ASA 8.X: AnyConnect starten voordat u de configuratie van de Aanbiedingsfuncties uitvoert

Inhoud

Inleiding

Met de optie *Start voordat* Logon (SBL) is ingeschakeld, ziet de gebruiker het dialoogvenster AnyConnect GUI-aanmelding voordat het aanmeldingsvenster van Windows® wordt weergegeven. Dit bevestigt eerst de VPN-verbinding. Alleen beschikbaar voor Windows-platforms, Start Vóór Logon, laat de beheerder het gebruik van inlogscripts, wachtwoorden caching, mapping Network Drive's naar lokale schijven controleren en meer. U kunt de SBL optie gebruiken om VPN te activeren als deel van de openingsvolgorde. SBL is standaard uitgeschakeld.

Raadpleeg voor meer informatie over het configureren van de functies van een AnyConnect VPN-client het gedeelte AnyConnect-clientfuncties configureren.

N.B.: Binnen de AnyConnect-client is de enige configuratie die u voor SBL doet, het inschakelen van deze functie. Netwerkbeheerders verwerken de verwerking die vóór aanmelding plaatsvindt op basis van de vereisten van hun situatie. Logon scripts kunnen worden toegewezen aan een domein of aan individuele gebruikers. Over het algemeen hebben de beheerders van het domein batchbestanden of de functies zoals gedefinieerd met gebruikers of groepen in Actieve Map. Zodra de gebruiker inlogt, wordt het inlogscript uitgevoerd.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ASA 5500 Series adaptieve security applicaties die softwareversie 8.x uitvoeren
- Cisco AnyConnect VPN versie 2.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Het punt van SBL is dat het een externe computer aan de infrastructuur van het bedrijf aansluit alvorens aan te melden aan de PC. Een gebruiker kan bijvoorbeeld buiten het fysieke bedrijfsnetwerk zijn en geen toegang hebben tot bedrijfsbronnen totdat zijn of haar pc zich bij het bedrijfsnetwerk heeft aangesloten. Als de SBL-functie is ingeschakeld, sluit de AnyConnect-client aan voordat de gebruiker het Microsoft inlogvenster ziet. De gebruiker moet ook zoals gebruikelijk aan Windows inloggen wanneer het Microsoft inlogvenster verschijnt.

Dit zijn verschillende redenen om SBL te gebruiken:

- De PC van de gebruiker wordt aangesloten bij een Actieve infrastructuur van de Map.
- De gebruiker kan geen inkervingen op de PC hebben gecached, dat wil zeggen, als het groepsbeleid inkervingen afbreekt.
- De gebruiker moet inlogscripts uitvoeren die vanuit een netwerkresource worden uitgevoerd of die toegang tot een netwerkresource vereisen.
- Een gebruiker heeft netwerk-in kaart gebrachte aandrijfsystemen die authenticatie met de Active Directory infrastructuur nodig hebben.
- Netwerkcomponenten, zoals MS NAP/CS NAC, kunnen verbinding met de infrastructuur vereisen.

SBL maakt een netwerk dat gelijk is aan inclusie in het lokale LAN. Met SBL geactiveerd, omdat de gebruiker toegang heeft tot de lokale infrastructuur, zijn de openings van een aanmelding scripts die normaal voor een gebruiker in het kantoor uitgevoerd worden ook beschikbaar voor de externe gebruiker.

Voor informatie over hoe om openings van een aanmelding scripts te maken, zie dit artikel van Microsoft TechNet.

Raadpleeg dit Microsoft-artikel voor informatie over het gebruik van locale aanmeldingsscripts in Windows XP.

In een ander voorbeeld, kan een systeem worden gevormd om gecached geloofsbrieven voor opening van een aanmelding bij de PC tegen te houden. In dit scenario moeten gebruikers kunnen communiceren met een domeincontroller op het bedrijfsnetwerk zodat hun geloofsbrieven worden gevalideerd voordat ze toegang hebben tot de pc. SBL vereist dat een netwerkverbinding aanwezig is op het moment dat het wordt opgeroepen. In sommige gevallen is dit niet mogelijk omdat een draadloze verbinding kan afhangen van gebruikersreferenties om verbinding te maken met de draadloze infrastructuur. Aangezien de SBL-modus voorafgaat aan de aanmeldingsfase van een aanmelding, is er geen verbinding beschikbaar in dit scenario. In dit geval moet de draadloze verbinding worden geconfigureerd om de aanmeldingsgegevens in de aanmelding te bewaren, of moet een andere draadloze verificatie worden geconfigureerd zodat SBL kan werken.

Installeer de start voor de inlogonderdelen (alleen Windows)

De optie Start voordat de aanmelding wordt gestart, moet worden geïnstalleerd nadat de kernclient is geïnstalleerd. Bovendien moet voor de begin-periode van AnyConnect 2.2 voor de aanmelding of de onderdelen versie 2.2 of later van de kernsoftware van AnyConnect worden geïnstalleerd. Als u de AnyConnect-client en de Start Vóór aanmelding componenten met de MSI-bestanden hebt geimplementeerd (bijvoorbeeld bij een groot bedrijf met een eigen softwareimplementatie (Altiris, Active Directory of SMS), moet u de opdracht goed krijgen. De volgorde van de installatie wordt automatisch verwerkt wanneer de beheerder AnyConnect laadt als het web wordt geïmplementeerd en/of bijgewerkt. Raadpleeg voor volledige installatie-informatie Releaseopmerkingen voor Cisco AnyConnect VPN-client, release 2.2.

Verschillen tussen Windows-Vista\Windows 7 en Pre-Vista start vóór de aanmelding

De procedures om SBL in te schakelen verschillen lichtjes van Windows Vista- en Windows 7-systemen. Pre-Vista-systemen gebruiken een component die "Virtual Private Network Identification and Verification" (VPNGINA) wordt genoemd om SBL te implementeren. Vista en Windows 7 systemen gebruiken een component genaamd PLAP om SBL te implementeren.

In de AnyConnect-client is de optie Windows Vista Start Voordat u de aanmelding start bekend als de PLAP (Pre-Login Access Provider), die een verbonden crediteur is. Hiermee kunnen netwerkbeheerders specifieke taken uitvoeren, zoals het verzamelen van aanmeldingsgegevens of het aansluiten op netwerkbronnen, voordat u inlogt. PLAP biedt Start voordat de inlogfunctie actief is in Windows Vista, Windows 7 en de Windows 2008-server. PLAP ondersteunt 32-bits en 64-bits versies van het besturingssysteem met respectievelijk vpnplap.dll en vpnplap64.dll. De PLAP-functie ondersteunt Windows Vista x86- en x64-versies.

