ASA 8.x: Konfiguration der AnyConnect Start-Funktion vor der Anmeldung

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Hintergrundinformationen
Installieren von Startkomponenten vor der Anmeldung (nur Windows)
Unterschiede zwischen Windows-Vista\Windows 7 und dem Start vor Vista vor der Anmeldung
XML-Einstellungen zum Aktivieren von SBL
SBL aktivieren
Konfiguration vor Anmeldung mit CLI starten
Konfiguration vor Anmeldung mit ASDM starten
Verwenden der Manifestdatei
Fehlerbehebung SBL
Problem 1
Lösung 1
Zugehörige Informationen

Einführung

Wenn *Start Before Logon* (SBL) aktiviert ist, sieht der Benutzer das Dialogfeld für die Anmeldung über die AnyConnect-GUI, bevor das Dialogfeld Windows® Anmeldung angezeigt wird. Dadurch wird zuerst die VPN-Verbindung hergestellt. Nur für Windows-Plattformen verfügbar: Start Before Logon ermöglicht dem Administrator die Kontrolle über die Verwendung von Anmeldeskripts, Kennwortzwischenspeicherung, Zuordnung von Netzlaufwerken zu lokalen Laufwerken usw. Sie können die SBL-Funktion verwenden, um das VPN als Teil der Anmeldungssequenz zu aktivieren. SBL ist standardmäßig deaktiviert.

Weitere Informationen zum Konfigurieren der Funktionen des AnyConnect VPN Client finden Sie im Abschnitt Konfigurieren der Funktionen des AnyConnect Client.

Hinweis: Innerhalb des AnyConnect-Clients können Sie nur die Funktion für SBL aktivieren. Netzwerkadministratoren verarbeiten die Verarbeitung vor der Anmeldung entsprechend den Anforderungen ihrer Situation. Anmeldeskripts können einer Domäne oder einzelnen Benutzern zugewiesen werden. Im Allgemeinen verfügen die Administratoren der Domäne über Stapeldateien oder Ähnliches, die mit Benutzern oder Gruppen in Active Directory definiert sind. Sobald sich der Benutzer anmeldet, wird das Anmeldeskript ausgeführt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliances der Serie ASA 5500 mit Softwareversion 8.x
- Cisco AnyConnect VPN Version 2.0

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

SBL verbindet einen Remote-Computer mit der Unternehmensinfrastruktur, bevor er sich am PC anmeldet. Ein Benutzer kann beispielsweise außerhalb des physischen Unternehmensnetzwerks arbeiten und nicht auf Unternehmensressourcen zugreifen, bis sein PC dem Unternehmensnetzwerk beigetreten ist. Wenn SBL aktiviert ist, stellt der AnyConnect-Client eine Verbindung her, bevor der Benutzer das Microsoft-Anmeldefenster sieht. Der Benutzer muss sich wie gewohnt auch bei Windows anmelden, wenn das Microsoft-Anmeldefenster angezeigt wird.

Dies sind mehrere Gründe für die Verwendung von SBL:

- Der PC des Benutzers ist mit einer Active Directory-Infrastruktur verbunden.
- Der Benutzer kann keine zwischengespeicherten Anmeldeinformationen auf dem PC haben, d. h., wenn die Gruppenrichtlinie zwischengespeicherte Anmeldeinformationen deaktiviert.
- Der Benutzer muss Anmeldeskripts ausführen, die von einer Netzwerkressource ausgeführt werden oder die Zugriff auf eine Netzwerkressource erfordern.
- Ein Benutzer verfügt über netzwerkbasierte Laufwerke, die eine Authentifizierung mit der Active Directory-Infrastruktur erfordern.
- Netzwerkkomponenten wie MS NAP/CS NAC können eine Verbindung zur Infrastruktur erfordern.

SBL erstellt ein Netzwerk, das der Einbindung in das lokale Firmen-LAN entspricht. Wenn SBL aktiviert ist, können die Benutzer, da sie Zugriff auf die lokale Infrastruktur haben, auch die Anmeldeskripts, die normalerweise für einen Benutzer im Büro ausgeführt werden, für den Remote-Benutzer nutzen.

Informationen zum Erstellen von Anmeldeskripts finden Sie in diesem Microsoft TechNet-Artikel .

Informationen zur Verwendung lokaler Anmeldeskripte in Windows XP finden Sie in diesem Microsoft-Artikel .

In einem anderen Beispiel kann ein System so konfiguriert werden, dass zwischengespeicherte Anmeldeinformationen für die Anmeldung am PC nicht zugelassen werden. In diesem Szenario müssen Benutzer mit einem Domänen-Controller im Unternehmensnetzwerk kommunizieren können, damit ihre Anmeldeinformationen vor dem Zugriff auf den PC validiert werden können. SBL erfordert, dass zum Zeitpunkt des Aufrufs eine Netzwerkverbindung vorhanden ist. In einigen Fällen ist dies nicht möglich, da eine Wireless-Verbindung von Benutzeranmeldeinformationen für die Verbindung mit der Wireless-Infrastruktur abhängen kann. Da der SBL-Modus der Anmeldephase vorausgeht, ist in diesem Szenario keine Verbindung verfügbar. In diesem Fall muss die Wireless-Verbindung so konfiguriert werden, dass die Anmeldeinformationen bei der Anmeldung zwischengespeichert werden, oder es muss eine andere Wireless-Authentifizierung konfiguriert werden, damit die SBL funktioniert.

Installieren von Startkomponenten vor der Anmeldung (nur Windows)

Die Komponenten Start Before Logon müssen nach der Installation des Core-Clients installiert werden. Darüber hinaus müssen für die Komponenten AnyConnect 2.2 Start Before Logon (Start vor Anmeldung) die Kernversion 2.2 oder höher der AnyConnect-Clientsoftware installiert sein. Wenn Sie den AnyConnect-Client und die Komponenten "Start Before Logon" mit den MSI-Dateien vorab bereitstellen (z. B. in einem großen Unternehmen mit eigener Softwarebereitstellung (Altiris, Active Directory oder SMS), müssen Sie die richtige Bestellung aufgeben. Die Reihenfolge der Installation wird automatisch gehandhabt, wenn der Administrator AnyConnect lädt, wenn die Installation über das Internet bereitgestellt und/oder über das Internet aktualisiert wird. Vollständige Installationsinformationen finden Sie in den Versionshinweisen für den Cisco AnyConnect VPN Client, Version 2.2.

