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

Contenu

Introduction

Le Start Before Logon (SBL) étant activé, l'utilisateur voit le dialogue d'entrée en communication GUI d'AnyConnect avant que la boîte de dialogue de connexion de ® de Windows apparaisse. 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 configurer des caractéristiques d'AnyConnect VPN Client, référez-vous à la section configurant des fonctionnalités client d'AnyConnect.

Remarque: Chez le client d'AnyConnect, la seule configuration que vous faites pour SBL est d'activer la caractéristique. Les administrateurs réseau effectuent le traitement cela continue avant la connexion basée sur les conditions requises de leur situation. Des scripts de connexion peuvent être assignés à un domaine ou aux utilisateurs individuels. Généralement, les administrateurs du domaine ont des fichiers batch ou analogues définis avec des utilisateurs ou des groupes dans le Répertoire actif. Dès que l'utilisateur ouvrira une session, le script de connexion est exécuté.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 cette version de logiciel 8.x de passage
- Version 2.0 du Cisco AnyConnect VPN

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Informations générales

Le point de SBL est qu'il connecte un ordinateur distant à l'infrastructure de société avant la connexion au PC. Par exemple, un utilisateur peut être en dehors du réseau d'entreprise physique, incapable d'accéder à des ressources de l'entreprise jusqu'à ce que son PC ait joint le réseau d'entreprise. Le SBL étant activé, le client d'AnyConnect se connecte avant que l'utilisateur voie la fenêtre de connexion de Microsoft. L'utilisateur doit également ouvrir une session, comme d'habitude, à Windows quand la fenêtre de connexion de Microsoft apparaît.

Ce sont plusieurs raisons d'utiliser SBL :

- Le PC de l'utilisateur est joint à une infrastructure de Répertoire actif.
- L'utilisateur ne peut pas avoir caché des qualifications sur le PC, c.-à-d., si la stratégie de groupe rejette les qualifications cachées.
- L'utilisateur doit exécuter les scripts de connexion qui exécutent d'une ressource de réseau ou qui exigent l'accès à une ressource de réseau.
- Un utilisateur réseau-a tracé les lecteurs qui ont besoin de l'authentification avec l'infrastructure de Répertoire actif.
- Les composants réseau, tels que le MS NAP/CS NAC, peuvent exiger la connexion à l'infrastructure.

SBL crée un réseau qui est équivalent à l'intégration sur le RÉSEAU LOCAL entreprise local. Le SBL étant activé, puisque l'utilisateur a accès à l'infrastructure locale, les scripts de connexion que normalement exécuté pour un utilisateur dans le bureau soyez également à la disposition de l'utilisateur distant.

Pour des informations sur la façon créer des scripts de connexion, référez-vous à cet article de TechNet de Microsoft .

Pour des informations sur la façon utiliser les scripts de connexion locaux dans Windows XP, référez-vous à cet article de Microsoft .

Dans un autre exemple, un système peut être configuré pour rejeter les qualifications cachées pour la connexion au PC. Dans ce scénario, les utilisateurs doivent pouvoir communiquer avec un contrôleur de domaine sur le réseau d'entreprise pour que leurs qualifications soient validées avant l'accès au PC. SBL exige d'une connexion réseau d'être présente lorsqu'il est appelé. Dans certains cas, ce n'est pas possible parce qu'une connexion Sans fil peut dépendre des identifiants utilisateurs pour se connecter à l'infrastructure Sans fil. Puisque le mode SBL précède la phase de créance d'une procédure de connexion, une connexion n'est pas disponible dans ce scénario. Dans ce cas, la connexion Sans fil doit être configurée pour cacher les qualifications à travers la procédure de connexion, ou une autre authentification Sans fil doit être configurée pour que SBL fonctionne.

Installez les composants de Start Before Logon (Windows seulement)

Les composants de Start Before Logon doivent être installés après que le principal client ait été installé. Supplémentaire, l'AnyConnect 2.2 composants de Start Before Logon exigent cette version 2.2, ou plus tard, du principal logiciel de client d'AnyConnect soyez installé. Si vous déployez à l'avance le client d'AnyConnect et les composants de Start Before Logon avec les fichiers MSI (par exemple, vous êtes à une grande société qui a son propre déploiement de progiciels (Altiris, Répertoire actif, ou SMS), vous devez obtenir la droite de commande. La commande de l'installation est manipulée automatiquement quand l'administrateur charge AnyConnect si c'est Web déployé et/ou Web mis à jour. Pour les informations complètes d'installation, référez-vous aux notes en version pour le Cisco AnyConnect VPN Client, version 2.2.

Différences entre les Windows Vista \ Windows 7 et le Start Before Logon de Pré-vista

Les procédures pour activer SBL diffèrent légèrement sur des systèmes de Windows Vista et de Windows 7. Les systèmes de Pré-vista utilisent un composant appelé l'identification graphique de réseau privé virtuel et l'authentification (VPNGINA) pour implémenter SBL. Les systèmes de vista et de Windows 7 utilisent un composant appelé le PLAP pour implémenter SBL.

Dans le client d'AnyConnect, la caractéristique de Start Before Logon de Windows Vista est connue en tant que fournisseur Internet De Pré-procédure de connexion (PLAP), qui est un fournisseur de créance raccordable. Cette caractéristique permet des administrateurs réseau d'effectuer des tâches spécifiques, telles que la collecte de qualifications ou de connexion aux ressources de réseau, avant la procédure de connexion. PLAP fournit des fonctions de Start Before Logon sur les Windows Vista, le Windows 7 et le serveur de Windows 2008. PLAP prend en charge des versions de 32 bits et 64-bit du système d'exploitation avec vpnplap.dll et vpnplap64.dll, respectivement. La fonction PLAP prend en charge les versions x86 et x64 de Windows Vista.

Remarque: Dans cette section, VPNGINA se rapporte à la caractéristique de Start Before Logon pour des Plateformes de pré-vista, et PLAP se rapporte à la caractéristique de Start Before Logon

pour des systèmes de Windows Vista et de Windows 7.

Dans des systèmes de pré-vista, le Start Before Logon utilise un composant connu sous le nom de bibliothèque de liens dynamiques graphique d'identification et d'authentification VPN (vpngina.dll) pour fournir des capacités de Start Before Logon. Le composant de Windows PLAP, qui fait partie des Windows Vista, remplace le composant de Windows GINA.