Opmerking: In dit gedeelte verwijst VPNGINA naar de optie Start Vóór aanmelding voor pre-Vista-platforms en PLAP naar de functie Start Vóór aanmelding voor Windows Vista en Windows 7-systemen.

In pre-Vista systemen, start voordat Logon een component gebruikt die bekend staat als de VPN Graphical Identification and Authentication Dynamic Link Library (vpina.dll) om Start voor Logon-functies te leveren. De component Windows PLAP, die deel uitmaakt van Windows Vista, vervangt de component Windows GINA.

Een GINA wordt geactiveerd wanneer een gebruiker op de toetsencombinatie Ctrl+Alt+Del drukt.

Met PLAP opent de combinatie van Ctrl+Alt+Del een venster waarin de gebruiker kan kiezen om in te loggen op het systeem of om netwerkverbindingen (PLAP-onderdelen) te activeren met de knop Network Connect in de rechterbenedenhoek van het venster.

De secties die direct volgen beschrijven de instellingen en procedures voor zowel VPNGINA als PLAP SBL. Voor een volledige beschrijving van de mogelijkheden en het gebruik van de SBL-functie (PLAP) op een Windows Vista-platform raadpleegt u Start Before Logon (PLAP) configureren op Windows Vista Systems.

XML-instellingen om SBL in te schakelen

De waarde van het element voor UseStartVoorLogon kan deze functie worden ingeschakeld (waar) of uit (onjuist). Als u deze waarde op **waar** in het profiel instelt, wordt extra verwerking uitgevoerd als deel van de openings- reeks. Zie voor meer informatie het gedeelte Start Vóór aanmelding. Stel de waarde van **<**USEStartBefore Logon**>** in het bestand CiscoAnyConnect.xml in op **waarheid** om SBL in te schakelen:

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

Om SBL uit te schakelen, stelt u dezelfde waarde in op **vals**.

Gebruik deze verklaring om de functie User Controllable te activeren wanneer u SBL activeert:

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

Elke gebruikersinstelling die bij deze eigenschap is gekoppeld, wordt elders opgeslagen.

SBL inschakelen

Om de downloadtijd te minimaliseren, vraagt de AnyConnect-client alleen downloads (van het security apparaat) van kernmodules die deze nodig heeft voor elke functie die deze ondersteunt. Om nieuwe functies in te schakelen, zoals SBL, moet u de modemnaam met de opdracht **svc modules** specificeren van groepsbeleid WebVPN of de configuratiemodus van gebruikersnaam WebVPN:

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

De string waarde voor SBL is **vpngina**.

In dit voorbeeld voert de netwerkbeheerder de groeidekenmodus in voor de telecommunicatie van het groepsbeleid; gaat de configuratie van WebVPN in voor het groepsbeleid; en specificeert de string VPNGINA om SBL in te schakelen:

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

Daarnaast moet de beheerder ervoor zorgen dat het bestand AnyConnect <profile.xml>, waarin <profile.xml> de naam is die de netwerkbeheerder aan het XML-bestand heeft toegewezen, de verklaring <USEStartBeforeLogon> op **waarheid** heeft ingesteld, bijvoorbeeld:

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

Het systeem moet opnieuw worden opgestart voordat de aanmelding start. U moet ook specificeren op het security apparaat dat u SBL wilt toestaan, of op enige andere modules voor extra functies. Raadpleeg de beschrijving in de Invoeringsmodules voor extra AnyConnect-functies, pagina 2-5 (ASDM) of de instelmodules voor extra AnyConnect-functies, pagina 3-4 (CLI) voor meer informatie.

Begin vóór Logon Configuration met CLI

Dit scenario laat je zien hoe je het XML bestand met CLI instelt:

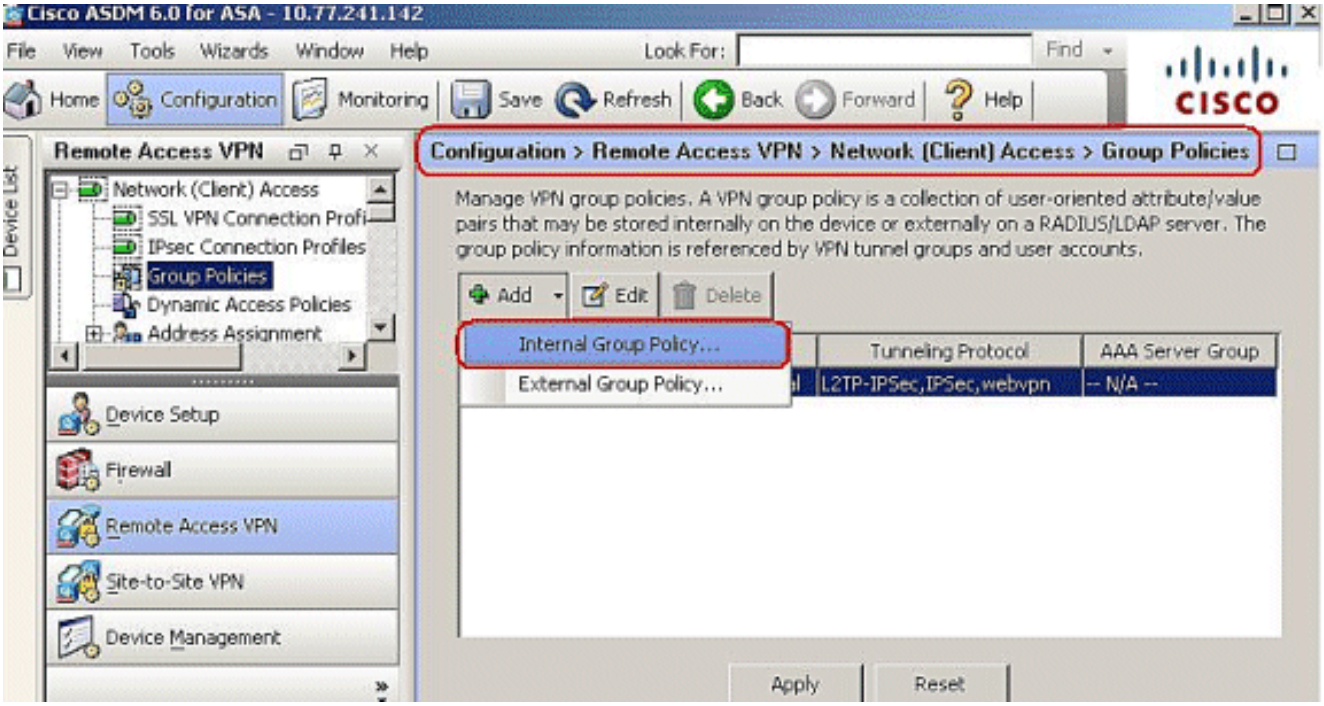
1. Maak een profiel dat naar beneden wordt geduwd naar de client-PC's die er op lijken:
```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ 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. Kopieert het bestand naar de Flash op het beveiligingsapparaat:
```
Copy tftp://x.x.x.x/AnyConnectProfile.xml AnyConnectProfile.xml
```
3. Voeg op het security apparaat het profiel als een beschikbaar profiel toe aan het wereldwijde gedeelte van WebVPN, zolang alle andere opties correct zijn ingesteld voor AnyConnect-verbindingen:
```
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)#
   svc profiles ReallyNewProfile disk0:/AnyConnectProfile.xml
```
4. Bewerk het groepsbeleid dat u gebruikt en voeg de opdrachten **svc-modules** en **svc-profiel** toe:

