config-webvpn-saml-idp)# base-url https://172.23.34.222
ciscoasa(config-webvpn-saml-idp)# signature
ciscoasa(config-webvpn-saml-idp)# timeout assertion 7200
```

7. Configurez un fournisseur d'identité pour un groupe de tunnels et activez l'authentification SAML.

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
ciscoasa(config)# tunnel-group cloud_idp_onelogin type remote-access
ciscoasa(config)# tunnel-group cloud_idp_onelogin webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication saml
ciscoasa(config-tunnel-webvpn)# group-alias cloud_idp enable
ciscoasa(config-tunnel-webvpn)# saml identity-provider
https://app.onelogin.com/saml/metadata/462950
```

8. Affichez les métadonnées SAML SP de l'ASA :

   Vous pouvez obtenir les métadonnées SAML SP de l'ASA à l'adresse `https://172.23.34.222/saml/sp/metadata/cloud_idp_onelogin`. Dans l'URL, `cloud_idp_onelogin` est le nom du groupe de tunnels.

9. Configurez un fournisseur de services SAML sur votre fournisseur d'identité tiers en suivant les procédures fournies par votre fournisseur d'identité tiers.

Dépannage de SAML 2.0

Utilisez *la valeur* **debug webvpn saml** pour déboguer le comportement de SAML 2.0. Les messages SAML suivants s'afficheront en fonction de la *valeur* :

- 8 : erreurs
- 16 : avertissements et erreurs
- 128 ou 255 : débogage, avertissements et erreurs

Surveiller les connexions Secure Client (services client sécurisés).

Pour afficher des renseignements sur les sessions actives, utilisez la commande **show vpn-sessiondb** :

Commande	Objectif
show vpn-sessiondb	Affiche des renseignements sur les sessions actives.
vpn-sessiondb logoff	Déconnecte les sessions VPN.
show vpn-sessiondb AnyConnect (afficher vpn-sessiondb AnyConnect)	Améliore le résumé des sessions VPN pour afficher les renseig les sessions OSPFv3.
show vpn-sessiondb ratio encryption (afficher vpn-sessiondb ratio encryption)	Affiche le nombre de tunnels et les pourcentages pour les algo suite B (comme AES-GCM-128, AES-GCM-192, AES-GCM- AES-GMAC-128, etc.).

Remarque **AnyConnect Parent Tunnel** (Tunnel parent AnyConnect)

Les tunnels parents AnyConnect n'ont pas d'adresses IP attribuées.

Il s'agit de la session principale créée pendant la négociation afin d'établir le jeton de session nécessaire si une reconnexion s'impose en raison de problèmes de connectivité réseau ou d'une mise en veille prolongée. En fonction du mécanisme de connexion, Cisco Adaptive Security Appliance (ASA) répertorie la session comme sans client (lancement Web via le portail) ou parent (autonome AnyConnect).

AnyConnect parent représente la session lorsque le client n'est pas activement connecté. En pratique, il fonctionne comme un témoin, puisqu'il s'agit d'une entrée de base de données sur l'ASA qui correspond à la connexion d'un client particulier. Si le client est mis en veille ou en veille prolongée, les tunnels (protocoles IPsec/Internet Key Exchange [IKE]/Transport Layer Security [TLS]/Datagram Transport Layer Security [DTLS]) sont démontés, mais le Parent reste en place jusqu'à ce que le délai d'inactivité ou la durée maximale de connexion prenne effet. Cela permet à l'utilisateur de se reconnecter sans devoir se réauthentifier.

Exemple

Le champ Inactivity (Inactivité) affiche le temps écoulé depuis qu'une session Secure Client (services client sécurisés) a perdu la connectivité. Si la session est active, 00:00m:00s s'affiche dans ce champ.

```
hostname# show vpn-sessiondb

Session Type: SSL VPN Client

Username     : lee
Index        : 1                        IP Addr      : 209.165.200.232
Protocol     : SSL VPN Client           Encryption   : 3DES
Hashing      : SHA1                     Auth Mode    : userPassword
TCP Dst Port : 443                      TCP Src Port : 54230
Bytes Tx     : 20178                    Bytes Rx     : 8662
Pkts Tx      : 27                       Pkts Rx      : 19
Client Ver   : Cisco STC 1.1.0.117
Client Type  : Internet Explorer
Group        : DfltGrpPolicy
Login Time   : 14:32:03 UTC Wed Mar 20 2007
Duration     : 0h:00m:04s
Inactivity    : 0h:00m:04s
Filter Name  :

hostname# vpn-sessiondb logoff
INFO: Number of sessions of type "" logged off : 1

hostname# vpn-sessiondb logoff name tester
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "tester" logged off : 1
```

Déconnecter les sessions VPN AnyConnect

Pour déconnecter toutes les sessions VPN, utilisez la commande **vpn-sessiondb logoff** en mode de configuration globale :

L'exemple suivant déconnecte toutes les sessions VPN :

```
hostname# vpn-sessiondb logoff
INFO: Number of sessions of type "" logged off : 1
```

Vous pouvez déconnecter les sessions individuelles en utilisant l'argument du nom ou l'argument de l'index :

vpn-sessiondb logoff name *name*
vpn-sessiondb logoff index *index*

Les sessions qui ont été inactives le plus longtemps sont marquées comme inactives (et sont automatiquement déconnectées) de sorte que la capacité de licence n'est pas atteinte et que les nouveaux utilisateurs peuvent se connecter. Si la session reprend ultérieurement, elle est supprimée de la liste inactive.

Vous pouvez trouver à la fois le nom d'utilisateur et le numéro d'index (établi par l'ordre des images client) dans la sortie de la commande **show vpn-sessiondb anyconnect**. Les exemples suivants montrent le nom d'utilisateur *lee* et le numéro d'index *1*.

```
hostname# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : lee                    Index        : 1
Assigned IP  : 192.168.246.1           Public IP    : 10.139.1.2
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 11079                  Bytes Rx     : 4942
Group Policy : EngPolicy            Tunnel Group : EngGroup
Login Time   : 15:25:13 EST Fri Jan 28 2011
Duration     : 0h:00m:15s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

L'exemple suivant met fin à la session en utilisant l'option **name** de la commande **vpn-session-db logoff** :

```
hostname# vpn-sessiondb logoff name lee
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "lee" logged off : 1

hostname#
```

Historique des fonctionnalités pour les connexions Secure Client (services client sécurisés)

Le tableau suivant présente l'historique des versions de cette fonctionnalité.

Tableau 2 : Historique des fonctionnalités pour les connexions Secure Client (services client sécurisés)

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Connexions Secure Client (services client sécurisés)	7.2(1)	Les commandes suivantes ont été introduites ou modifiées : authent eap-proxy, authentification ms-chap-v1, authentification ms-chap-v authentification pap, tunnel hello l2tp, vpn-tunnel-protocol l2tp-ipse

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
IPsec IKEv2	v 8.4(1)	IKEv2 a été ajouté pour prendre en charge les connexions IPsec IKEv2 pc Client (services client sécurisés) et LAN à LAN.

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.