GINA est lancée quand un utilisateur appuie sur la combinaison de touches Ctrl+Alt+Del. Avec PLAP, la combinaison de touches Ctrl+Alt+Del ouvre une fenêtre où l'utilisateur peut choisir d'ouvrir une session au système ou de lancer toutes les connexions réseau (composants PLAP) avec le bouton Connect de réseau dans l'angle inférieur droit de la fenêtre.

Les sections qui suivent immédiatement décrivent les configurations et les procédures pour VPNGINA et PLAP SBL. Pour une description complète de l'activation et de l'utilisation de la caractéristique SBL (PLAP) sur une plate-forme de Windows Vista, référez-vous à configurer le Start Before Logon (PLAP) sur des systèmes de Windows Vista.

Configurations XML pour activer SBL

La valeur d'élément pour UseStartBeforeLogon permet cette caractéristique à activer (vrai) ou hors fonction (faux). Si vous placez cette valeur **pour rectifier** dans le profil, le traitement supplémentaire se produit en tant qu'élément de l'ordre de connexion. Voyez la description de Start Before Logon pour des détails supplémentaires. Placez la valeur de Logon**>** de **<**UseStartBefore dans le fichier CiscoAnyConnect.xml à l'enable SBL de trueto :

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

Afin de désactiver SBL, placez la même valeur à **faux**.

Afin d'activer la caractéristique d'UserControllable, utilisez cette déclaration quand vous activez SBL :

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

N'importe quel paramètre utilisateur associé avec cet attribut est enregistré ailleurs.

Enable SBL

Afin de réduire le temps du téléchargement, le client d'AnyConnect demande des téléchargements (des dispositifs de sécurité) seulement des principaux modules des lesquels ils ont besoin pour chaque caractéristique qu'ils prennent en charge. Afin d'activer de nouvelles caractéristiques, telles que SBL, vous devez spécifier le nom du module avec la commande de **modules de svc du** webvpn de stratégie de groupe ou du mode de configuration de 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 entre le mode d'attributs de stratégie de groupe pour les télétravailleurs de stratégie de groupe ; écrit le mode de configuration de 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 d'AnyConnect <profile.xml>, où <profile.xml> est le nom que l'administrateur réseau a assigné au fichier XML, a la déclaration de <UseStartBeforeLogon> réglée pour rectifier, **par exemple** :

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

Le système doit être redémarré avant que le Start Before Logon le prenne effet. Vous devez également spécifier sur les dispositifs de sécurité que vous voulez pour permettre SBL, ou tous les autres modules pour des fonctionnalités supplémentaires. Référez-vous à la description dans les modules de activation pour les caractéristiques supplémentaires d'AnyConnect, paginez 2-5 la section (ASDM) ou en activant des modules pour les caractéristiques supplémentaires d'AnyConnect, paginez 3-4 le pour en savoir plus (CLI).

Configuration de Start Before Logon avec le CLI

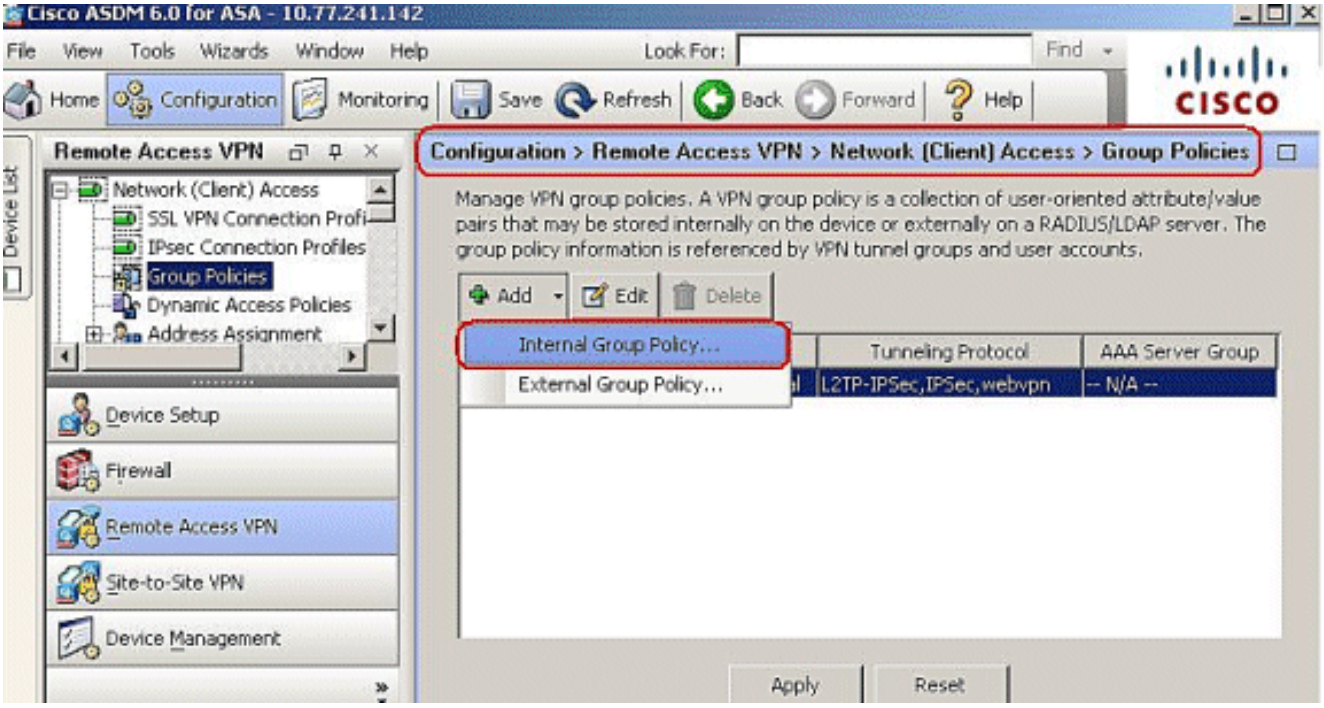
Ce scénario t'affiche comment installer le fichier XML avec le CLI :