```
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
```

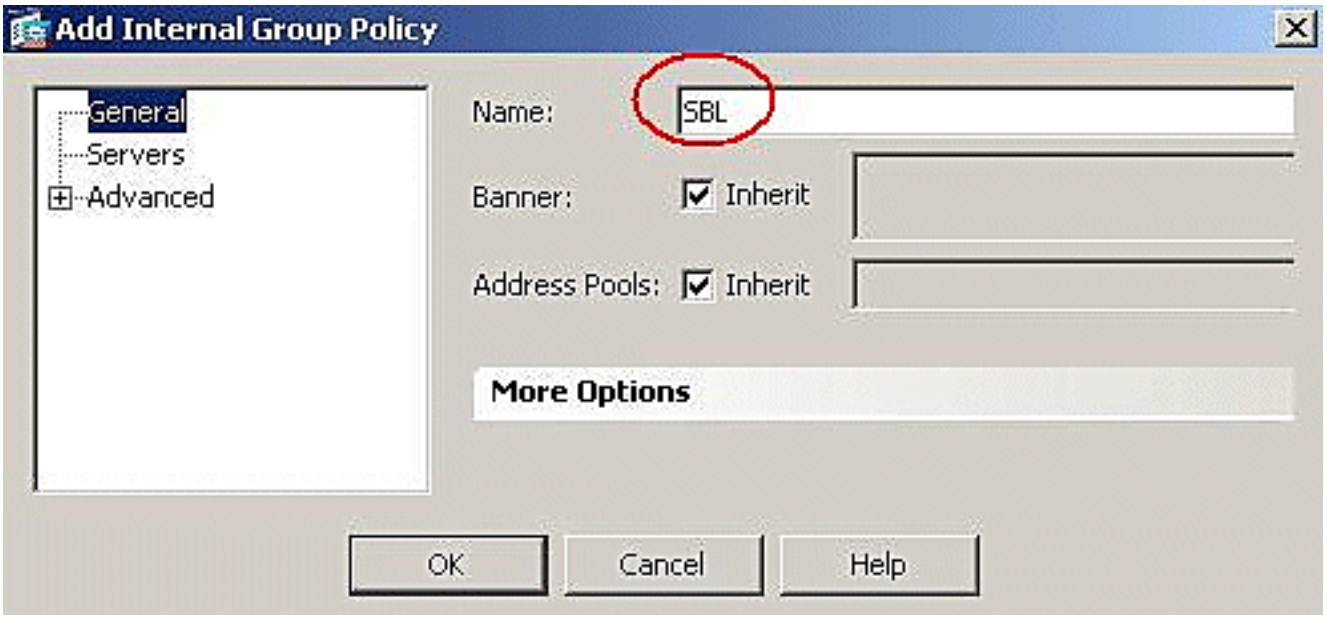
Begin voor loginconfiguratie met ASDM

Volg deze stappen om de SBL met ASDM te configureren:

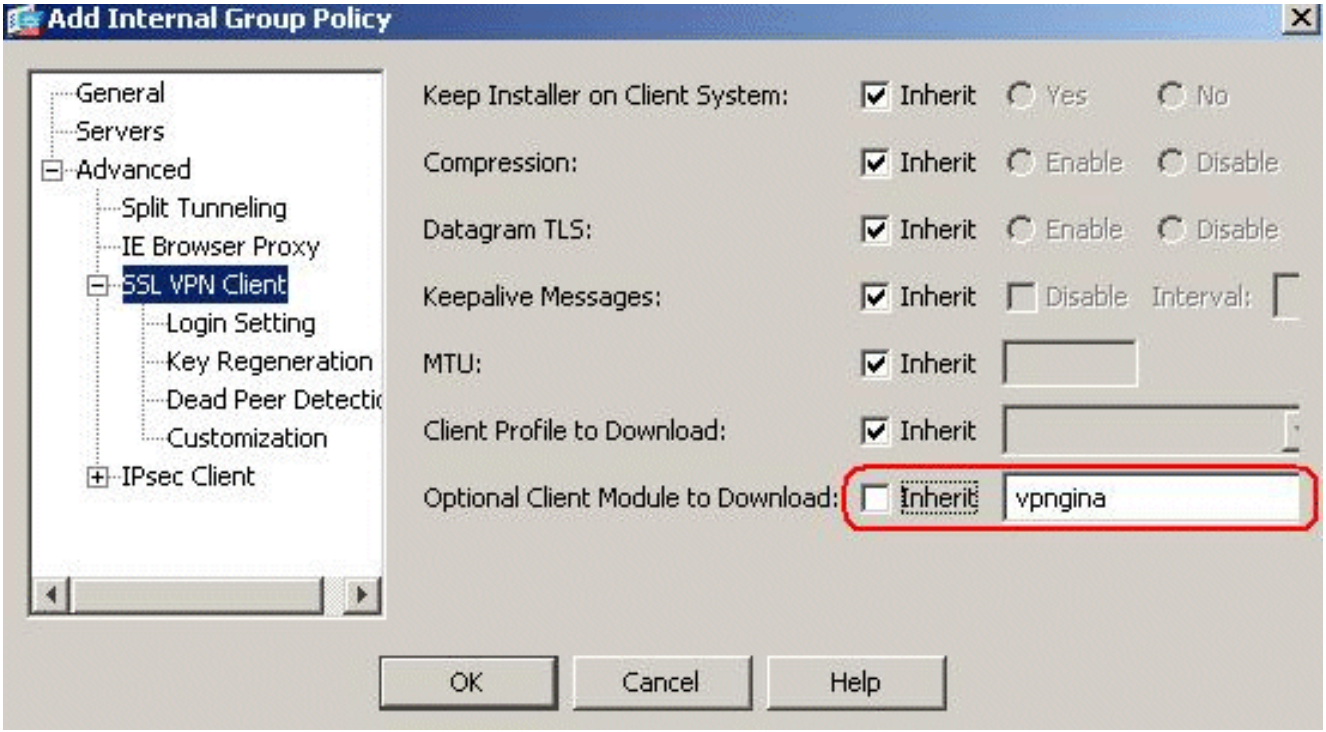
1. Maak een profiel dat naar beneden wordt geduwd naar de client-PC's die er op lijken:
```
<?xml version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ 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. Sla het profiel op als **AnyConnectProfile.xml** in de lokale computer.
3. Start ASDM en ga naar de startpagina.
4. Ga naar **Configuration > Remote Access VPN > Network (Client) Access > Group Policy > Add** en klik op het **Interne groepsbeleid**.



