ASA 8.X : Configuration de la fonction Start Before Logon dans AnyConnect

Contenu

Introduction

Lorsque *Start Before Logon* (SBL) est activé, l'utilisateur voit la boîte de dialogue d'ouverture de session de l'interface utilisateur graphique d'AnyConnect avant que la boîte de dialogue d'ouverture de session de Windows® ne s'affiche. Ceci établit la connexion VPN d'abord. Disponible seulement pour des plates-formes Windows, le Start Before Logon permet à l'administrateur de contrôler l'utilisation des scripts de connexion, de la mise en cache de mot de passe, du mappage des lecteurs réseau aux lecteurs locaux, et plus. Vous pouvez employer la caractéristique SBL pour lancer le VPN en tant qu'élément de séquence de connexion. SBL est désactivé par défaut.

Pour plus d'informations sur la configuration des fonctionnalités du client VPN AnyConnect, reportez-vous à la section Configuration des fonctionnalités du client AnyConnect.

Remarque : Dans le client AnyConnect, la seule configuration que vous effectuez pour SBL est d'activer la fonctionnalité. Les administrateurs réseau gèrent le traitement qui se poursuit avant l'ouverture de session en fonction des besoins de leur situation. Les scripts d'ouverture de session peuvent être attribués à un domaine ou à des utilisateurs individuels. En règle générale, les administrateurs du domaine ont des fichiers de lot ou similaires définis avec des utilisateurs ou des groupes dans Active Directory. Dès que l'utilisateur se connecte, le script de connexion est

exécuté.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appareils de sécurité adaptatifs de la gamme Cisco ASA 5500 qui exécutent le logiciel version 8.x
- Cisco AnyConnect VPN version 2.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

SBL permet de connecter un ordinateur distant à l'infrastructure de l'entreprise avant de se connecter au PC. Par exemple, un utilisateur peut se trouver en dehors du réseau physique de l'entreprise et ne pas pouvoir accéder aux ressources de l'entreprise tant que son PC n'a pas rejoint le réseau de l'entreprise. Lorsque SBL est activé, le client AnyConnect se connecte avant que l'utilisateur ne voit la fenêtre de connexion Microsoft. L'utilisateur doit également se connecter, comme d'habitude, à Windows lorsque la fenêtre de connexion Microsoft apparaît.

Voici plusieurs raisons d'utiliser SBL :

- Le PC de l'utilisateur est joint à une infrastructure Active Directory.
- L'utilisateur ne peut pas disposer d'informations d'identification mises en cache sur le PC, c'est-à-dire si la stratégie de groupe désactive les informations d'identification mises en cache.
- L'utilisateur doit exécuter des scripts de connexion qui s'exécutent à partir d'une ressource réseau ou qui nécessitent un accès à une ressource réseau.
- Un utilisateur dispose de lecteurs mappés sur le réseau qui nécessitent une authentification avec l'infrastructure Active Directory.
- Les composants réseau, tels que MS NAP/CS NAC, peuvent nécessiter une connexion à l'infrastructure.

SBL crée un réseau équivalent à l'inclusion sur le réseau local de l'entreprise. Lorsque SBL est activé, puisque l'utilisateur a accès à l'infrastructure locale, les scripts d'ouverture de session qui

s'exécutent normalement pour un utilisateur du bureau sont également disponibles pour l'utilisateur distant.

Pour plus d'informations sur la création de scripts d'ouverture de session, reportez-vous à cet article Microsoft TechNet.

Pour plus d'informations sur l'utilisation de scripts d'ouverture de session locaux dans Windows XP, reportez-vous à cet article Microsoft.

Dans un autre exemple, un système peut être configuré pour interdire les informations d'identification mises en cache pour l'ouverture de session sur le PC. Dans ce scénario, les utilisateurs doivent pouvoir communiquer avec un contrôleur de domaine sur le réseau de l'entreprise pour que leurs informations d'identification soient validées avant d'accéder au PC. SBL nécessite la présence d'une connexion réseau au moment où elle est appelée. Dans certains cas, cela n'est pas possible car une connexion sans fil peut dépendre des informations d'identification de l'utilisateur pour se connecter à l'infrastructure sans fil. Étant donné que le mode SBL précède la phase des informations d'identification d'une connexion, aucune connexion n'est disponible dans ce scénario. Dans ce cas, la connexion sans fil doit être configurée pour mettre en cache les informations d'identification à travers la connexion, ou une autre authentification sans fil doit être configurée pour que SBL fonctionne.

Installer Démarrer avant de connecter les composants (Windows uniquement)

Les composants Start Before Logon doivent être installés après l'installation du client principal. En outre, les composants AnyConnect 2.2 Start Before Logon nécessitent l'installation de la version 2.2 ou ultérieure du logiciel client AnyConnect principal. Si vous pré-déployez le client AnyConnect et les composants Start Before Logon avec les fichiers MSI (par exemple, vous êtes dans une grande entreprise qui a son propre déploiement logiciel (Altiris, Active Directory ou SMS), vous devez obtenir la bonne commande. L'ordre de l'installation est traité automatiquement lorsque l'administrateur charge AnyConnect s'il est déployé sur le Web et/ou mis à jour sur le Web. Pour obtenir des informations complètes sur l'installation, reportez-vous aux Notes de version du client VPN Cisco AnyConnect, version 2.2.

Différences entre Windows-Vista\Windows 7 et Windows Vista Start Before Logon

Les procédures d'activation de SBL diffèrent légèrement sur les systèmes Windows Vista et Windows 7. Les systèmes pré-Vista utilisent un composant appelé VPNGINA (Virtual Private Network Grapical Identification and Authentication) pour implémenter SBL. Les systèmes Vista et Windows 7 utilisent un composant appelé PLAP pour implémenter SBL.

Dans le client AnyConnect, la fonction Démarrer avant connexion de Windows Vista est appelée Prestataire d'accès avant connexion (PLAP), qui est un fournisseur d'informations d'identification connectable. Cette fonctionnalité permet aux administrateurs réseau d'effectuer des tâches spécifiques, telles que la collecte d'informations d'identification ou la connexion aux ressources réseau, avant de se connecter. PLAP fournit des fonctions de démarrage avant connexion sur Windows Vista, Windows 7 et le serveur Windows 2008. PLAP prend en charge les versions 32 bits et 64 bits du système d'exploitation avec vpnplap.dll et vpnplap64.dll, respectivement. La fonction PLAP prend en charge les versions Windows Vista x86 et x64.

Remarque : Dans cette section, VPNGINA fait référence à la fonctionnalité Démarrer avant

connexion pour les plates-formes pré-Vista, et PLAP fait référence à la fonctionnalité Démarrer avant connexion pour les systèmes Windows Vista et Windows 7.