1. Créez un profil pour être abaissé aux PC de client ces des sembler semblables 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 sur l'éclair sur les dispositifs de sécurité :
```
Copy tftp://x.x.x.x/AnyConnectProfile.xml AnyConnectProfile.xml
```
3. Sur les dispositifs de sécurité, ajoutez le profil comme profil disponible à la section globale de webvpn, tant que tout autrement est installé correctement pour des connexions d'AnyConnect :
```
hostname(config-group-policy)# webvpn hostame(config-group-webvpn)# svc
profiles ReallyNewProfile disk0:/AnyConnectProfile.xml
```
4. Éditez la stratégie de groupe que vous utilisation, et ajoutez les **modules de svc** et les commandes de **profil de 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
```

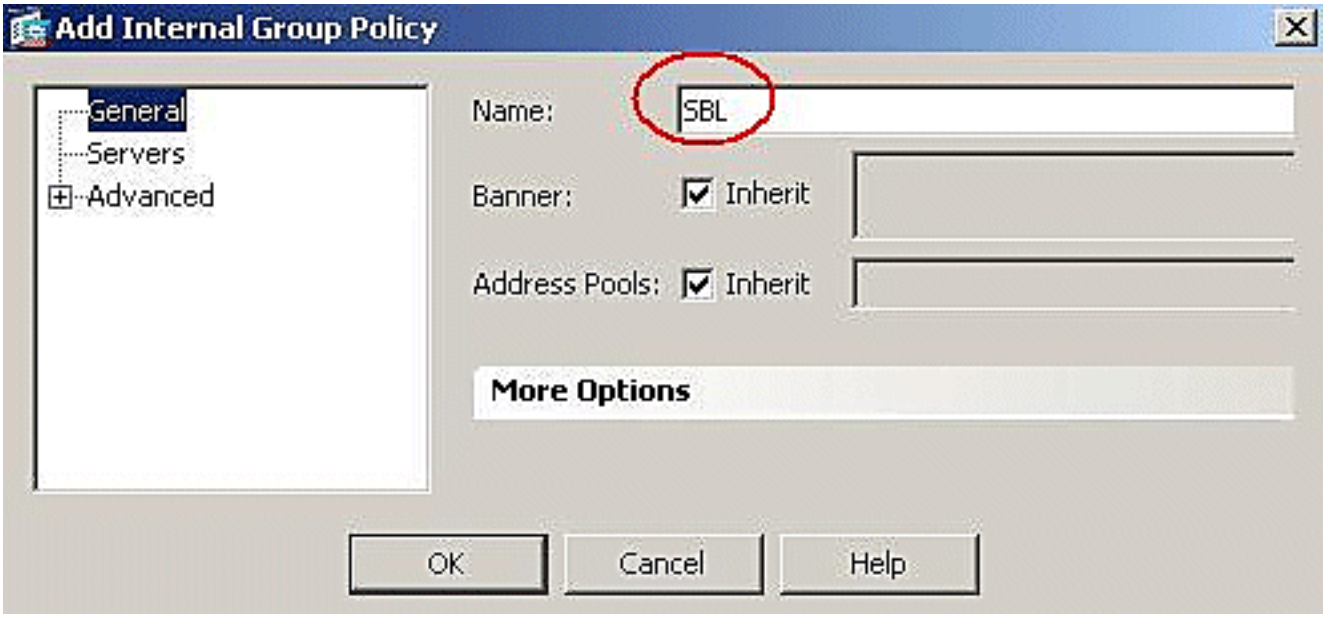
Configuration de Start Before Logon avec l'ASDM

Terminez-vous ces étapes pour configurer le SBL avec l'ASDM :

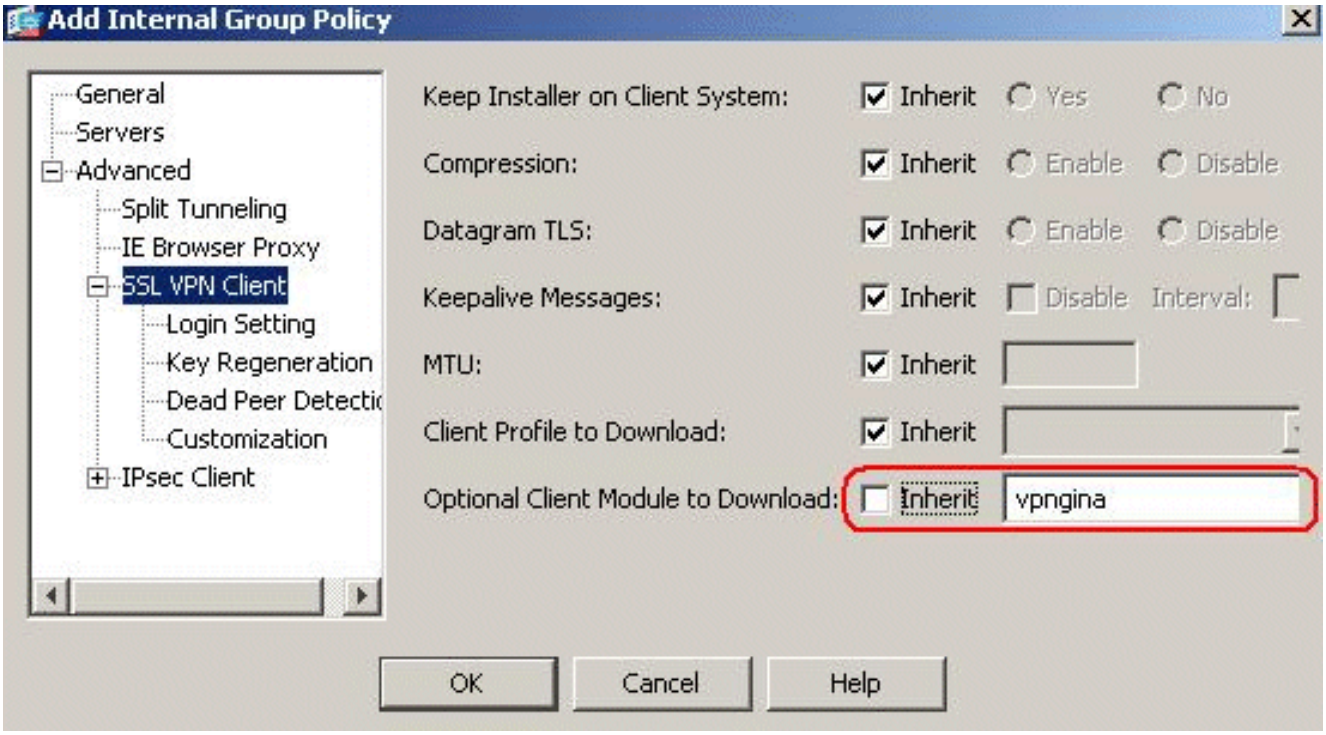
1. Créez un profil pour être abaissé aux PC de client ces des sembler semblables à ceci :
```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ 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. Sauvegardez le profil comme **AnyConnectProfile.xml dans l'**ordinateur local.
3. Lancez l'ASDM, et allez à la page d'accueil.
4. Allez au **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > ajoutent**, et cliquent sur la **stratégie de groupe interne**.