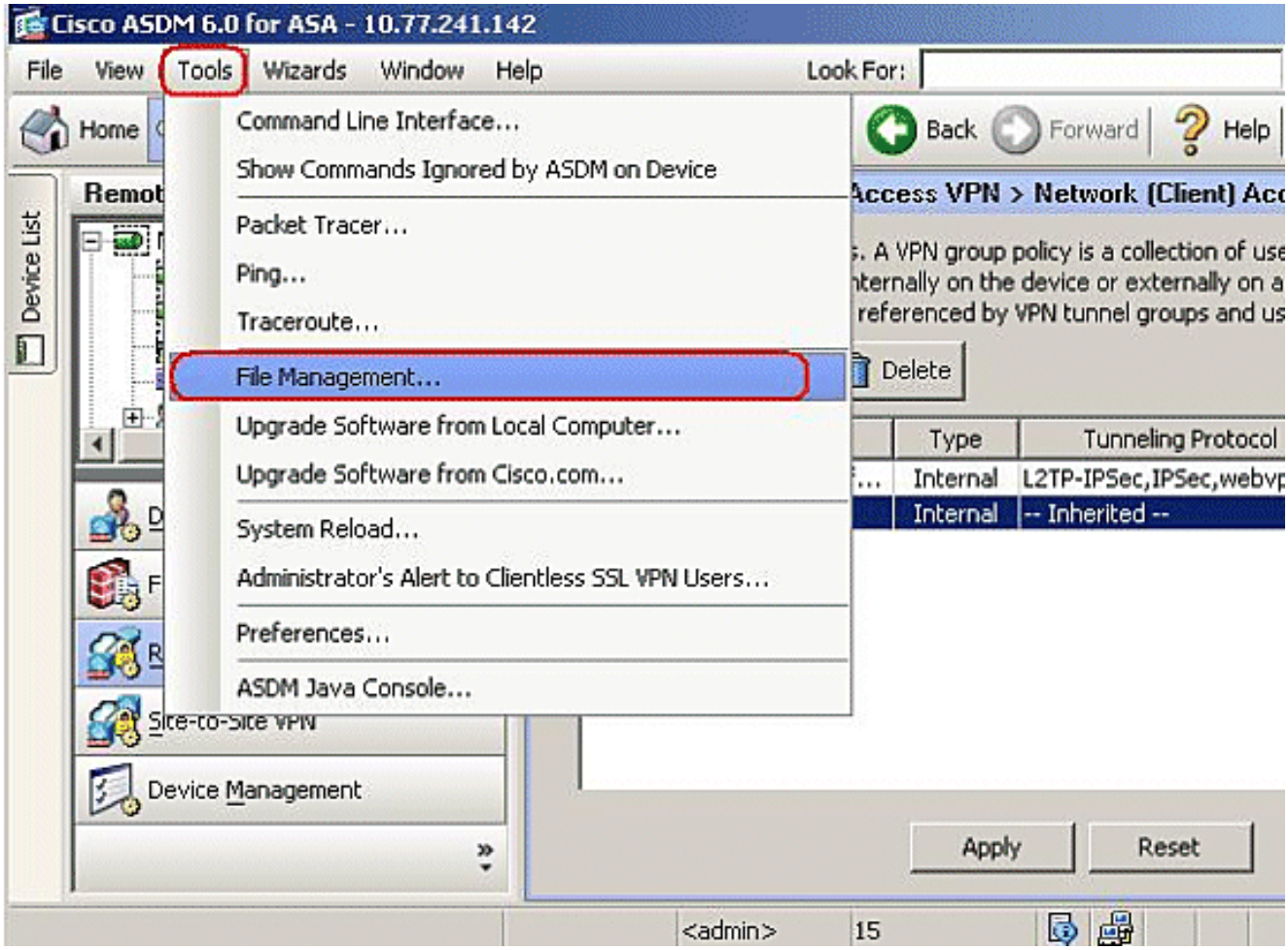
5. Voer de naam van het groepsbeleid in, bijvoorbeeld **SBL**.