Dans les systèmes pré-Vista, Start Before Logon utilise un composant appelé VPN Graphical Identification and Authentication Dynamic Link Library (vpngina.dll) pour fournir les fonctionnalités Start Before Logon. Le composant Windows PLAP, qui fait partie de Windows Vista, remplace le composant Windows GINA.

Un GINA est activé lorsqu'un utilisateur appuie sur la combinaison de touches Ctrl+Alt+Suppr. Avec PLAP, la combinaison de touches Ctrl+Alt+Suppr ouvre une fenêtre dans laquelle l'utilisateur peut choisir de se connecter au système ou d'activer n'importe quelle connexion réseau (composants PLAP) avec le bouton Connexion réseau dans le coin inférieur droit de la fenêtre.

Les sections qui suivent décrivent immédiatement les paramètres et les procédures pour VPNGINA et PLAP SBL. Pour obtenir une description complète de l'activation et de l'utilisation de la fonctionnalité SBL (PLAP) sur une plate-forme Windows Vista, reportez-vous à Configuration du démarrage avant connexion (PLAP) sur les systèmes Windows Vista.

Paramètres XML pour activer SBL

La valeur de l'élément UseStartBeforeLogon permet d'activer (true) ou de désactiver (false) cette fonctionnalité. Si vous définissez cette valeur sur **true** dans le profil, un traitement supplémentaire est effectué dans le cadre de la séquence d'ouverture de session. Pour plus d'informations, reportez-vous à la description Start Before Logon. Définissez la valeur <UseStartBefore Logon> dans le fichier CiscoAnyConnect.xml sur **true** pour activer SBL :

```
<?xml version="1.0" encoding="UTF-8" ?>
<Configuration>
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
```

Afin de désactiver SBL, définissez la même valeur sur **false**.

Afin d'activer la fonctionnalité UserControllable, utilisez cette instruction lorsque vous activez SBL :

```
<UseStartBeforeLogon userControllable="false">true</UseStartBeforeLogon>
```

Tout paramètre utilisateur associé à cet attribut est stocké ailleurs.

Activer SBL

Afin de minimiser le temps de téléchargement, le client AnyConnect demande des téléchargements (à partir de l'appliance de sécurité) uniquement des modules de base dont il a besoin pour chaque fonctionnalité qu'il prend en charge. Afin d'activer de nouvelles fonctionnalités, telles que SBL, vous devez spécifier le nom de module avec la commande **svc modules** à partir du mode de configuration WebVPN de stratégie de groupe ou WebVPN de nom d'utilisateur :

```
[no] svc modules {none | value string}
```

La valeur de chaîne pour SBL est **vpngina**.

Dans cet exemple, l'administrateur réseau passe en mode d'attributs de stratégie de groupe pour les télétravailleurs de stratégie de groupe ; passe en mode de configuration WebVPN pour la stratégie de groupe ; et spécifie la chaîne VPNGINA pour activer SBL :

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

En outre, l'administrateur doit s'assurer que le fichier <profile.xml> AnyConnect, où <profile.xml> est le nom que l'administrateur réseau a attribué au fichier XML, a la valeur **true** pour l'instruction <UseStartBeforeLogon>, par exemple :

```
UseStartBeforeLogon UserControllable="false">true
```

Le système doit être redémarré avant que le démarrage ne prenne effet. Vous devez également spécifier sur l'appliance de sécurité que vous voulez autoriser SBL, ou tout autre module pour des fonctionnalités supplémentaires. Reportez-vous à la description de la section Activation des modules pour des fonctionnalités AnyConnect supplémentaires, page 2-5 (ASDM) ou Activation des modules pour des fonctionnalités AnyConnect supplémentaires, page 3-4 (CLI) pour plus d'informations.

Démarrer avant la configuration de connexion avec CLI

Ce scénario vous montre comment configurer le fichier XML avec l'interface de ligne de commande :

1. Créez un profil à transmettre aux PC clients qui ressemble à ceci :
   ```
   <?xml version="1.0" encoding="UTF-8" ?>
   <AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi :schemaLocation=
      "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
   <ClientInitialization>
   <UseStartBeforeLogon>true</UseStartBeforeLogon>
   </ClientInitialization>
   <ServerList>
   <HostEntry>
   <HostName>text.cisco.com</HostName>
   </HostEntry>
   <HostEntry>
   <HostName>test1.cisco.com</HostName>
   <HostAddress>1.1.1.1</HostAddress>
   </HostEntry>
   .
   .
   .
   <HostEntry>
   <HostName>test2.cisco.com</HostName>
   <HostAddress>1.1.1.2</HostAddress>
   </HostEntry>
   </ServerList>
   </AnyConnectProfile>
   ```
2. Copiez le fichier dans la mémoire Flash sur l'appliance de sécurité :

```
Copy tftp://x.x.x.x/AnyConnectProfile.xml AnyConnectProfile.xml
```

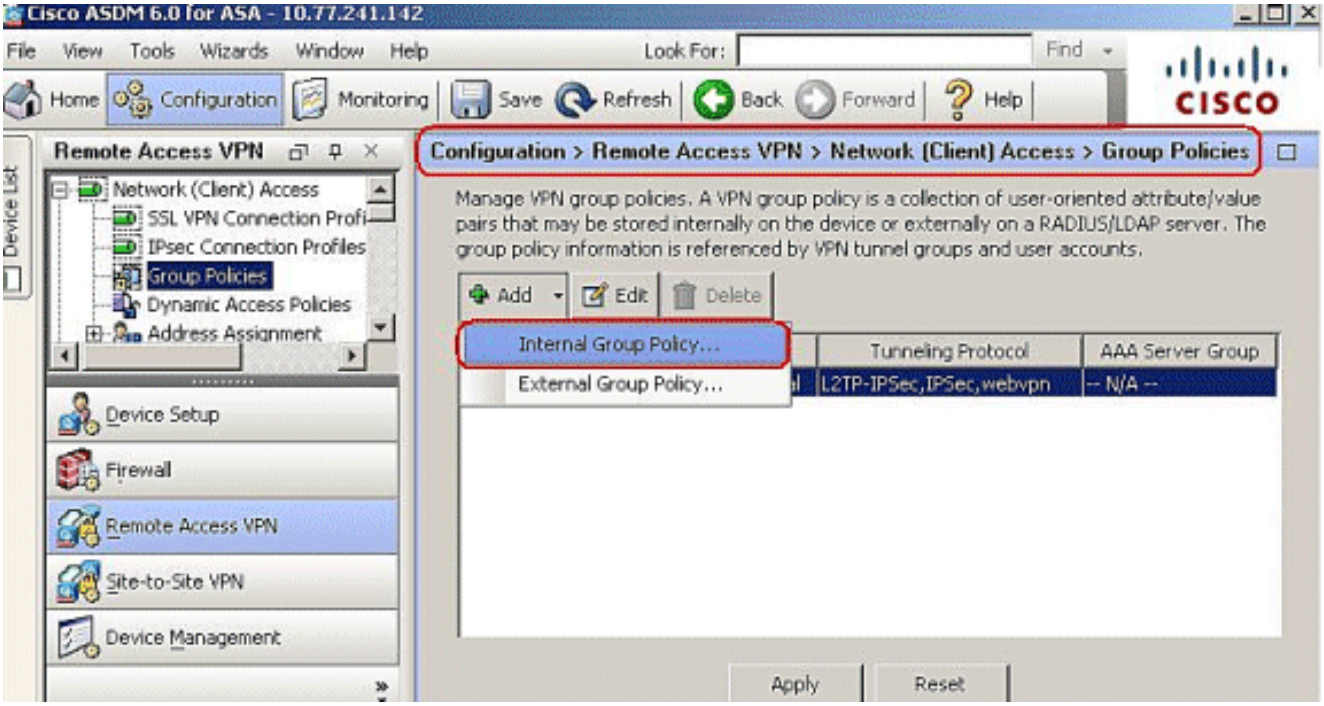
3. Sur le dispositif de sécurité, ajoutez le profil en tant que profil disponible à la section globale WebVPN, à condition que tout le reste soit correctement configuré pour les connexions AnyConnect :
```
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)#
   svc profiles ReallyNewProfile disk0:/AnyConnectProfile.xml
```