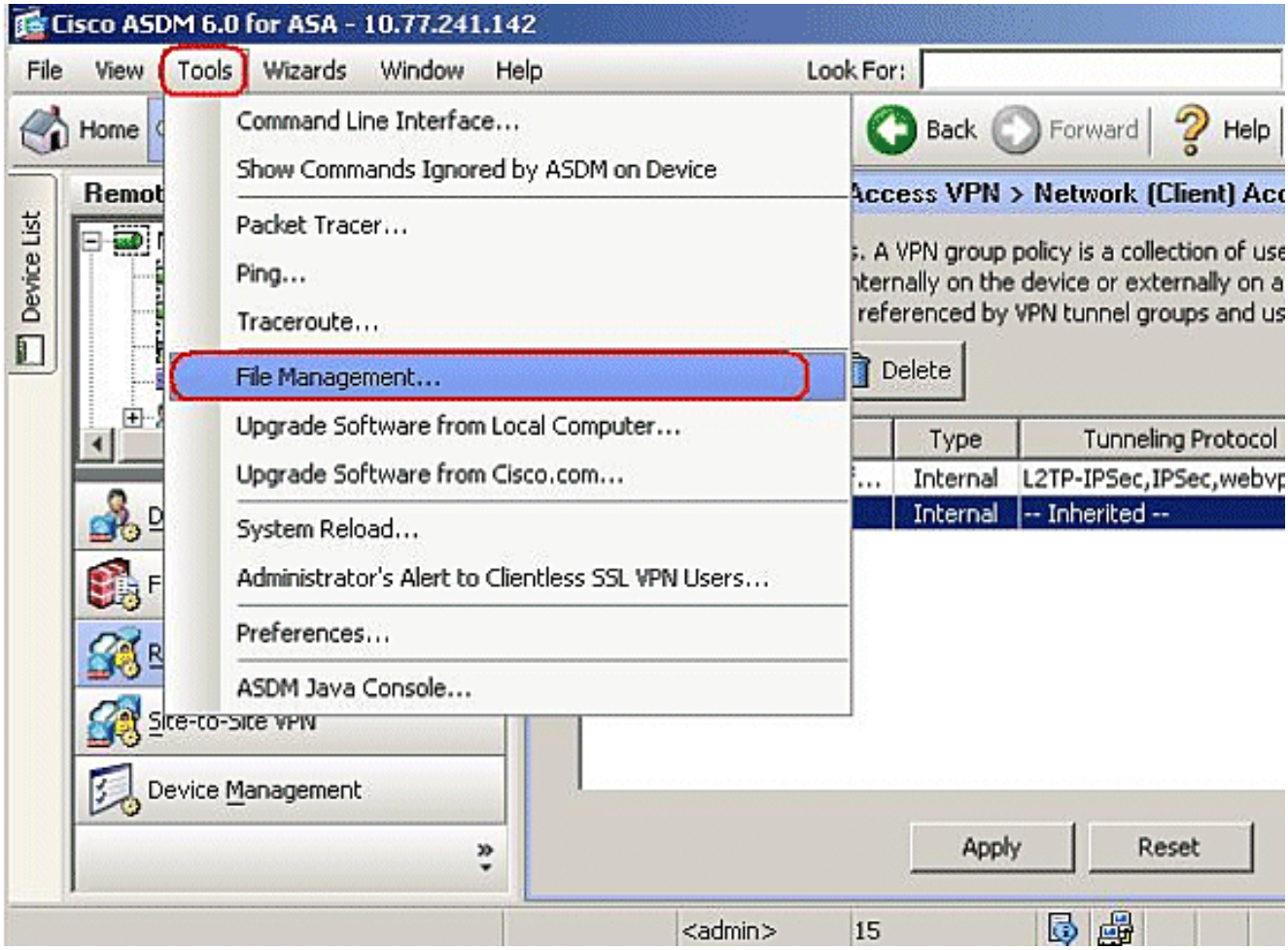
5. Écrivez le nom de la stratégie de groupe, par exemple, **SBL**.