Unterschiede zwischen Windows-Vista\Windows 7 und dem Start vor Vista vor der Anmeldung

Die Vorgehensweise zum Aktivieren von SBL ist in Windows Vista- und Windows 7-Systemen leicht unterschiedlich. Systeme vor Vista verwenden eine Komponente namens Virtual Private Network Graphical Identification and Authentication (VPNGINA), um SBL zu implementieren. Vista- und Windows 7-Systeme verwenden eine Komponente namens PLAP, um SBL zu implementieren.

Im AnyConnect-Client wird die Windows Vista-Funktion "Start Before Logon" (Start vor Anmeldung) als Pre-Login Access Provider (PLAP) bezeichnet, der eine Verbindung mit Anmeldeinformationen herstellt. Mit dieser Funktion können Netzwerkadministratoren vor der Anmeldung bestimmte Aufgaben ausführen, z. B. die Erfassung von Anmeldeinformationen oder die Verbindung mit Netzwerkressourcen. Die PLAP stellt die Funktionen "Start Before Logon" (Start vor Anmeldung) unter Windows Vista, Windows 7 und dem Windows 2008-Server bereit. PLAP unterstützt 32-Bit- und 64-Bit-Versionen des Betriebssystems mit vpnplap.dll bzw. vpnplap64.dll. Die PLAP-Funktion unterstützt die Versionen Windows Vista x86 und x64.

Hinweis: In diesem Abschnitt bezieht sich VPNGINA auf die Funktion "Start vor Anmeldung" für Pre-Vista-Plattformen, und die PLAP bezieht sich auf die Funktion "Start vor Anmeldung" für

Windows Vista- und Windows 7-Systeme.

In Systemen vor Vista verwendet Start Before Logon eine Komponente, die als VPN Graphical Identification and Authentication Dynamic Link Library (vpngina.dll) bezeichnet wird, um Funktionen für den Start Before Logon bereitzustellen. Die Windows-PLAP-Komponente, die Teil von Windows Vista ist, ersetzt die Windows-GINA-Komponente.

Ein GINA wird aktiviert, wenn ein Benutzer die Tastenkombination Strg+Alt+Entf drückt. Bei PLAP öffnet die Tastenkombination Strg+Alt+Entf ein Fenster, in dem der Benutzer entweder eine Anmeldung beim System durchführen oder Netzwerkverbindungen (PLAP-Komponenten) aktivieren kann. Die Schaltfläche Network Connect (Netzwerkverbindung) befindet sich in der rechten unteren Ecke des Fensters.

In den folgenden Abschnitten werden die Einstellungen und Verfahren für VPNGINA und PLAP SBL beschrieben. Eine vollständige Beschreibung der Aktivierung und Verwendung der SBL-Funktion (PLAP) auf einer Windows Vista-Plattform finden Sie unter Konfigurieren von Start Before Logon (PLAP) auf Windows Vista-Systemen.

XML-Einstellungen zum Aktivieren von SBL

Mit dem Elementwert für UseStartBeforeLogon kann dieses Feature aktiviert (true) oder deaktiviert (false) werden. Wenn Sie diesen Wert im Profil auf **true** festlegen, erfolgt die weitere Verarbeitung als Teil der Anmeldungssequenz. Weitere Informationen finden Sie in der Beschreibung Start Before Logon (Vor Anmeldung starten). Legen Sie den <UseStartBefore Logon>-Wert in der Datei CiscoAnyConnect.xml auf **true fest**, um SBL zu aktivieren:

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

Um SBL zu deaktivieren, legen Sie denselben Wert auf **false fest**.

Um die UserControllable-Funktion zu aktivieren, verwenden Sie diese Anweisung, wenn Sie SBL aktivieren:

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

Alle Benutzereinstellungen, die diesem Attribut zugeordnet sind, werden an einem anderen Ort gespeichert.

SBL aktivieren

Um die Download-Zeit zu minimieren, fordert der AnyConnect-Client nur die Kernmodule (von der Sicherheits-Appliance) an, die er für jede unterstützte Funktion benötigt. Um neue Funktionen, wie z. B. SBL, zu aktivieren, müssen Sie den Modulnamen mit dem Befehl **svc modules** aus dem Gruppenrichtlinien-WebVPN oder dem WebVPN-Konfigurationsmodus für den Benutzernamen angeben:

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

Der Zeichenfolgenwert für SBL ist **vpngina**.

In diesem Beispiel wechselt der Netzwerkadministrator in den Gruppenrichtlinien-Attributmodus für die Gruppenrichtlinien-Telearbeiter. Wechselt in den WebVPN-Konfigurationsmodus für die Gruppenrichtlinie. und gibt die Zeichenfolge VPNGINA an, um SBL zu aktivieren:

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

Darüber hinaus muss der Administrator sicherstellen, dass die <UseStartBeforeLogon>-Anweisung in der Datei "AnyConnect <profile.xml>", in der der Netzwerkadministrator der XML-Datei zugewiesen hat, auf **true** festgelegt ist, z. B.:

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

Das System muss neu gestartet werden, bevor die Anmeldung wirksam wird. Sie müssen außerdem auf der Sicherheits-Appliance angeben, dass Sie SBL zulassen möchten, oder andere Module für zusätzliche Funktionen. Weitere Informationen finden Sie in der Beschreibung im Abschnitt Enabling Modules (ASDM) (Enabling Modules for Additional AnyConnect Features), Seite 2-5 (ASDM) oder Enabling Modules for Additional AnyConnect Features, Seite 3-4 (CLI).