4. Modifiez la stratégie de groupe que vous utilisez et ajoutez les commandes **svc modules** et **profil svc** :
```
hostname(config)# group-policy GroupPolicy internal
hostname(config)# group-policy GroupPolicy attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc modules value vpngina
hostame(config-group-webvpn)# svc profiles value ReallyNewProfile
```

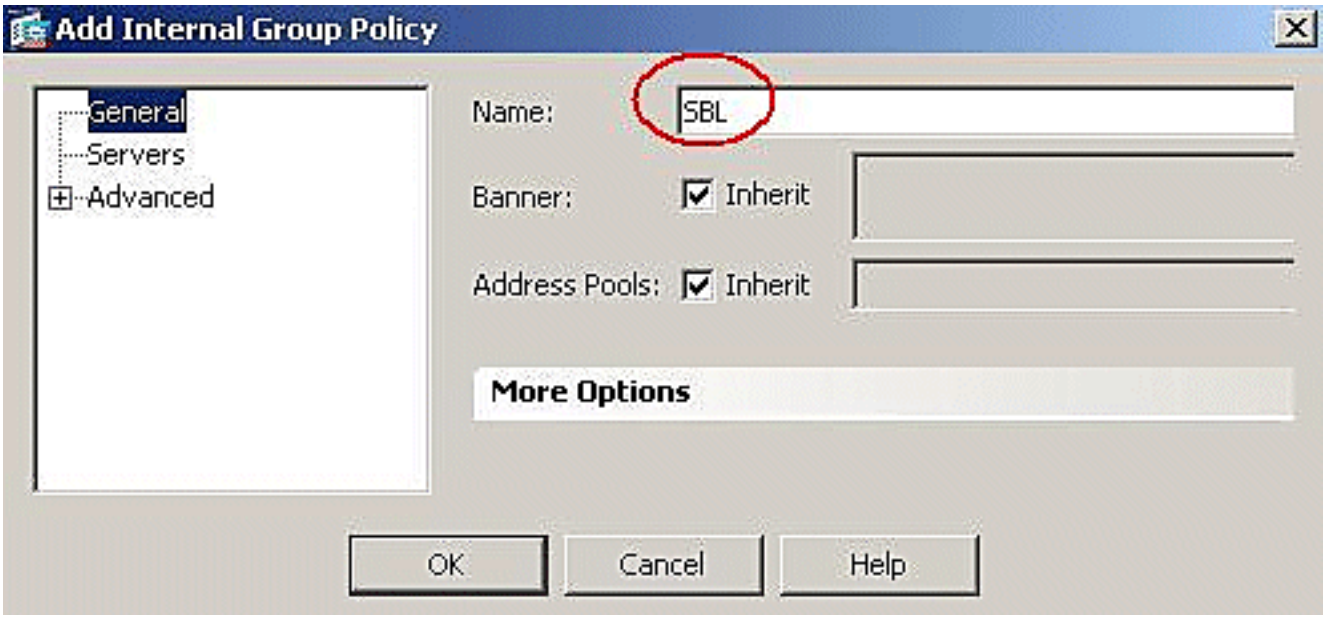
Démarrer avant la configuration de connexion avec ASDM

Complétez ces étapes pour configurer SBL avec ASDM :