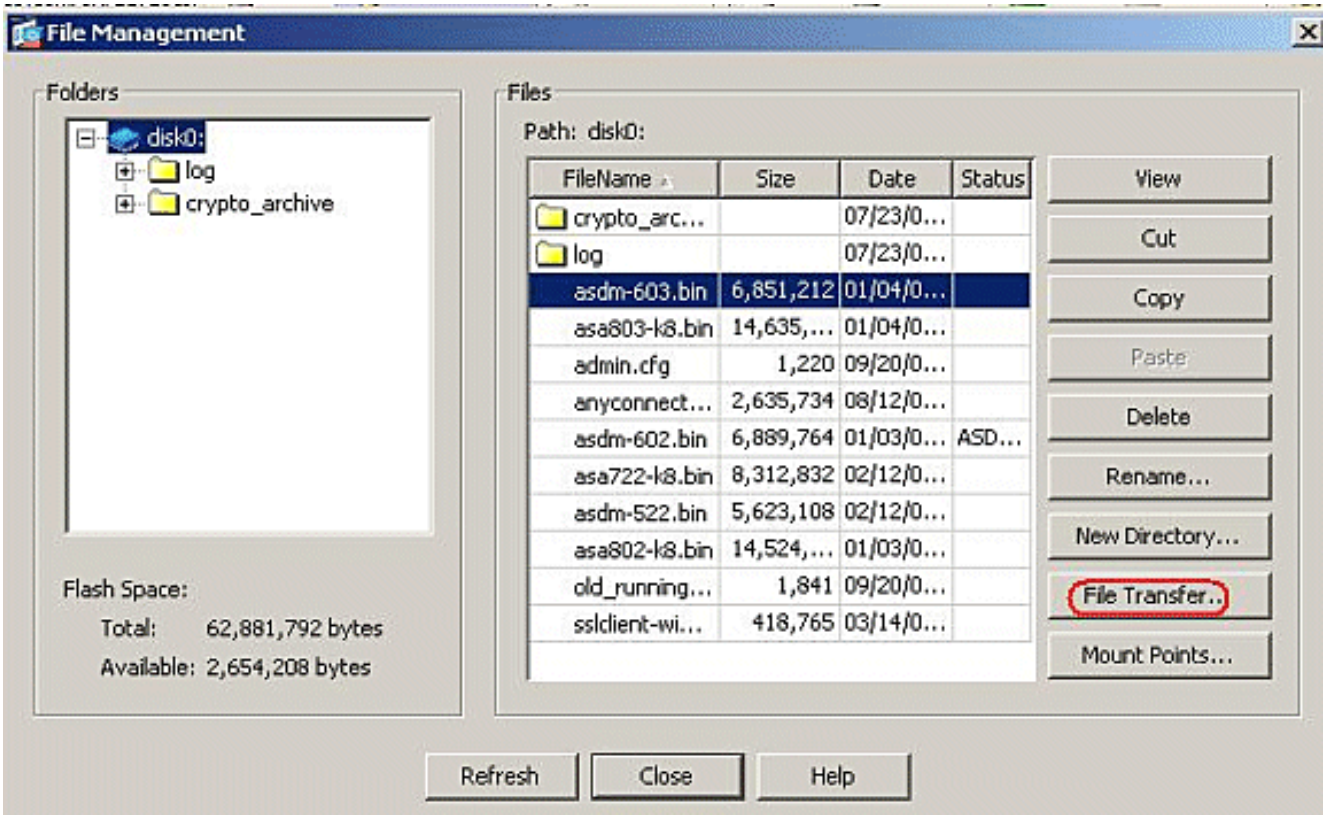
6. Allez à **avancé > client de VPN SSL**. Retirez le coche d'héritage dans le **module facultatif de client pour le télécharger**, et choisissez le **vpngina de la** liste déroulante.



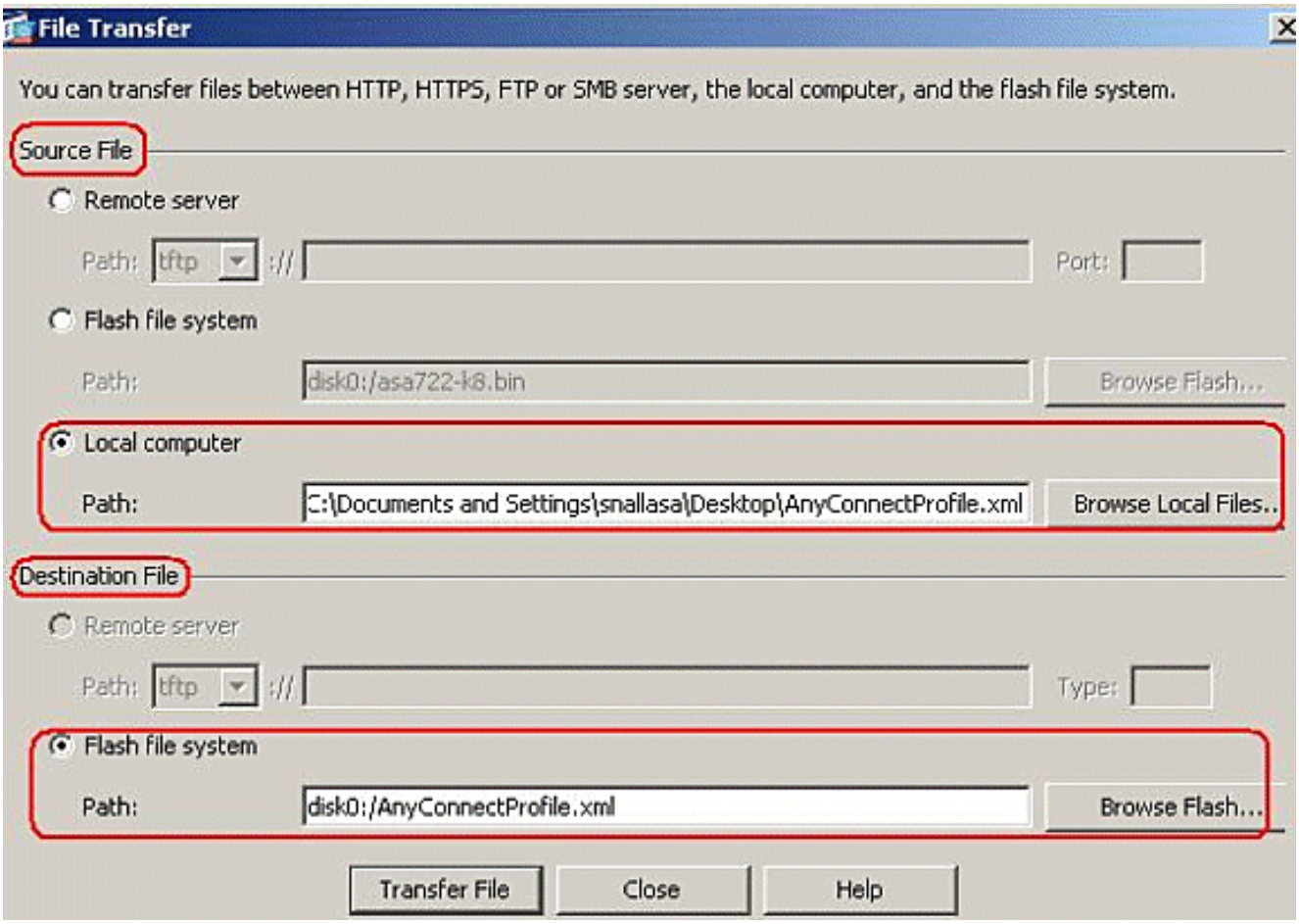
7. Afin de transférer le profil **AnyConnectProfile.xml à partir de l'**ordinateur local pour flasher, allez aux outils**, et** cliquez sur FileManagement**.**