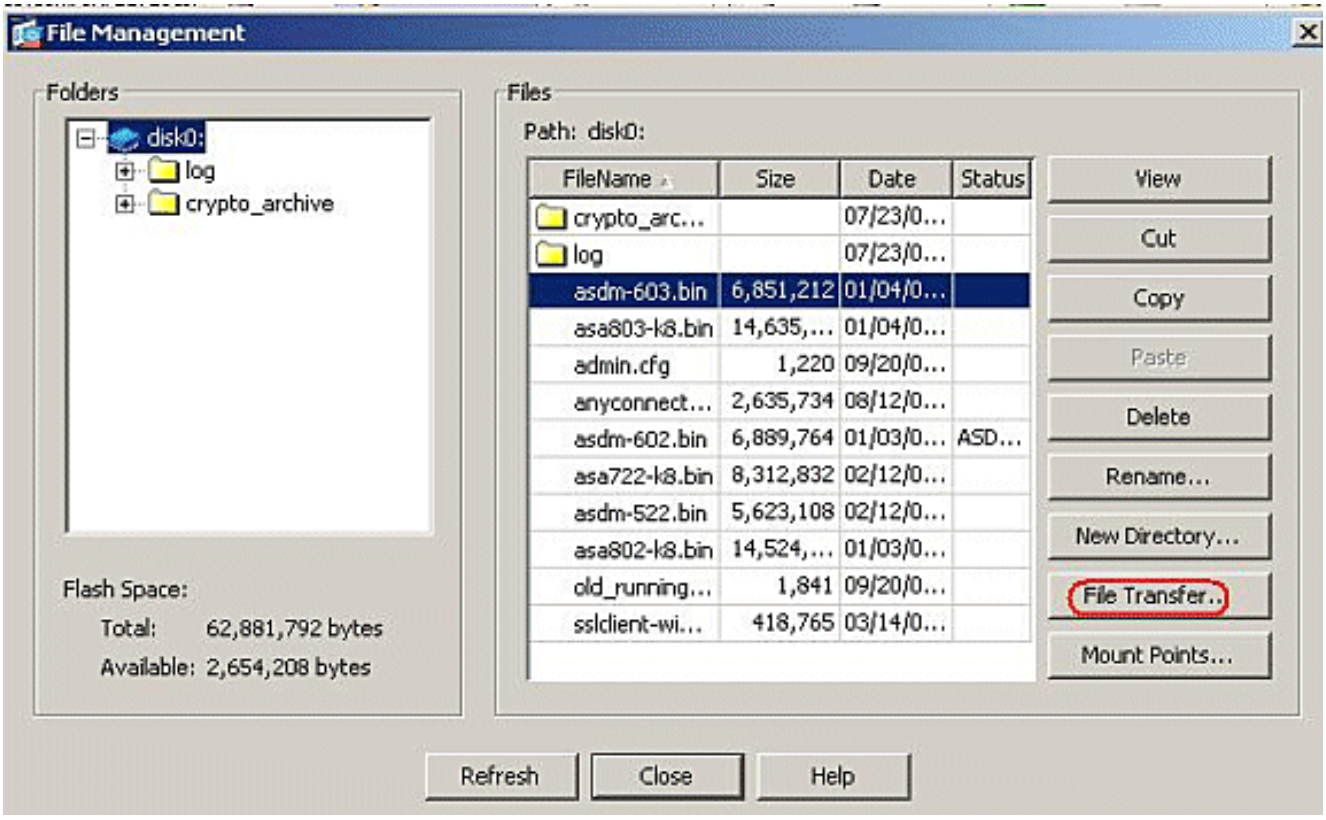
6. Ga naar **geavanceerde > SSL VPN-client**. Verwijder het aanvinkvakje Inherit in het **optionele clientmodule om te downloaden** en kies **VPN** in het uitrolvak.



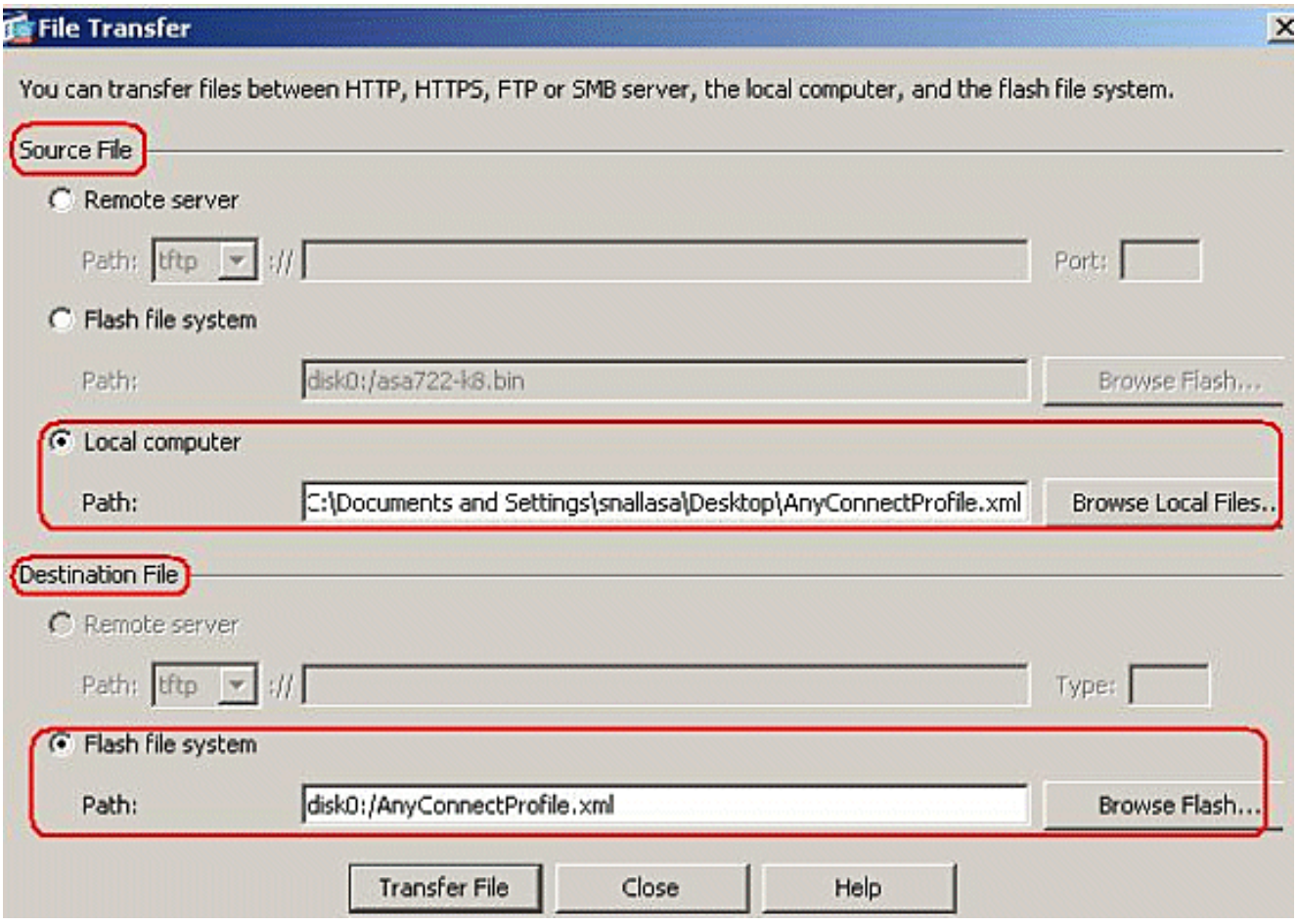
7. U kunt het profiel **AnyConnectProfile.xml** van de lokale computer naar Flash overdragen, naar **Gereedschappen** gaan en op **File Management** klikken.