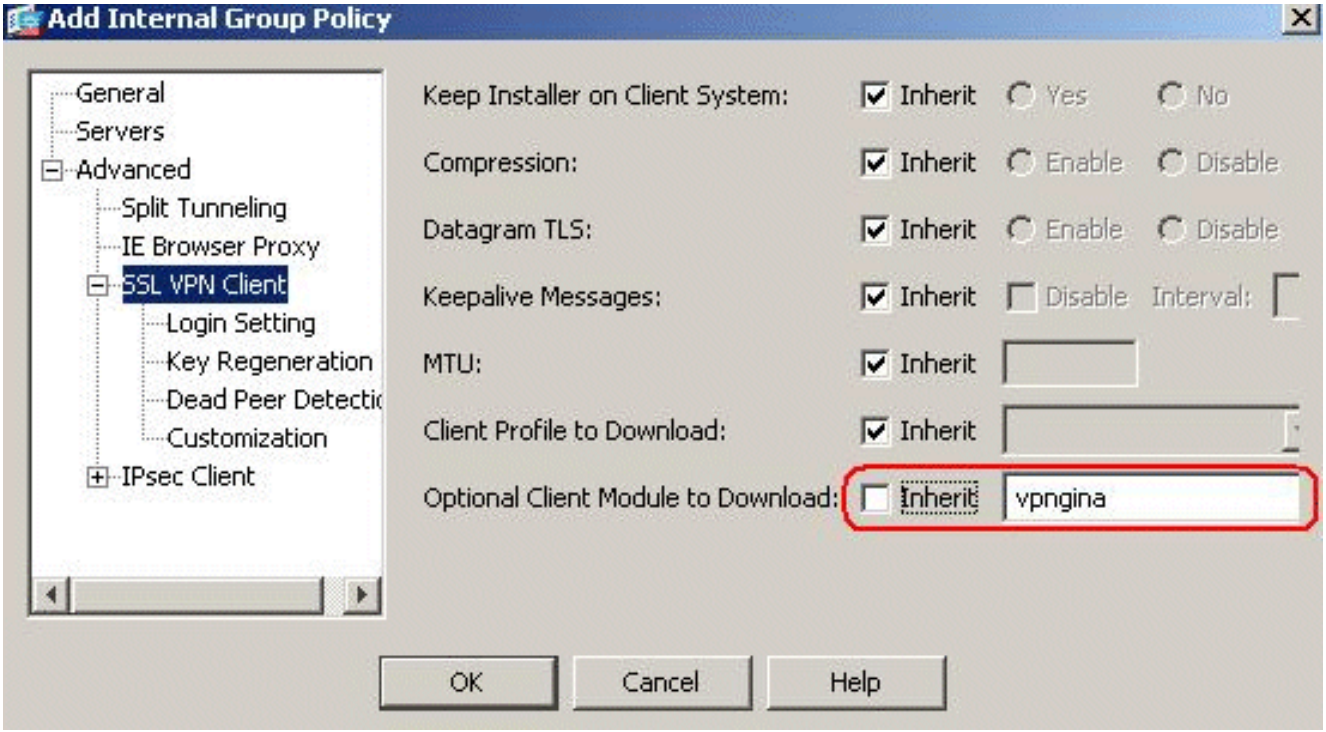
1. Créez un profil à transmettre aux PC clients qui ressemble à ceci :
```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon>true</UseStartBeforeLogon>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>text.cisco.com</HostName>
</HostEntry>
<HostEntry>
<HostName>test1.cisco.com</HostName>
<HostAddress>1.1.1.1</HostAddress>
</HostEntry>
.
.
.
<HostEntry>
<HostName>test2.cisco.com</HostName>
<HostAddress>1.1.1.2</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```
2. Enregistrez le profil sous **AnyConnectProfile.xml** sur l'ordinateur local.
3. Lancez l'ASDM et accédez à la page d'accueil.