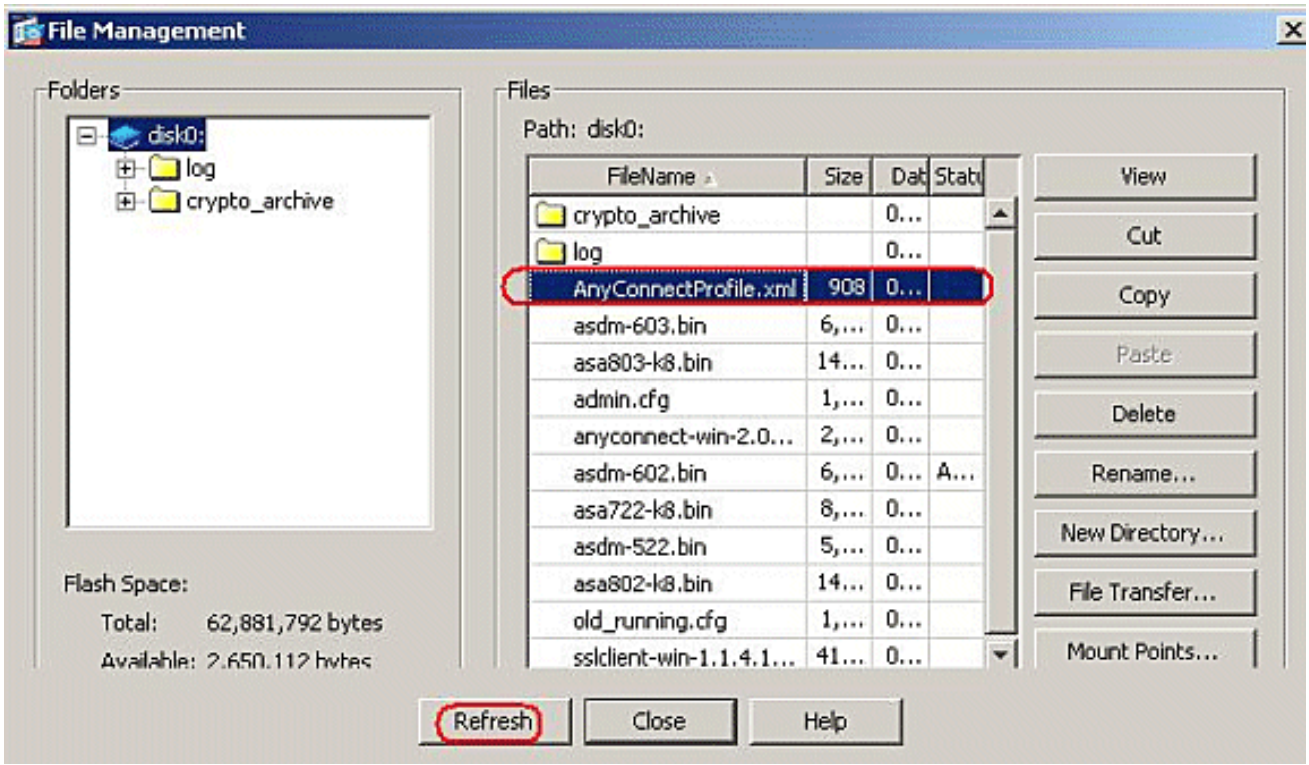
8. Cliquez sur le bouton de **transfert de fichiers**.



9. Afin de transférer le profil à partir de l'ordinateur local vers la mémoire flash ASA, choisissez le **fichier source**, le chemin du fichier XML (ordinateur local), et le **chemin de fichier de destination** selon votre condition
requise.