Konfiguration vor Anmeldung mit CLI starten

Dieses Szenario zeigt Ihnen, wie Sie die XML-Datei mit CLI einrichten:

1. Erstellen Sie ein Profil, das auf die Client-PCs übertragen werden soll, die ähnlich wie folgt aussehen:
```
<?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. Kopieren Sie die Datei in den Flash-Speicher der Sicherheits-Appliance:

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

3. Fügen Sie auf der Sicherheits-Appliance das Profil als verfügbares Profil zum globalen WebVPN-Abschnitt hinzu, sofern für AnyConnect-Verbindungen alles andere richtig eingerichtet ist:

```
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)#
   svc profiles ReallyNewProfile disk0:/AnyConnectProfile.xml
```

4. Bearbeiten Sie die von Ihnen verwendete Gruppenrichtlinie, und fügen Sie die Befehle **svc-Module** und **svc-Profil hinzu**:

```
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
```

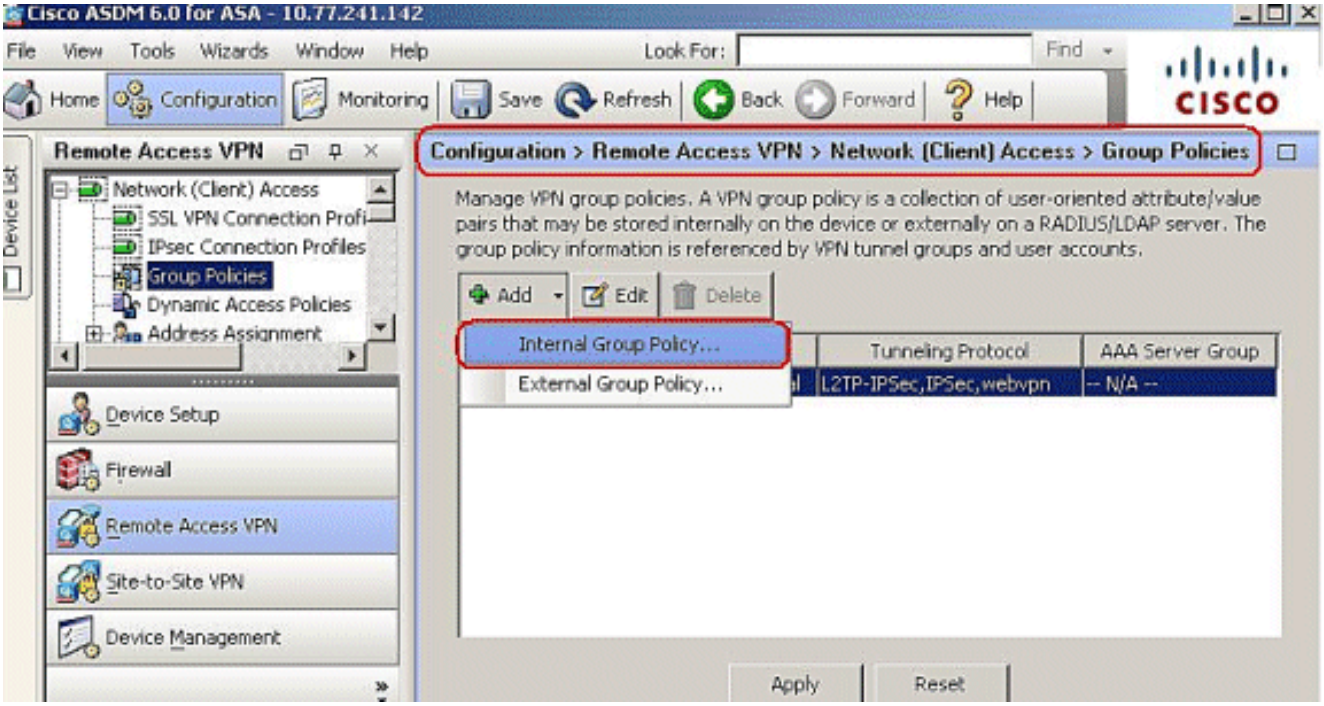
Konfiguration vor Anmeldung mit ASDM starten

Gehen Sie wie folgt vor, um das SBL mit ASDM zu konfigurieren:

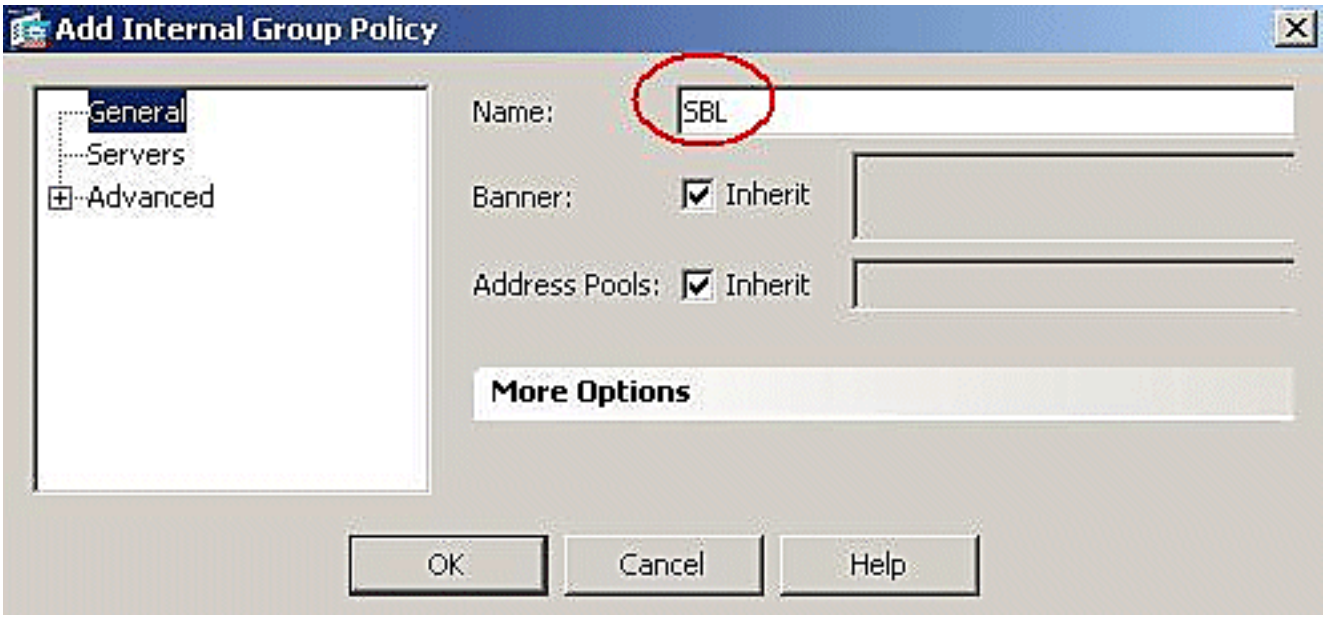
1. Erstellen Sie ein Profil, das auf die Client-PCs übertragen werden soll, die ähnlich wie folgt aussehen:

```
<?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>
```

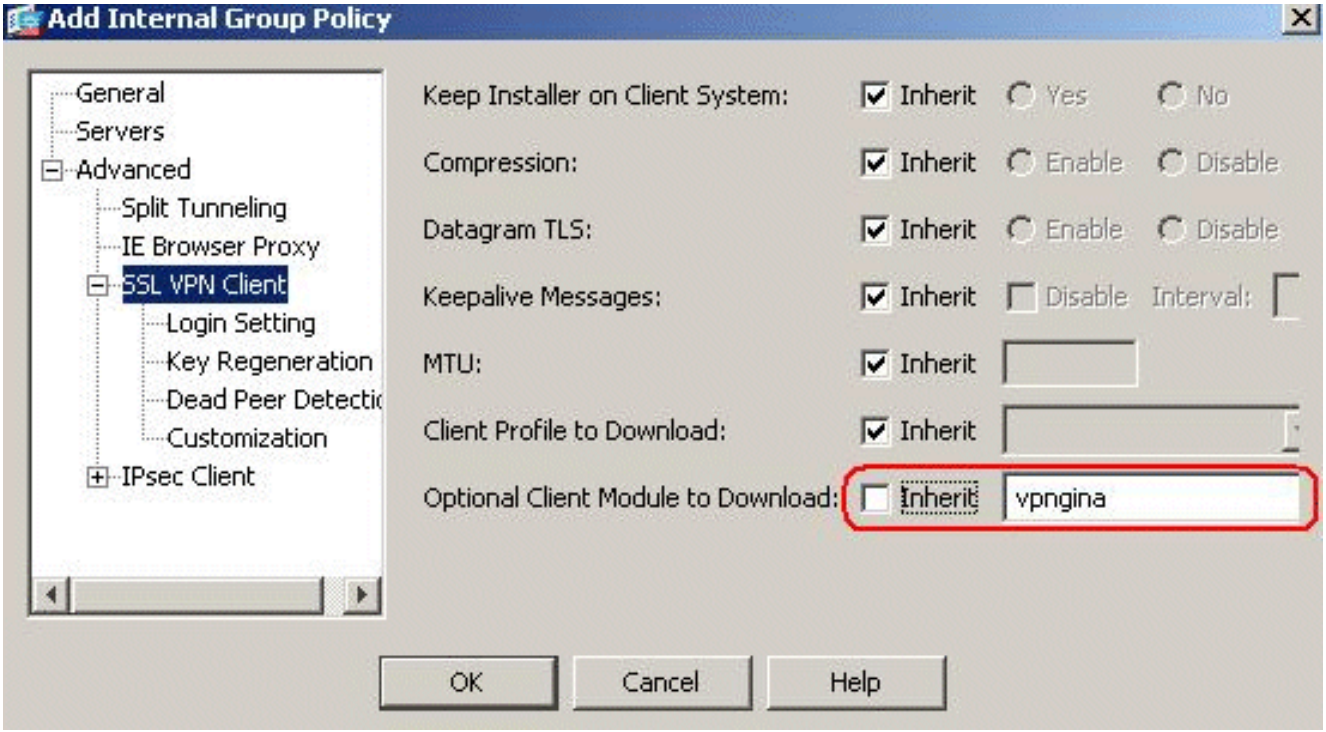
2. Speichern Sie das Profil als **AnyConnectProfile.xml** auf dem lokalen Computer.
3. Starten Sie das ASDM, und wechseln Sie zur Startseite.
4. Gehen Sie zu **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add** , und klicken Sie auf **Internal Group Policy (Interne Gruppenrichtlinie)**.