4. Accédez à **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add**, puis cliquez sur **Internal Group Policy**.



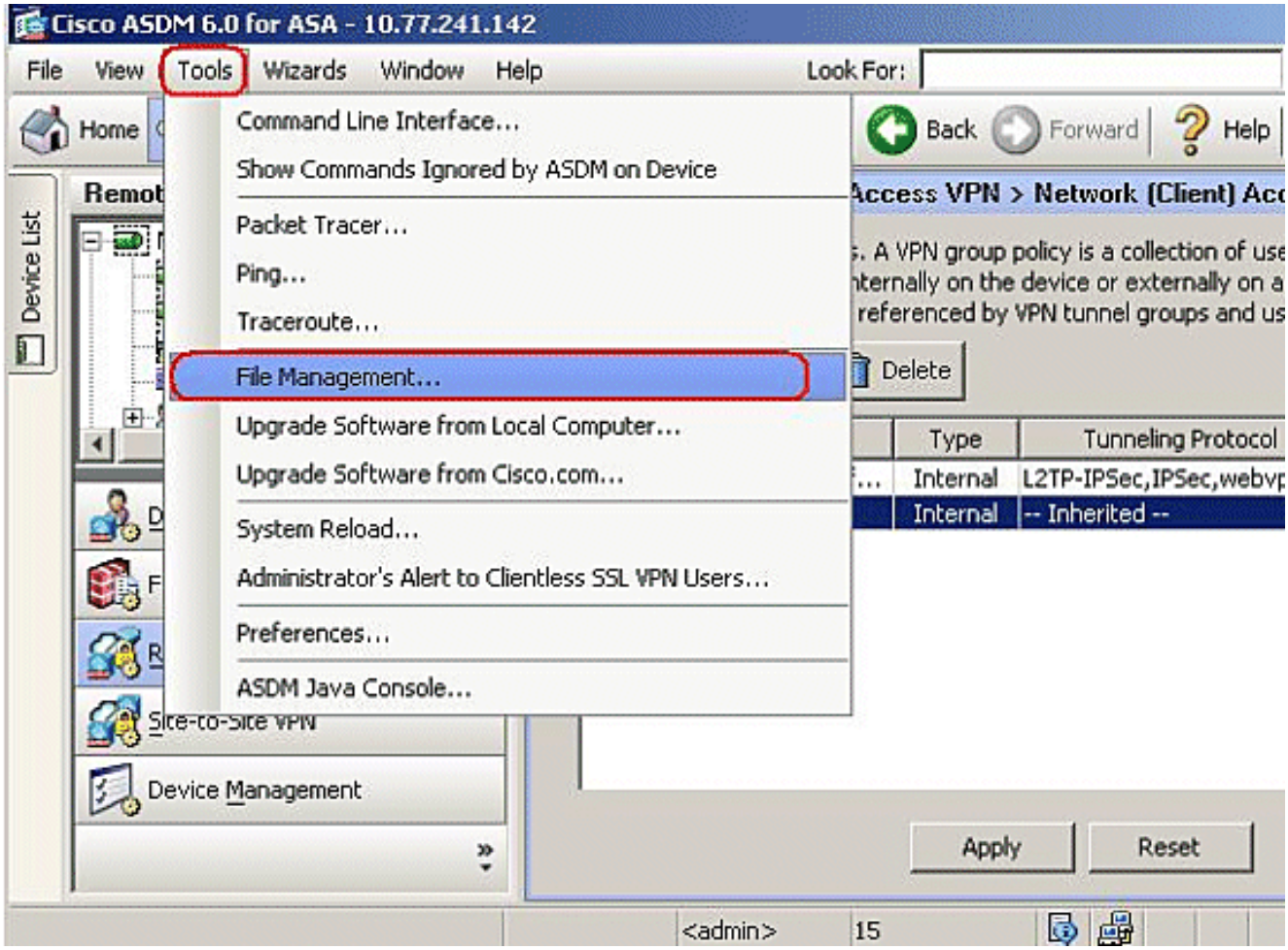
5. Entrez le nom de la stratégie de groupe, par exemple **SBL**.



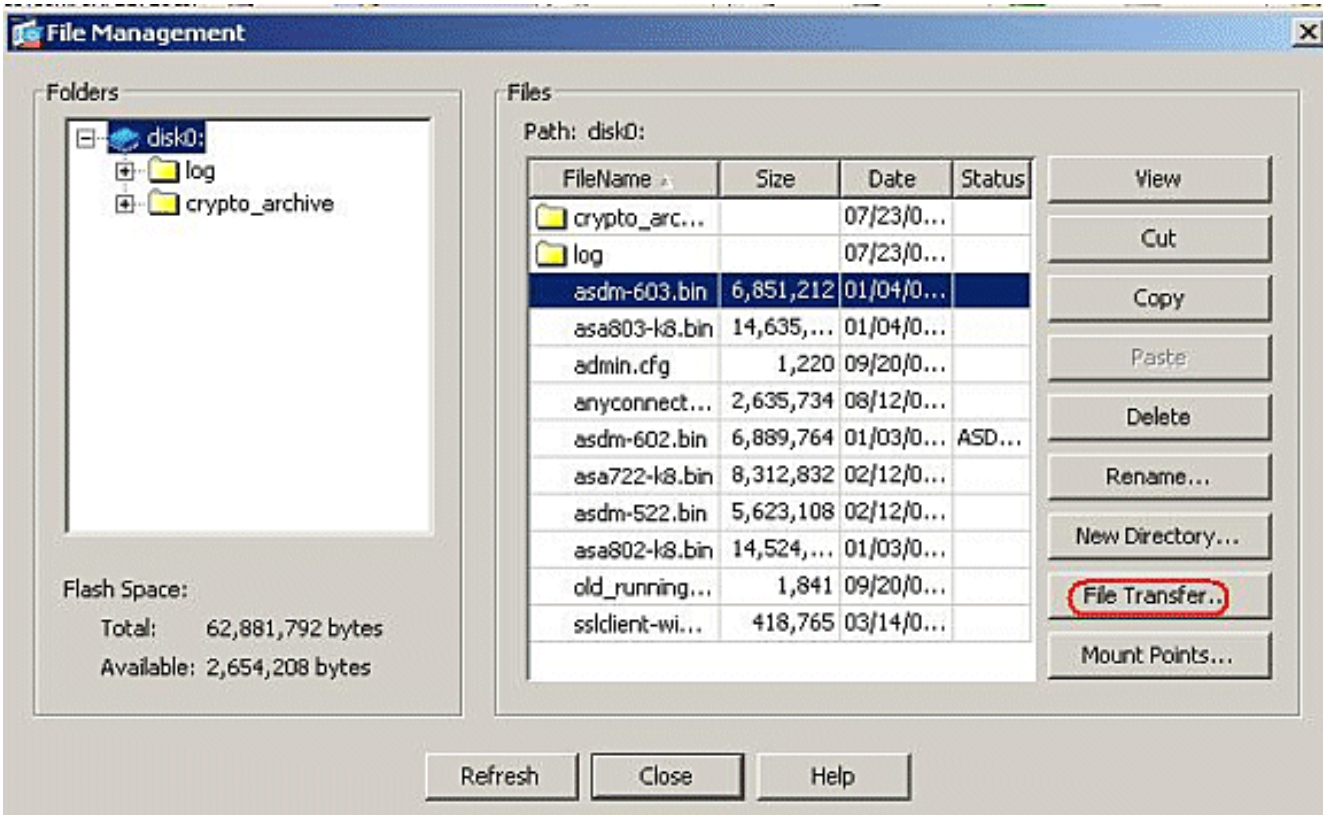
6. Accédez à **Advanced > SSL VPN Client**. Désactivez la case à cocher Hériter dans le **module client facultatif à télécharger**, puis sélectionnez **vpngina** dans la liste déroulante.



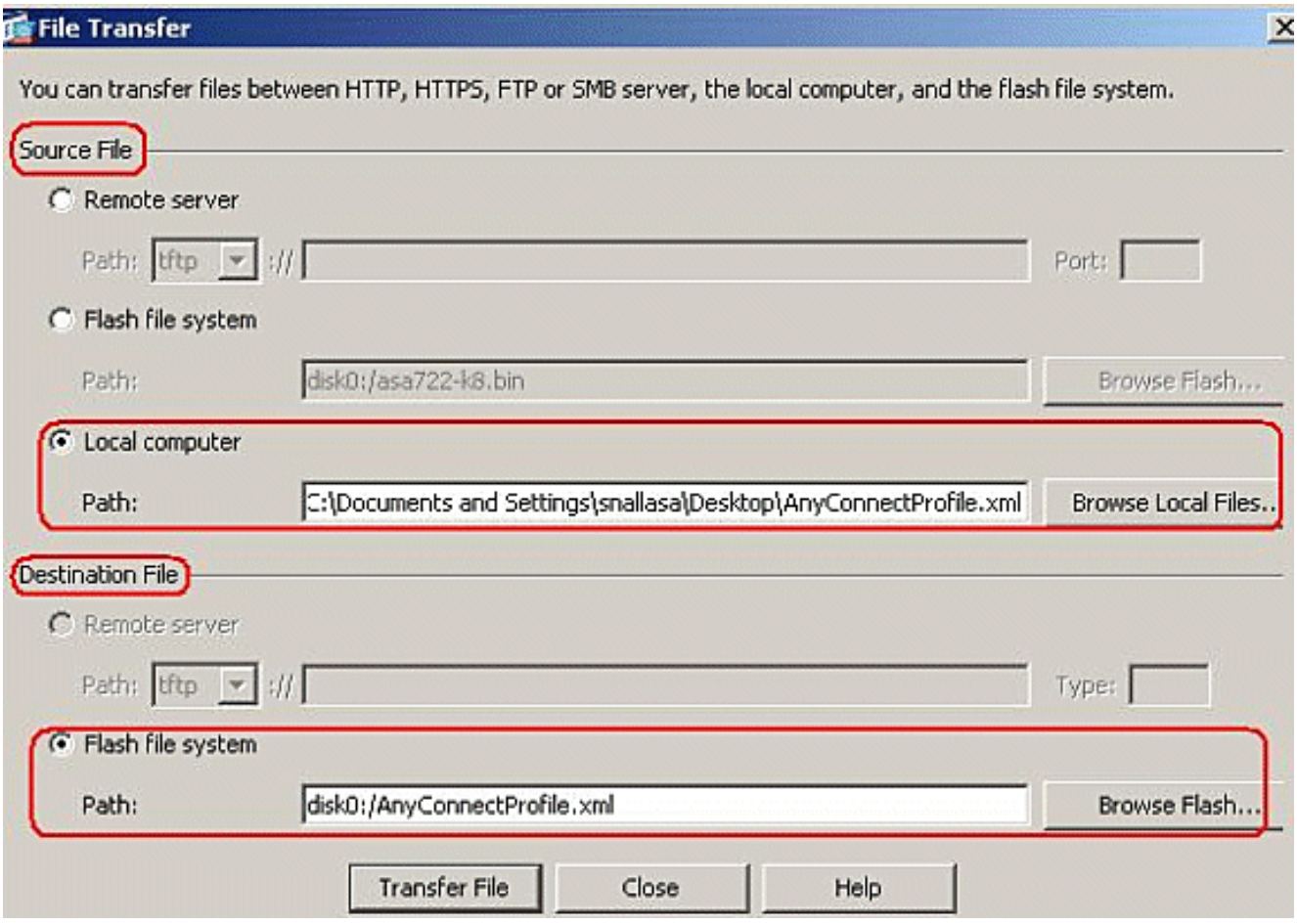
7. Afin de transférer le profil **AnyConnectProfile.xml** de l'ordinateur local vers Flash, accédez à **Outils**, puis cliquez sur **Gestion des fichiers**.



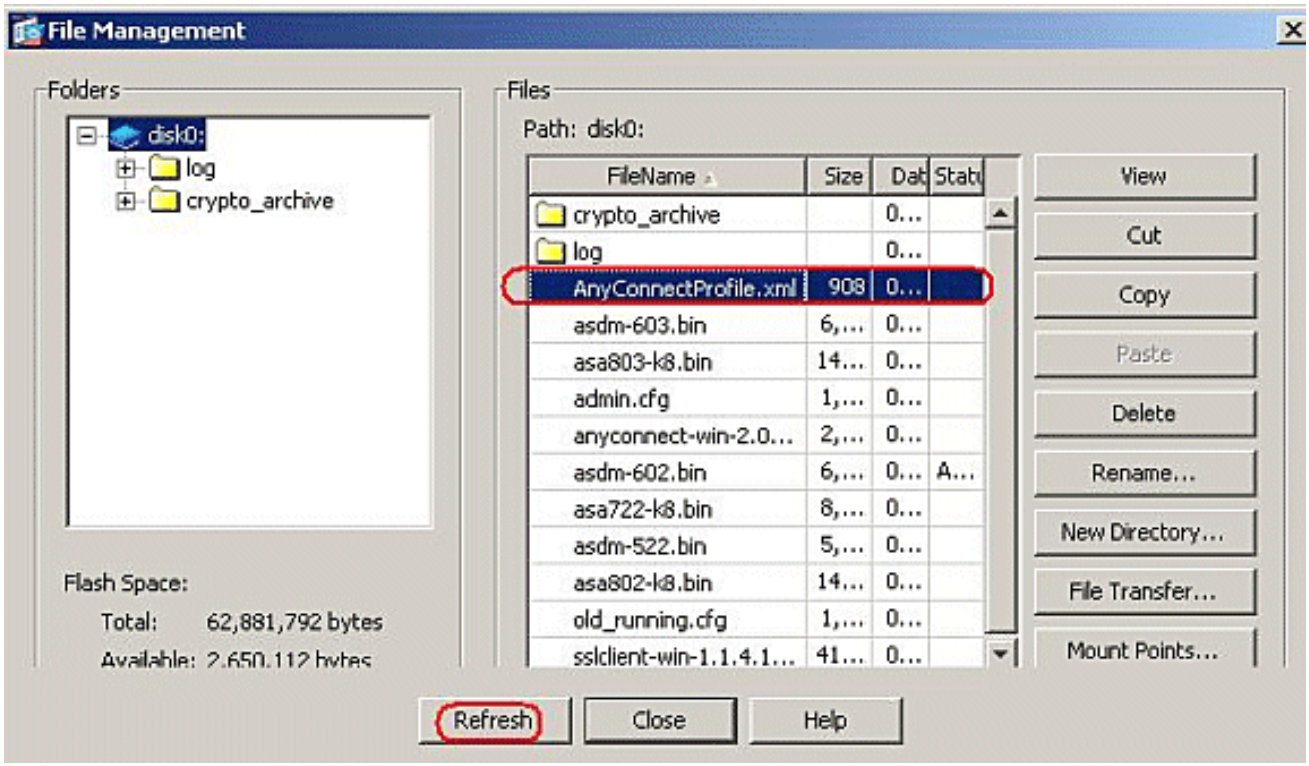
8. Cliquez sur le bouton **Transfert de fichiers**.