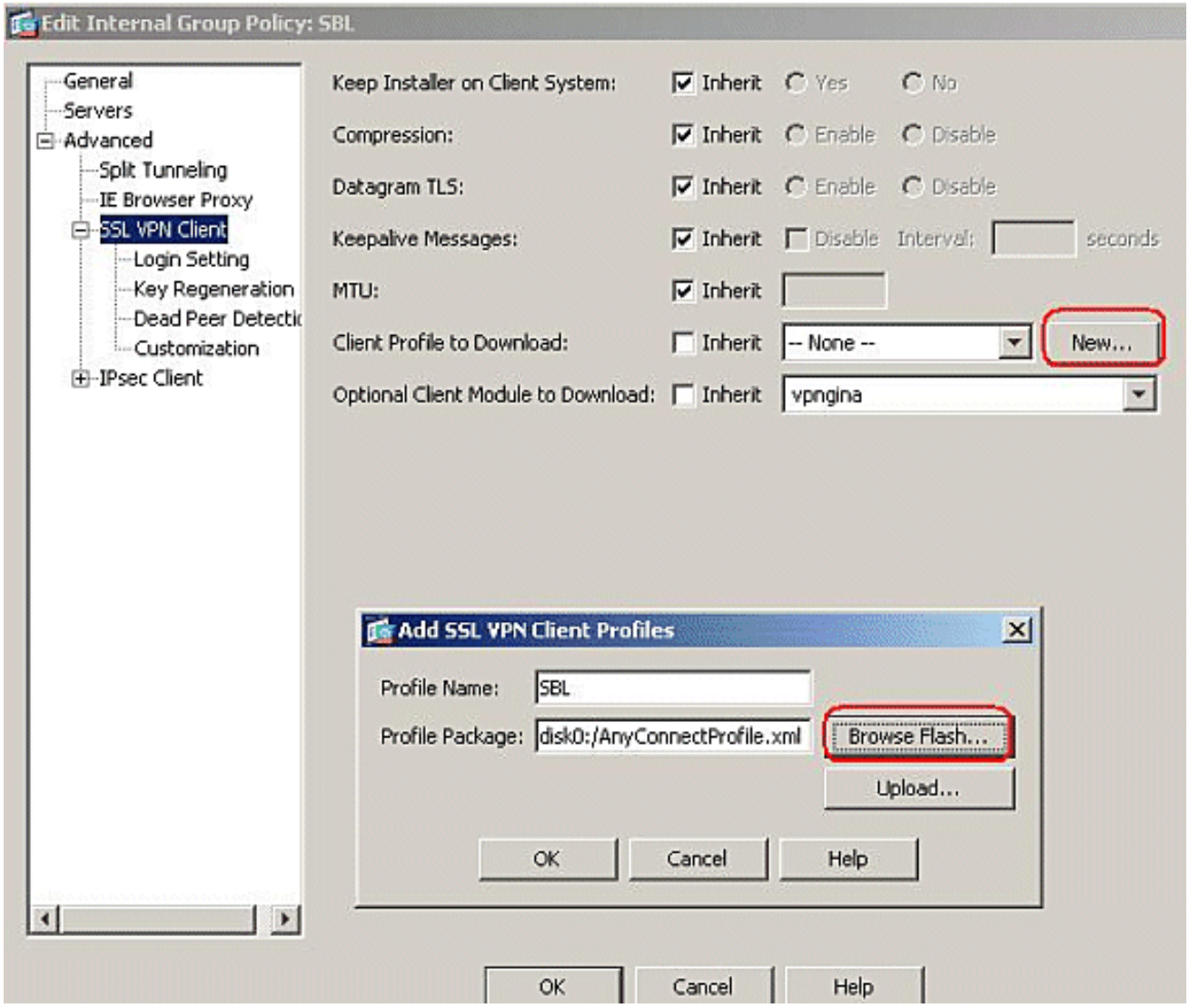


10. Après que le transfert, cliquent sur le bouton de **régénération** pour vérifier si le fichier des profils est dans la mémoire
flash.

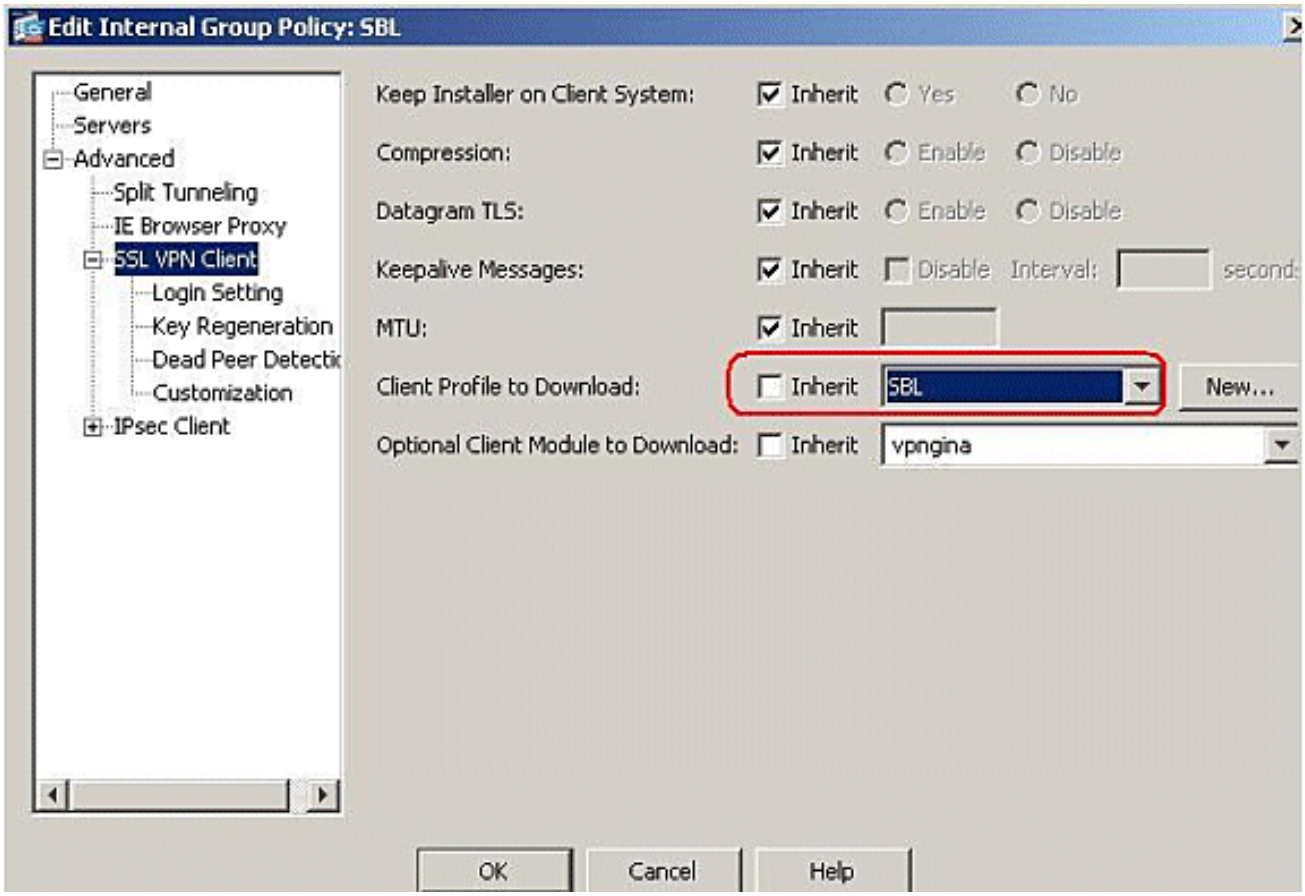


11. Assignez le profil à la stratégie de groupe interne (**SBL**).Suivez ce chemin, le **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > éditent SBL (stratégie de groupe interne) > a avancé > client de VPN SSL > profil de client au télécharger**, et clique sur le **bouton Nouveau**.Dans les **profils de client de VPN SSL d'ajouter**, cliquez sur le **bouton Parcourir** pour choisir l'emplacement du profile(AnyConnectProfile.xml) **enregistré**