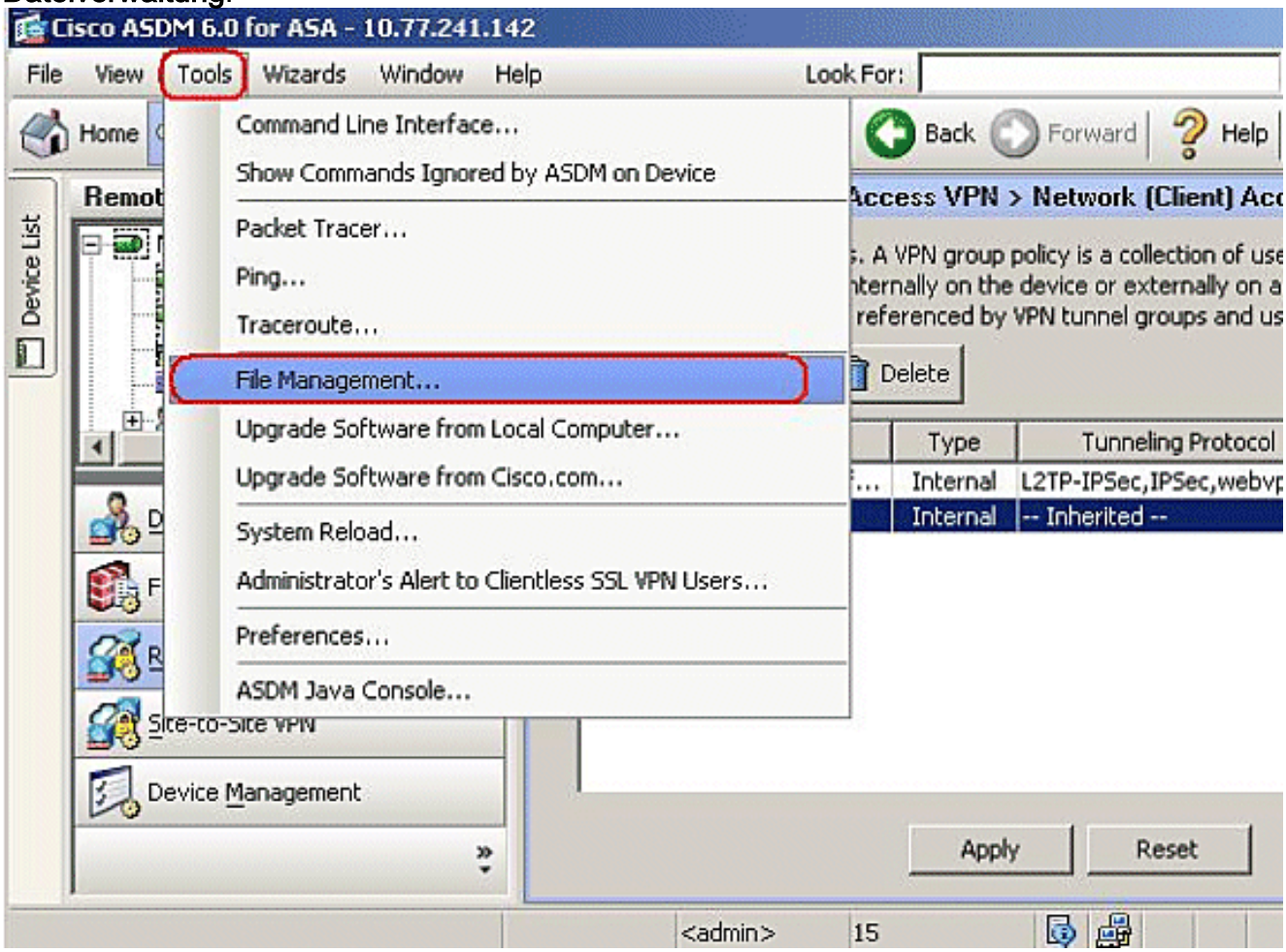
5. Geben Sie den Namen der Gruppenrichtlinie ein, z. B. **SBL**.



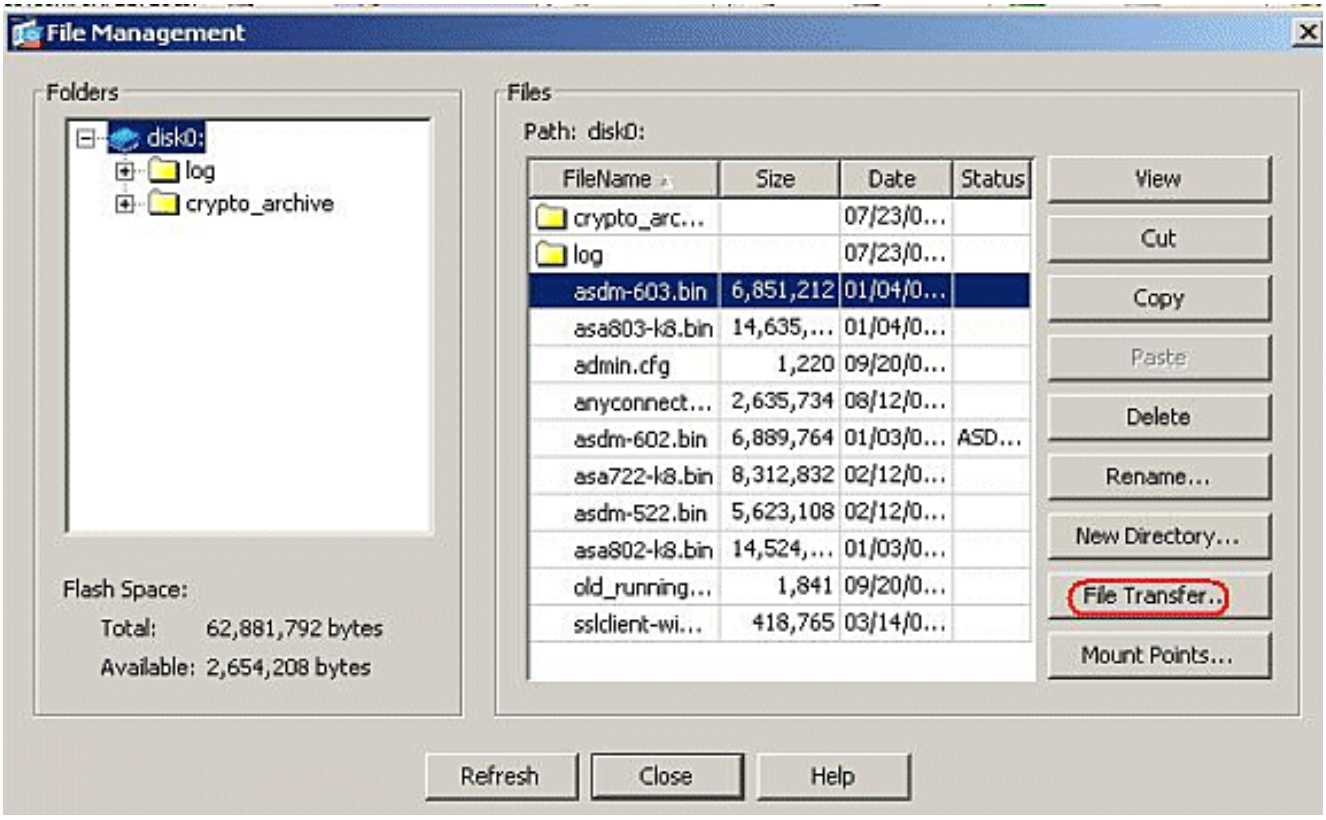
6. Gehen Sie zu **Advanced > SSL VPN Client**. Entfernen Sie das Häkchen Erben im **optionalen Client-Modul zum Download**, und wählen Sie **vpngina** aus dem Dropdown-Feld aus.



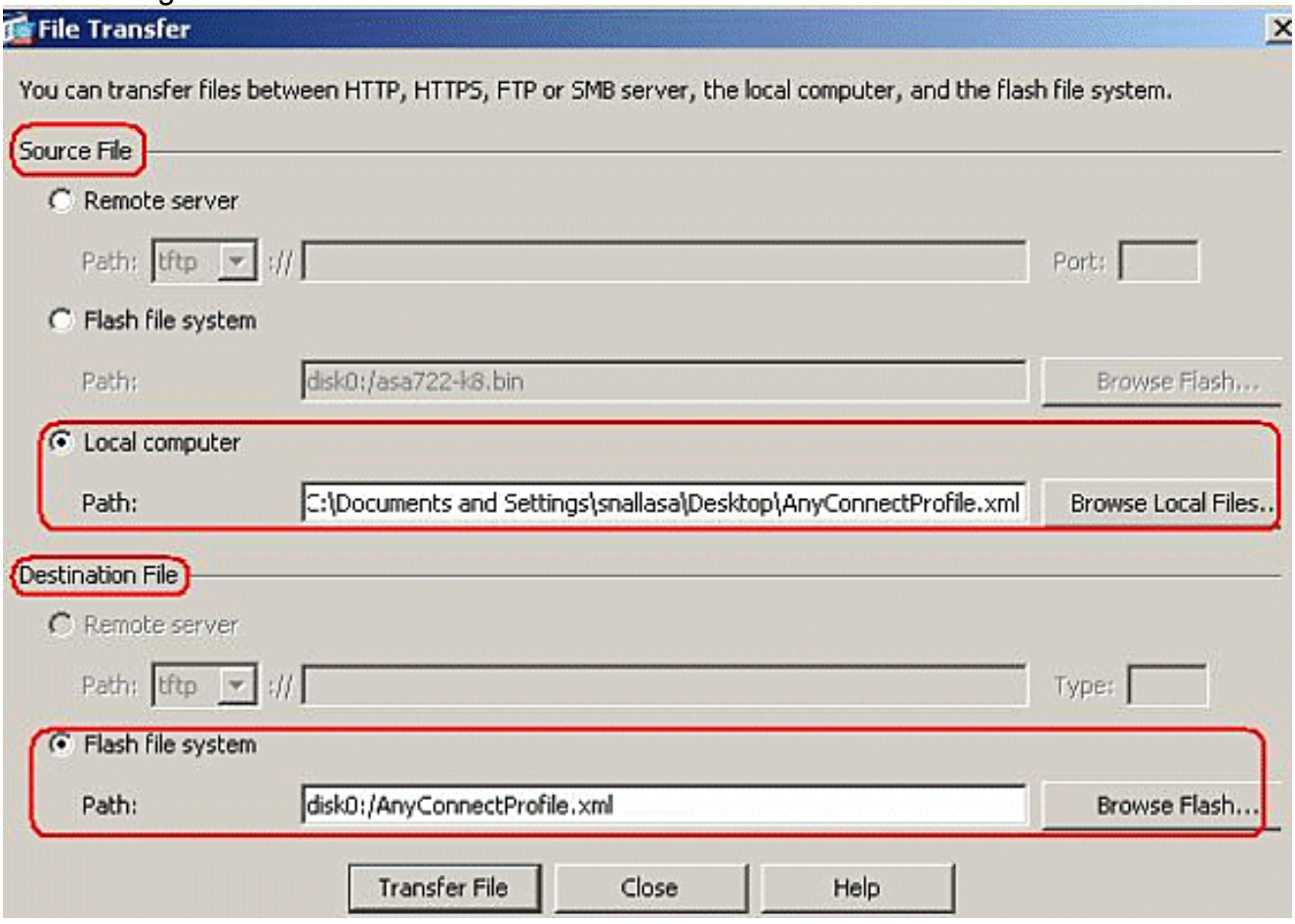
7. Um das Profil **AnyConnectProfile.xml** vom lokalen Computer in Flash