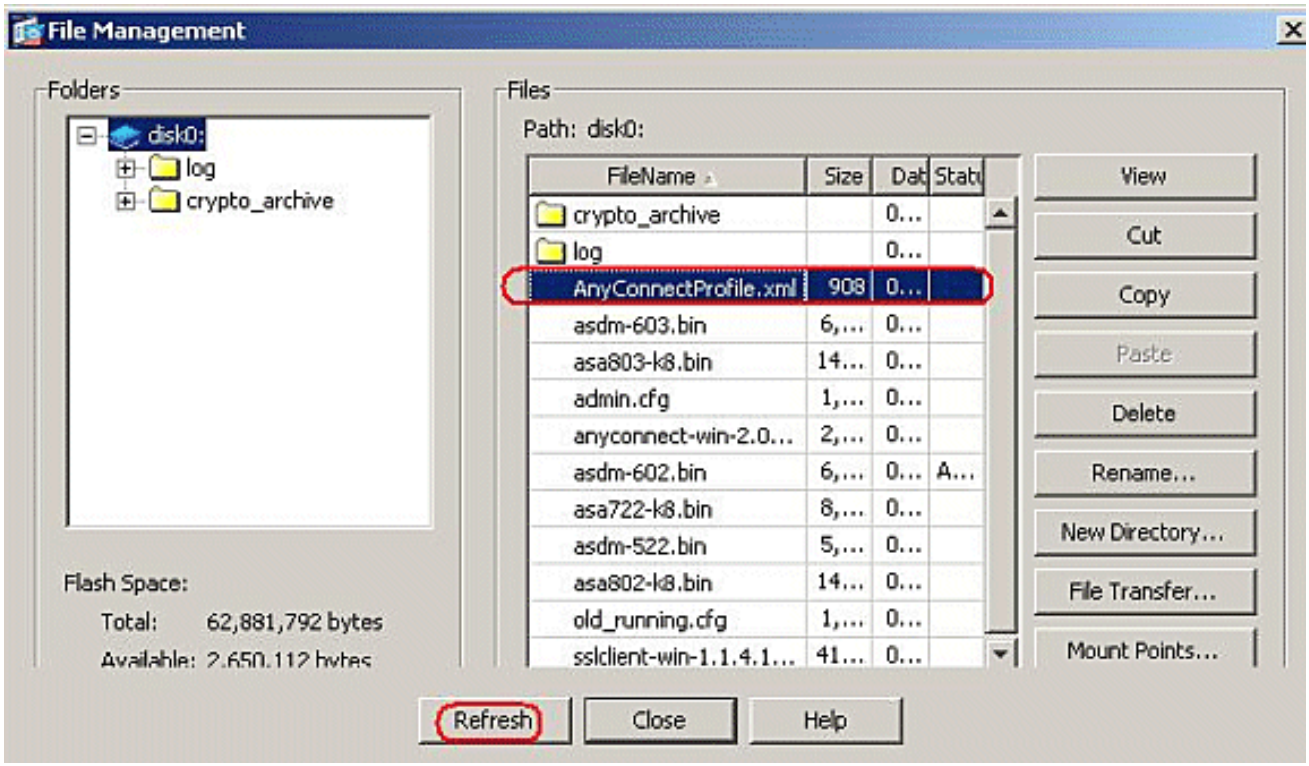
8. Klik op de knop **Bestandsoverdracht**.



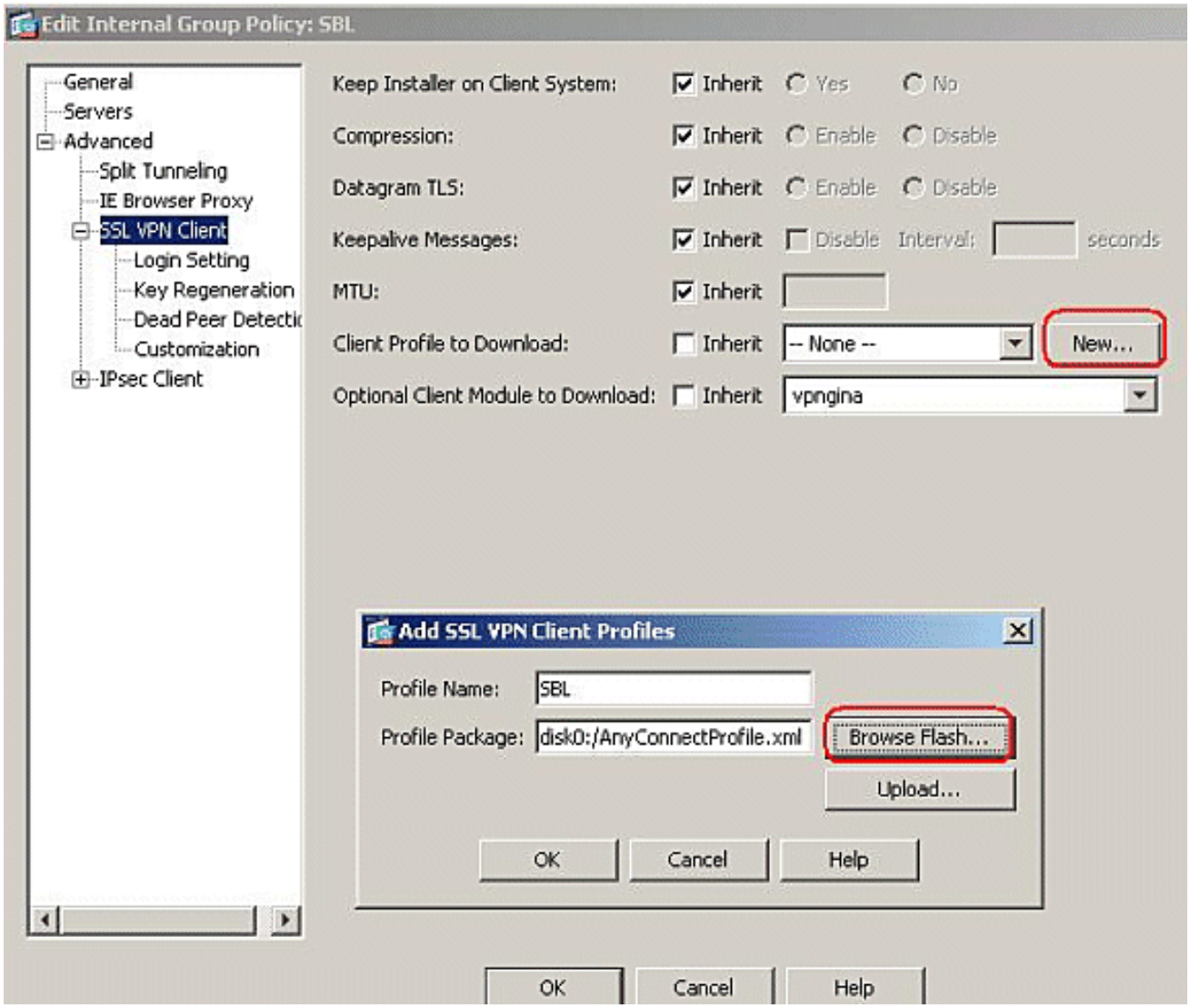
9. Om het profiel van de lokale computer naar het ASA Flash geheugen over te brengen, kies het **bronbestand**, het pad van het XML-bestand (lokale computer) en het pad naar **doelbestand** volgens uw vereiste.