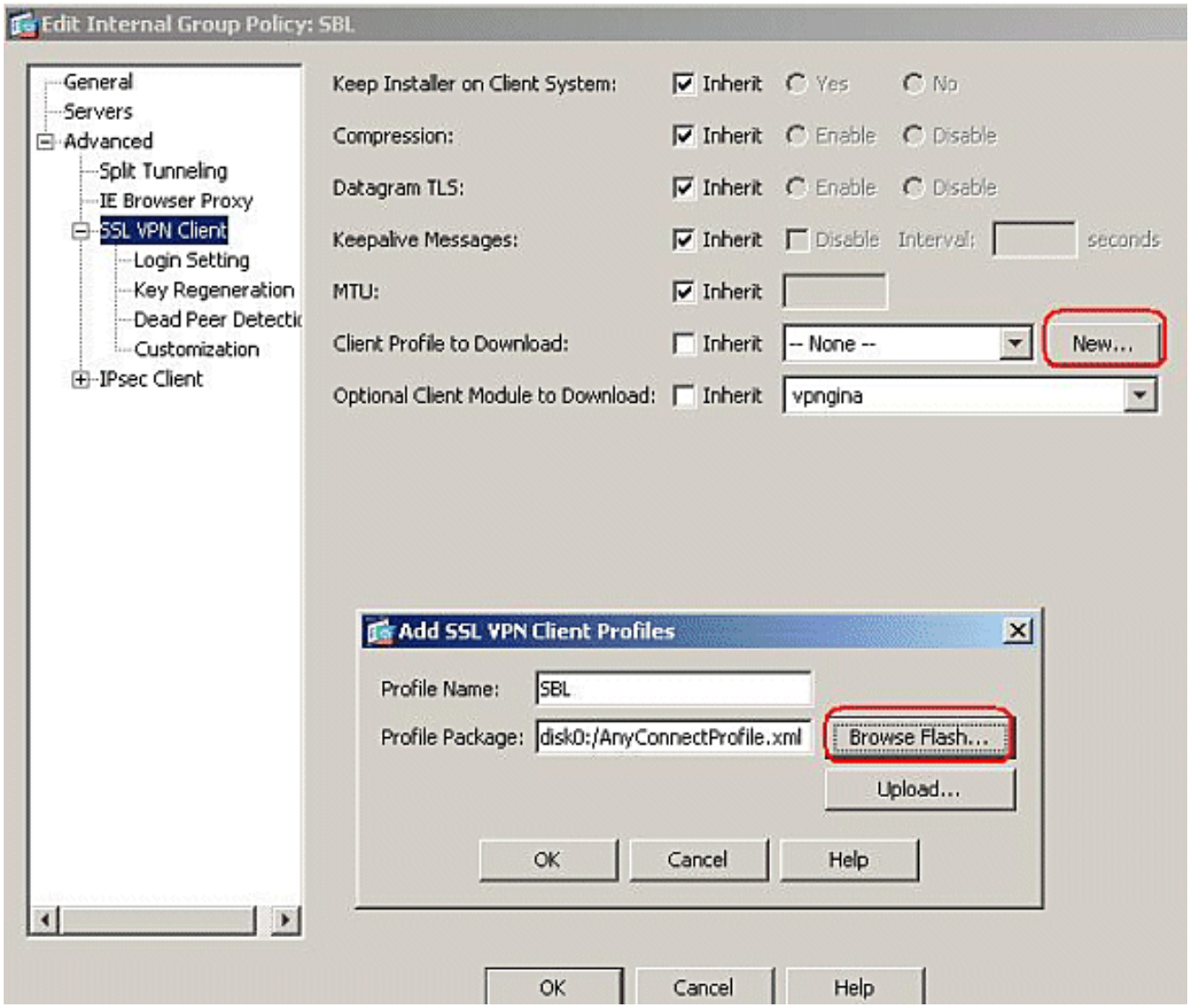
9. Afin de transférer le profil de l'ordinateur local vers la mémoire Flash ASA, choisissez le **fichier source**, le chemin du fichier XML (ordinateur local) et le chemin du **fichier de destination** selon vos
besoins.



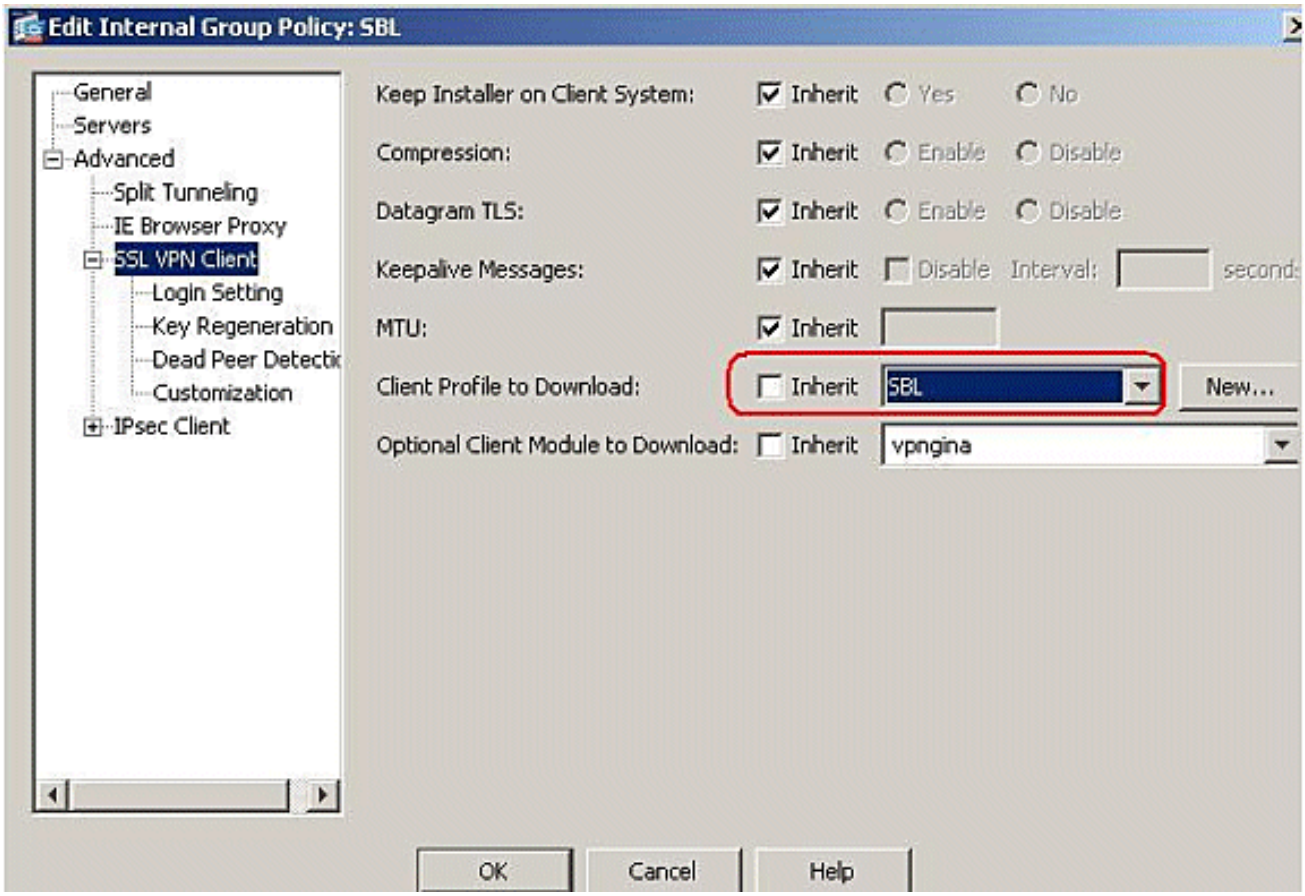
10. Après le transfert, cliquez sur le bouton **Actualiser** pour vérifier si le fichier de profil se trouve dans la mémoire
Flash.



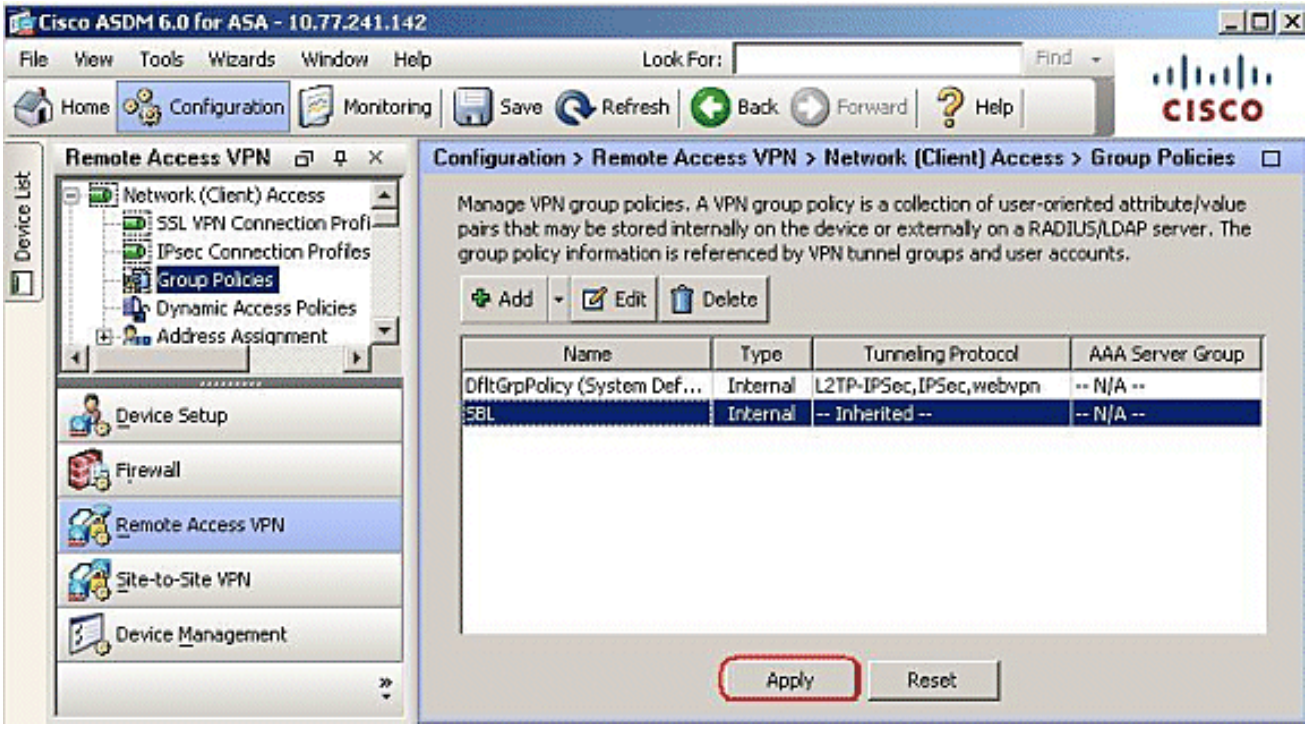
11. Affectez le profil à la stratégie de groupe interne (**SBL**).Suivez ce chemin, **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Edit SBL (Internal Group Policy) > Advanced > SSL VPN Client > Client Profile to Download**, puis cliquez sur le bouton **New**.Dans la section **Ajouter des profils client VPN SSL**, cliquez sur le bouton **Parcourir** pour choisir l'emplacement du profil (**AnyConnectProfile.xml**) stocké dans la mémoire Flash ASA. Attribuez le **nom** du profil, par exemple **SBL**. Cliquez sur **OK pour terminer.**



12. Désactivez la case à cocher Hériter et sélectionnez **SBL** dans le champ **Profil client à télécharger**. Click
    OK.



13. Cliquez sur **Apply** pour terminer.



Utiliser le fichier manifeste

Le package AnyConnect téléchargé sur l'appliance de sécurité contient un fichier appelé VPNManifest.xml. Cet exemple montre un exemple de contenu de ce fichier :