zu übertragen, gehen Sie zu **Extras**, und klicken Sie auf **Dateiverwaltung**.



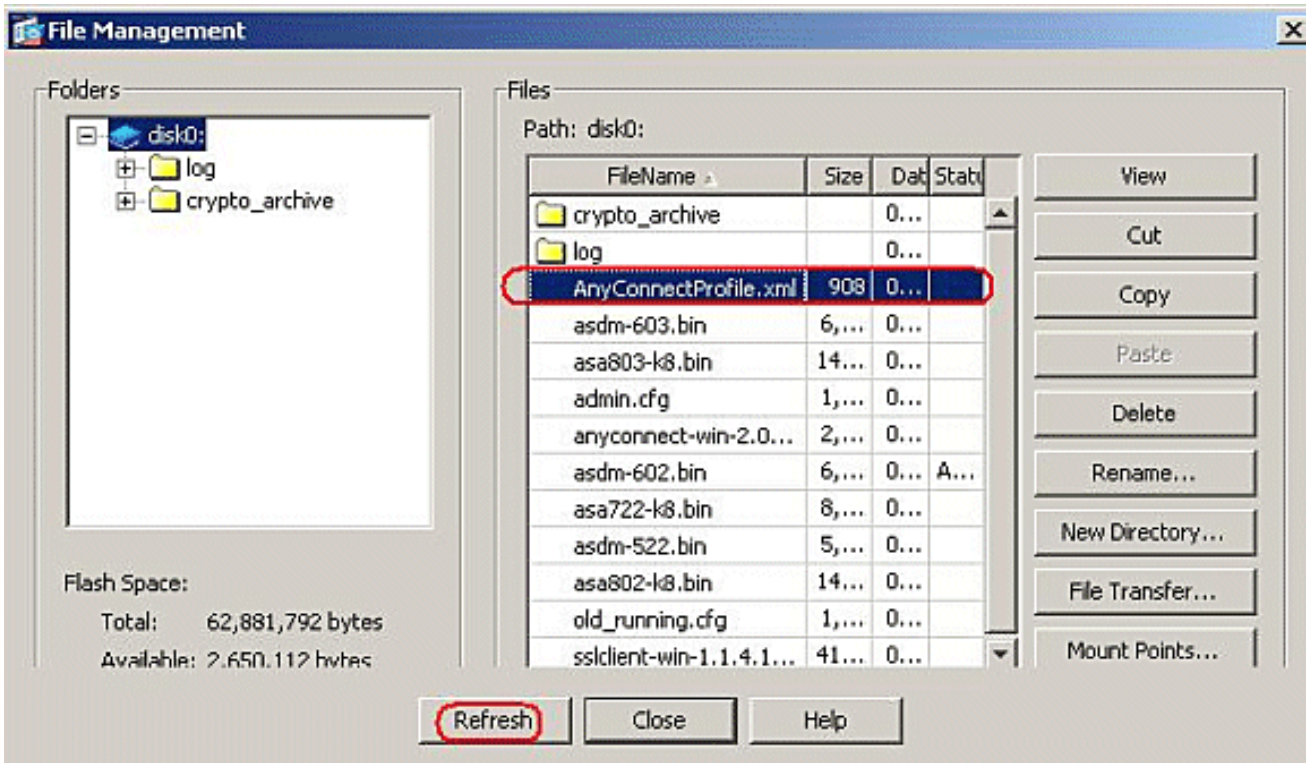
8. Klicken Sie auf die Schaltfläche **Dateiübertragung**.



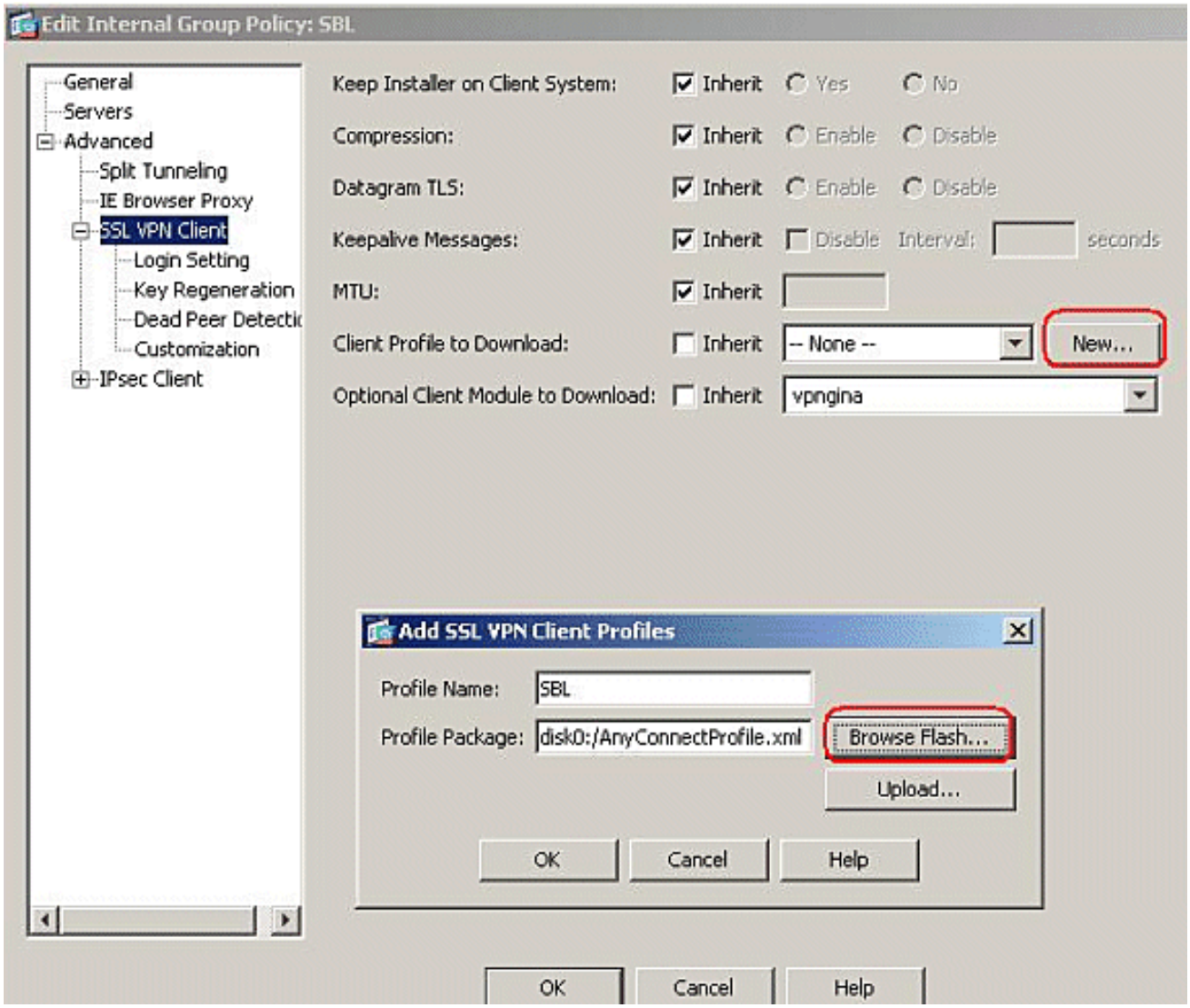
9. Um das Profil vom lokalen Computer in den ASA Flash-Speicher zu übertragen, wählen Sie die **Quelldatei**, den Pfad der XML-Datei (lokaler Computer) und den Pfad der **Zieldatei** entsprechend Ihrer Anforderungen.