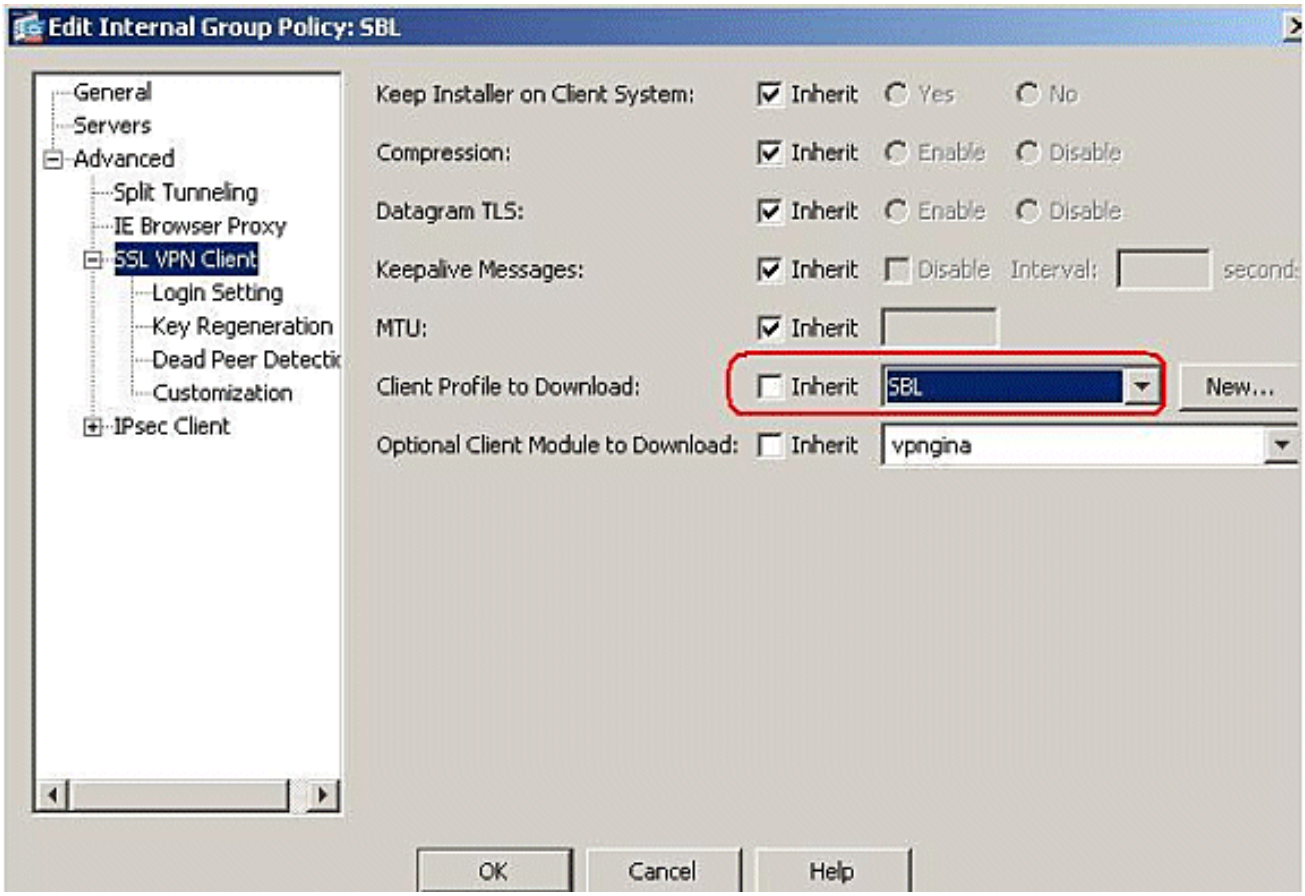
10. Klik na de overdracht op de **knop Vernieuwen** om te controleren of het profielbestand in het Flash-geheugen is.