```
<?xml version="1.0" encoding="UTF-7"?> <vpn rev="1.0">
<file version="2.1.0150" id="VPNCore"
```

```
   is_core="yes" type="exe" action="install">
   <uri>binaries/anyconnect-win-2.1.0150-web-deploy-k9.exe</uri>
 </file>
 <file version="2.1.0150" id="gina"
   is_core="yes" type="exe" action="install" module="vpngina">
   <uri>binaries/anyconnect-gina-win-2.1.0150-web-deploy-k9.exe</uri>
 </file>
</vpn>
```

L'appliance de sécurité a enregistré sur ses profils configurés, comme expliqué à l'étape 1, et elle stocke également un ou plusieurs packages AnyConnect qui contiennent le client AnyConnect lui-même, l'utilitaire de téléchargement, le fichier manifeste et tout autre module ou fichier de support facultatif.

Lorsqu'un utilisateur distant se connecte à l'appliance de sécurité avec WebLaunch ou un client autonome en cours, le téléchargeur est d'abord téléchargé et exécuté. Il utilise le fichier manifeste pour déterminer s'il existe un client en cours sur le PC de l'utilisateur distant qui doit être mis à niveau ou s'il est nécessaire d'effectuer une nouvelle installation. Le fichier manifeste contient également des informations sur l'existence ou non de modules facultatifs devant être téléchargés et installés, dans ce cas, le VPNGINA. Le profil client est également désactivé à partir de l'appliance de sécurité. L'installation de VPNGINA est activée par la commande **svc modules value vpngina** configurée sous le mode de commande **group-policy (webvpn)** comme expliqué à l'étape 4. Le client AnyConnect et VPNGINA sont installés et l'utilisateur voit le client AnyConnect au prochain redémarrage, avant l'ouverture de session du domaine Windows.

Lorsque l'utilisateur se connecte, le client et le profil sont transmis au PC de l'utilisateur ; le client et VPNGINA sont installés ; et l'utilisateur voit le client AnyConnect au prochain redémarrage, avant de se connecter.

Un exemple de profil est fourni sur le PC client lors de l'installation d'AnyConnect : **C:\Documents and Settings\All Users\Application Data\Cisco\Cisco\AnyConnect VPN Client\Profile\AnyConnectProfile**.

Dépannage de SBL

Utilisez cette procédure si vous rencontrez un problème avec SBL :

1. Assurez-vous que le profil est poussé.
2. Supprimer les profils antérieurs ; recherchez-les sur le disque dur pour trouver l'emplacement : *.xml.
3. Lorsque vous accédez aux programmes Add/Remove, avez-vous une installation AnyConnect et une installation AnyConnect VPNGINA ?
4. Désinstallez le client AnyConnect.
5. Effacez le journal AnyConnect de l'utilisateur dans l'Observateur d'événements et retestez.
6. Revenez à l'appliance de sécurité pour réinstaller le client.
7. Assurez-vous que le profil apparaît également.
8. Redémarrer une fois. Lors du prochain redémarrage, l'invite Start Before Logon vous invite.
9. Envoyez le journal des événements AnyConnect à Cisco au format .evt .
10. Si vous voyez cette erreur, supprimez le profil utilisateur et utilisez le profil par défaut :

    ```
    Description: Unable to parse the profile
    C:\Documents and Settings\All Users\Application Data\Cisco
    \Cisco AnyConnect VPN Client\Profile\VABaseProfile.xml.
    Host data not available.
    ```

Problème 1

Ce message d'erreur s'affiche lors de la tentative de téléchargement du profil AnyConnect : `Erreur lors de la validation du fichier XML par rapport au dernier schéma`. Comment cette erreur est-elle résolue ?

Solution 1

Ce message d’erreur se produit principalement en raison de problèmes de syntaxe ou de configuration dans le profil AnyConnect. Afin de résoudre ce problème, assurez-vous que le profil AnyConnect configuré est similaire à l'exemple de profil AnyConnect présent dans la section Exemple de profil AnyConnect et schéma XML du Guide d'administration du client VPN Cisco AnyConnect.

Informations connexes

- Guide de l'administrateur Cisco AnyConnect VPN Client, Version 2.0
- Création de scripts d'ouverture de session - Windows TechNet
- Configuration du programme de démarrage avant ouverture de session (PLAP) sur les systèmes Windows Vista
- Exemple de configuration de l'accès VPN ASA 8.x avec le client VPN SSL AnyConnect
- Cisco AnyConnect VPN Client
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Support et documentation techniques - Cisco Systems