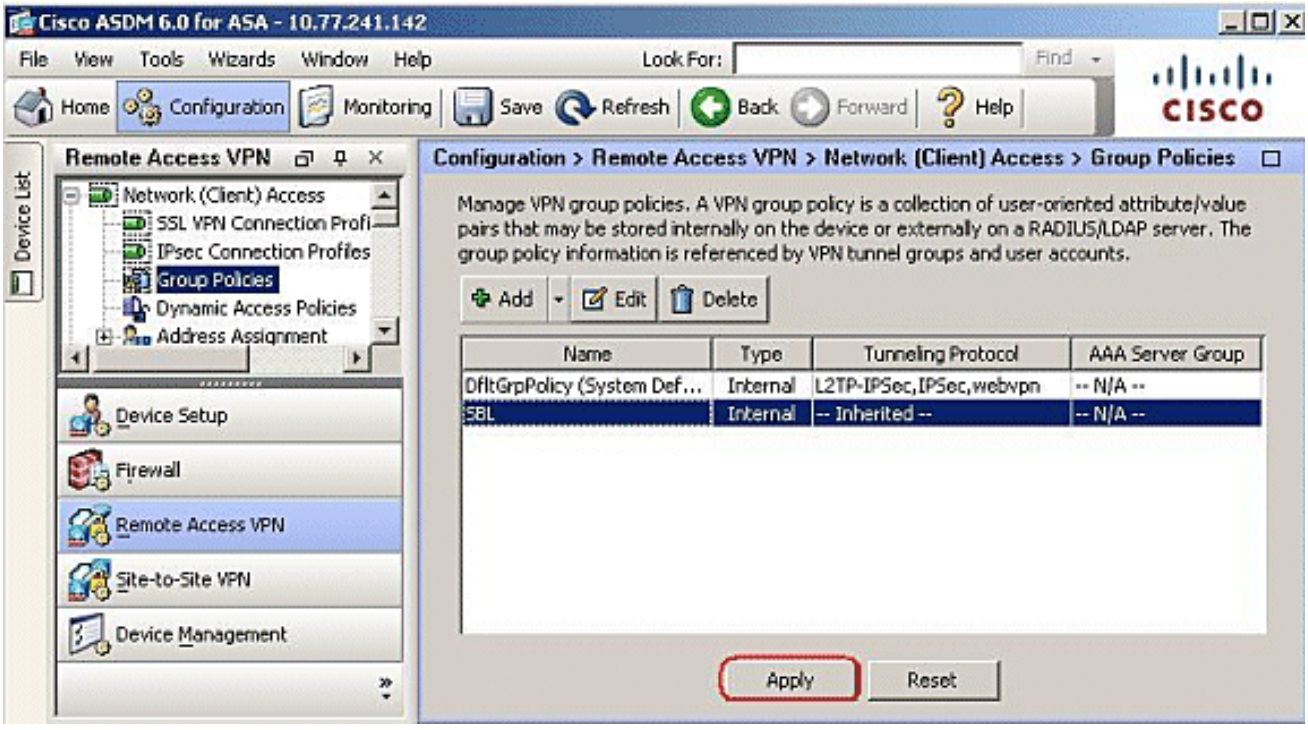
dans la mémoire flash ASA. Assignez au Namefor le profil, par exemple, SBL**. Le clic** OKTO se
terminent.



12. Retirez la case d'héritage et choisissez **SBL** dans le **profil de client pour télécharger le** champ. Cliquez sur
OK.



13. Cliquez sur Apply pour se terminer.



Utilisez le fichier manifeste

Le module d'AnyConnect qui est téléchargé sur les dispositifs de sécurité contient un fichier appelé le VPNManifest.xml. Cet exemple affiche une teneur témoin 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>
```

Les dispositifs de sécurité ont enregistré là-dessus ont configuré des profils, comme expliqué dans l'étape 1, et ils enregistrent également on ou les plusieurs modules d'AnyConnect qui contiennent le client d'AnyConnect lui-même, l'utilitaire de téléchargeur, le fichier manifeste, et tous les autres modules ou fichiers facultatifs de support.

Quand un utilisateur distant se connecte aux dispositifs de sécurité à WebLaunch ou à un client autonome en cours, le téléchargeur est téléchargé d'abord et passage. Il utilise le fichier manifeste pour s'assurer qu'il y a un client en cours sur le PC d'utilisateur distant qui doit être mis à jour, ou une installation fraîche est exigée. Le fichier manifeste contient également des informations sur s'il y a des modules facultatifs qui doivent être téléchargés et installés, dans ce cas, le VPNGINA. Le profil de client également est abaissé des dispositifs de sécurité. L'installation de VPNGINA est lancée par le **vpngina de valeur de modules de svc de** commande configuré sous le mode de commande de **stratégie de groupe (webvpn)** comme expliqué dans l'étape 4. Le client d'AnyConnect et les VPNGINA sont installés, et l'utilisateur voit le client d'AnyConnect à la prochaine réinitialisation, avant la connexion de domaine windows.

Quand l'utilisateur se connecte, le client et le profil sont passés vers le bas au PC utilisateur ; le client et les VPNGINA sont installés ; et l'utilisateur voit le client d'AnyConnect à la prochaine réinitialisation, avant la connexion.

Un exemple de profil est fourni sur le PC client quand AnyConnect est installé : **Utilisateurs \ données des applications \ Cisco de C:\Documents and Settings\All \ Cisco \ AnyConnect VPN Client \ profil \ AnyConnectProfile**.

Dépannez SBL

Utilisez cette procédure si vous rencontrez un problème avec SBL :

1. Assurez-vous que le profil est poussé.
2. Profils antérieurs d'effacement ; recherchez-les sur le disque dur pour trouver l'emplacement : *.xml.
3. Quand vous allez à l'ajout/suppression les programmes, avez-vous une installation d'AnyConnect et l'installation d'AnyConnect VPNGINA ?
4. Désinstallez le client d'AnyConnect.
5. Effacez le log d'AnyConnect du visualiseur et du contre-essai d'utilisateur en cas.
6. Le Web parcourent de nouveau aux dispositifs de sécurité pour réinstaller le client.
7. Assurez-vous que le profil apparaît également.
8. Réinitialisation une fois. Sur la prochaine réinitialisation, vous êtes incité avec la demande de Start Before Logon.
9. Envoyez le journal d'événements d'AnyConnect à Cisco dans le 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 est vu tout en essayant de télécharger le profil d'AnyConnect : `Erreur en validant le fichier XML contre le dernier schéma`. Comment cette erreur est-elle résolue ?

Solution 1

Ce message d'erreur se produit en grande partie en raison des questions de syntaxe ou de configuration dans le profil d'AnyConnect. Afin de résoudre ce problème, assurez-vous que le profil d'AnyConnect configuré est semblable au profil d'AnyConnect d'échantillon actuel dans la section de profil et de schéma XML d'AnyConnect d'échantillon du guide de l'administrateur de Cisco AnyConnect VPN Client.

Informations connexes

- Guide de l'administrateur Cisco AnyConnect VPN Client, Version 2.0
- Créant des scripts de connexion - TechNet de Windows
- Configurer le Start Before Logon (PLAP) sur des systèmes de Windows Vista
- Accès VPN ASA 8.x avec l'exemple de configuration de client de VPN SSL d'AnyConnect
- Cisco AnyConnect VPN Client
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Support et documentation techniques - Cisco Systems