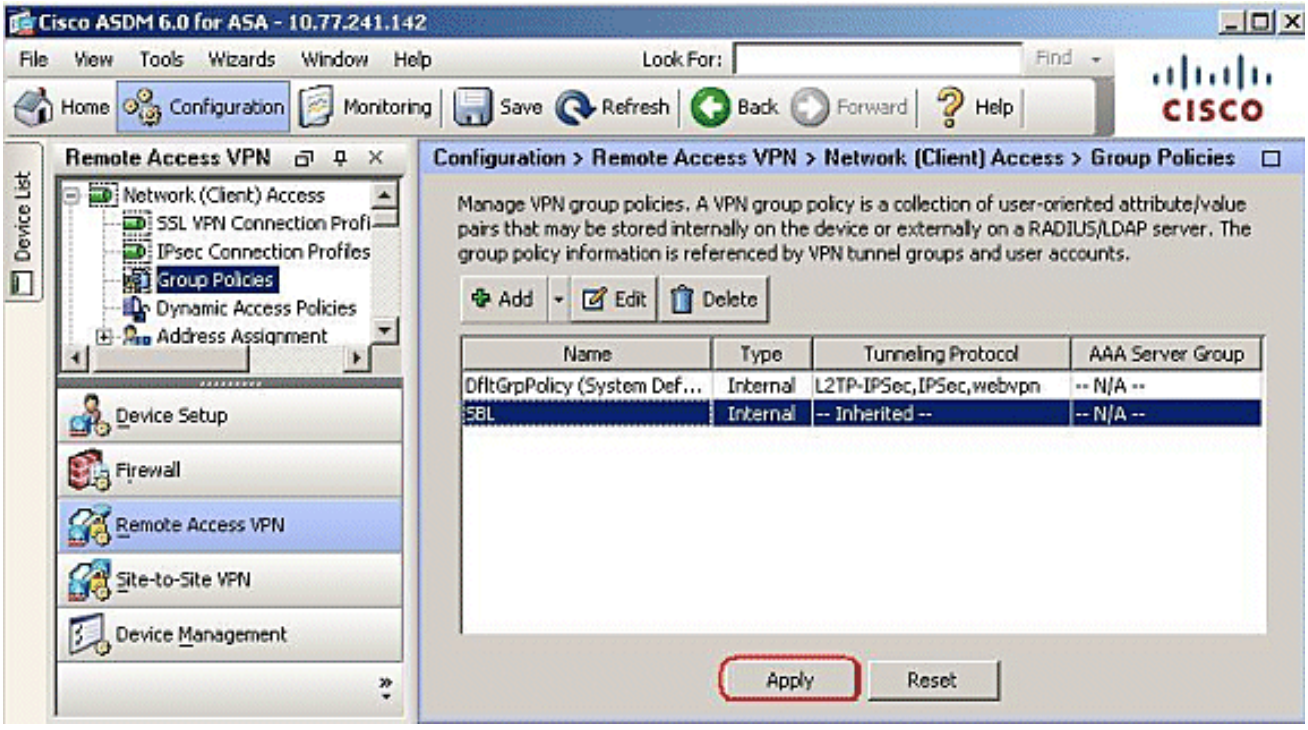
11. Het profiel toewijzen aan het interne groepsbeleid (**SBL**).Volg dit pad, **Configuration > Remote Access VPN > Network (Client) Access > Group Policy > Save SBL (Intern Groepsbeleid) > Advanced > SSL VPN-client > Client Profile to Download**, en klik op de **New**-knop.In de **Add SSL VPN Client Profiles**, klik op de knop **Bladeren** om de locatie van het profiel (**AnyConnectProfile.xml**) te kiezen dat in het ASA Flash-geheugen is opgeslagen. Pas de **naam** aan voor het profiel, bijvoorbeeld, **SBL**. Klik op **OK** om dit te voltooien.



12. Verwijder het aankruisvakje en kies **SBL** in het veld **Clientprofiel om te downloaden**. Klik op **OK**.



13. Klik op **Toepassen** om te voltooien.



Gebruik het uitvoerbestand

Het AnyConnect-pakket dat op het beveiligingsapparaat wordt geüpload, bevat een bestand dat VPNManifest.xml heet. Dit voorbeeld toont een voorbeeldinhoud van dit bestand:

```
<?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>
```

Het security apparaat heeft op de geconfigureerde profielen opgeslagen, zoals uitgelegd in Stap 1, en het slaat ook een of meerdere AnyConnect-pakketten op die de AnyConnect-client zelf, de downloader-hulpprogramma, het manifest-bestand en andere optionele modules of ondersteuningsbestanden bevatten.

Wanneer een externe gebruiker zich met Webex of een huidige standalone client op het beveiligingsapparaat aansluit, wordt eerst de downloader gedownload en uitgevoerd. Het gebruikt het manifest bestand om na te gaan of er een huidige client op de PC van de afstandsgebruiker is die moet worden bijgewerkt, of dat een nieuwe installatie vereist is. Het manifest bestand bevat ook informatie over de vraag of er optionele modules zijn die gedownload en geïnstalleerd moeten worden, in dit geval de VPNGINA. Het clientprofiel wordt ook uit het security apparaat verwijderd. De installatie van VPNGINA wordt geactiveerd door de opdracht **svc modules waarde vpngina** die is geconfigureerd onder de opdrachtmodus **groepsbeleid (webvVPN)** zoals uitgelegd in Stap 4. De AnyConnect-client en VPNGINA zijn geïnstalleerd en de gebruiker ziet de AnyConnect-client bij de volgende herstart, voordat u Windows-domeinaanmelding opent.

Wanneer de gebruiker verbinding maakt, worden de client en het profiel doorgegeven naar de PC van de gebruiker. de cliënt en de VPNGINA zijn geïnstalleerd; en de gebruiker ziet de AnyConnect-client bij de volgende herstart, voordat u zich aanmeldt.

Er wordt een voorbeeldprofiel op de client-pc geleverd wanneer AnyConnect is geïnstalleerd: **C:\Documents and Settings\All Users\Application Data\Cisco\Cisco\AnyConnect VPN Client\Profile\AnyConnectProfile**.

Probleemoplossing SBL

Gebruik deze procedure als u een probleem met SBL hebt:

1. Zorg ervoor dat het profiel is ingedrukt.
2. Verwijder eerdere profielen. zoek naar een locatie op de harde schijf : *.xml.
3. Wanneer u naar de programma's Add/Remove gaat, hebt u zowel een AnyConnect-installatie als een AnyConnect VPN-installatie?
4. Installeer de AnyConnect-client.
5. Schakel het AnyConnect-logbestand van de gebruiker in het Event Viewer uit en test opnieuw.
6. Blader weer naar het security apparaat om de client opnieuw te installeren.
7. Zorg dat het profiel ook verschijnt.
8. Opnieuw beginnen. Bij de volgende herstart wordt u gevraagd met de knop Start voordat u zich aangemeld hebt.
9. Verzend het log van AnyConnect-gebeurtenis naar Cisco in .evt-formaat.
10. Als u deze fout ziet, verwijdert u het gebruikersprofiel en gebruikt u het standaardprofiel:

```
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.
```

Probleem 1

Deze foutmelding wordt gezien tijdens het uploaden van het AnyConnect-profiel: `Fout bij valideren van het XML-bestand tegen het nieuwste schema`. Hoe is deze fout opgelost?

Oplossing 1

Deze foutmelding wordt meestal veroorzaakt door de syntaxis of door configuratieproblemen in het AnyConnect-profiel. Zorg ervoor dat het geconfigureerde AnyConnect-profiel vergelijkbaar is met het Sample AnyConnect-profiel dat in het AnyConnect-profiel en het XML-gedeelte van de Cisco AnyConnect VPN-clientbeheerdershandleiding aanwezig is.

Gerelateerde informatie

- Cisco AnyConnect VPN-clientbeheerdershandleiding, versie 2.0
- Logon-scripts maken - Windows TechNet
- Starten voor aanmelding (PLAP) configureren op Windows Vista-systemen
- ASA 8.500 VPN-toegang met AnyConnect SSL VPN-clientconfiguratievoorbeeld
- Cisco AnyConnect VPN-client
- Cisco ASA 5500 Series adaptieve security applicaties
- Technische ondersteuning en documentatie – Cisco Systems