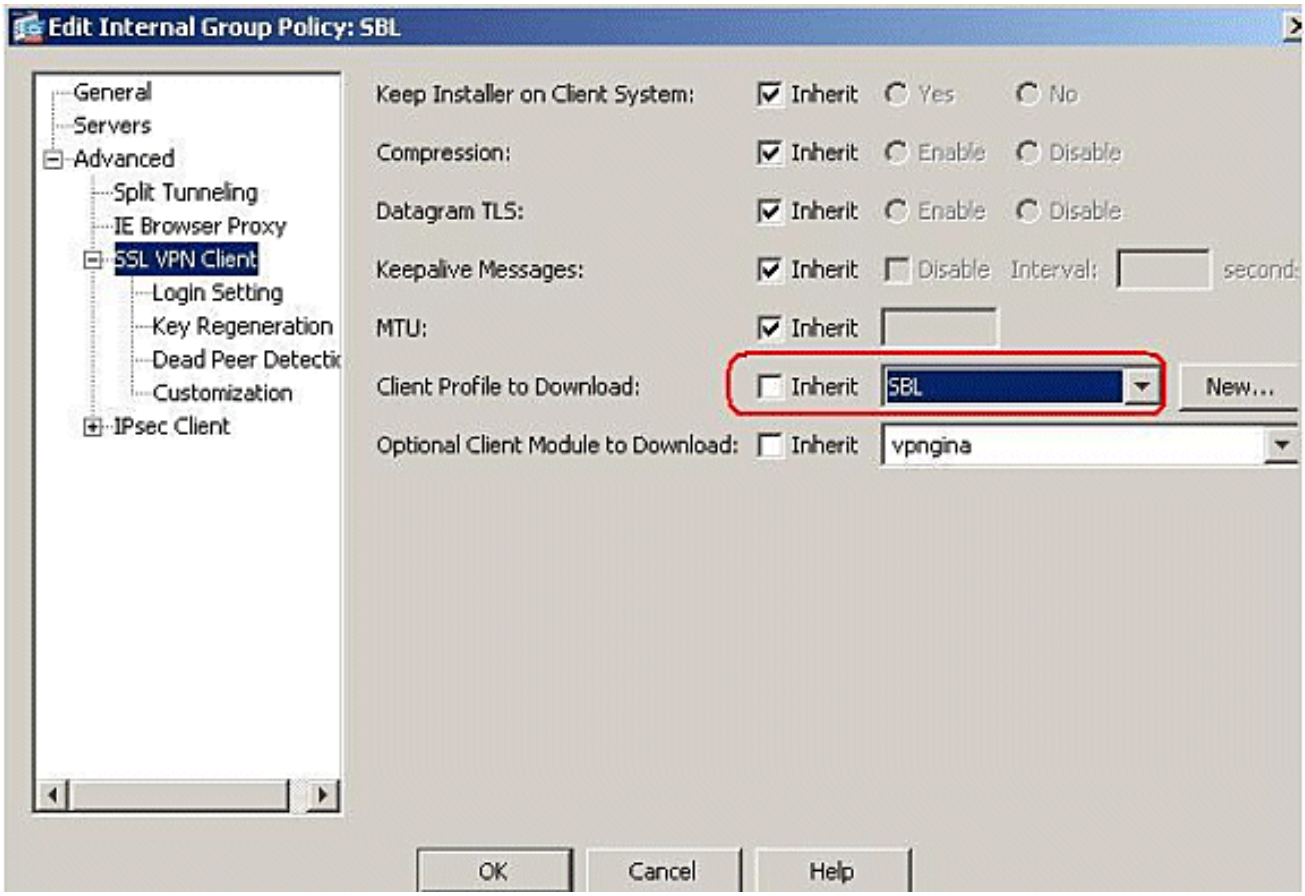
10. Klicken Sie nach der Übertragung auf die Schaltfläche **Aktualisieren**, um zu überprüfen, ob sich die Profildatei im Flash-Speicher befindet.



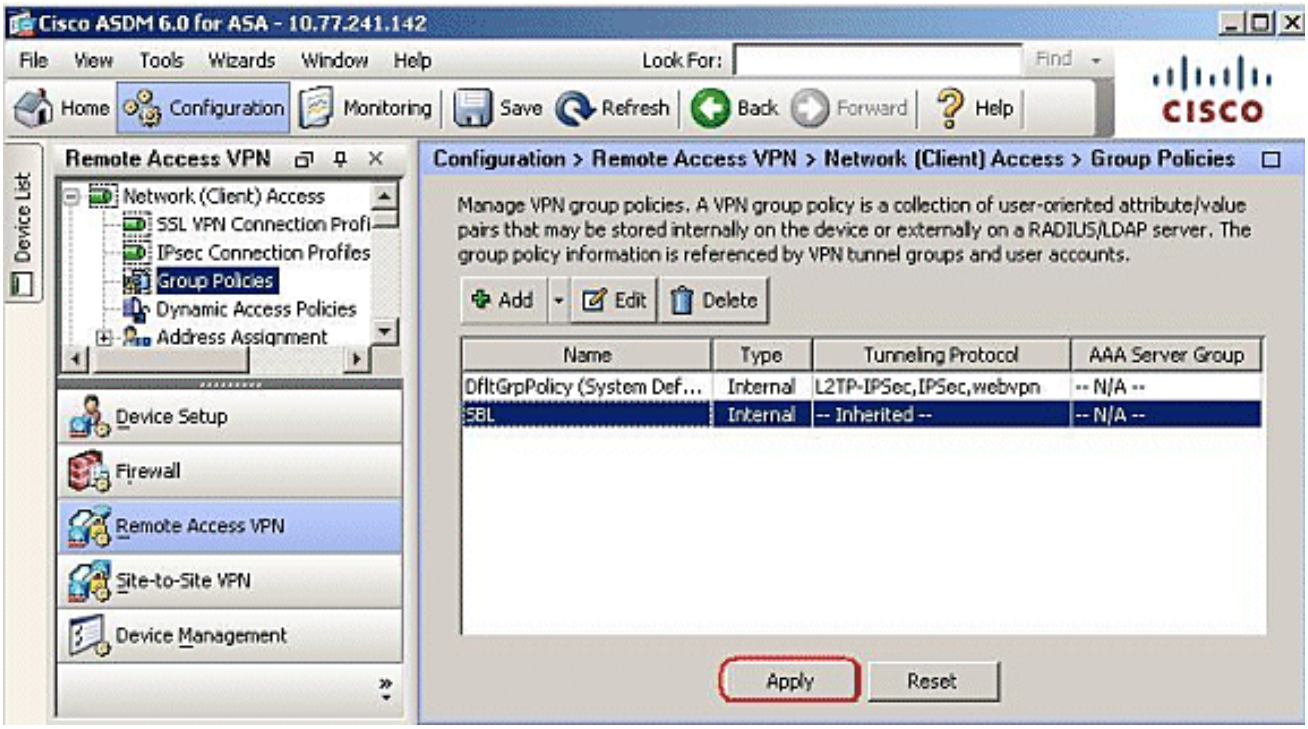
11. Weisen Sie das Profil der internen Gruppenrichtlinie (**SBL**) zu.Folgen Sie diesem Pfad, **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Edit SBL (Internal Group Policy) > Advanced > SSL VPN Client > Client Profile to Download**, und klicken Sie auf die **Schaltfläche New**.Klicken Sie in **Add SSL VPN Client Profiles (SSL VPN-Clientprofile hinzufügen)** auf die **Schaltfläche Browse (Durchsuchen)**, um den Speicherort des Profils (**AnyConnectProfile.xml**) auszuwählen, das im ASA Flash-Speicher gespeichert ist. Weisen Sie den **Namen** für das Profil zu, z. B. **SBL**. Klicken Sie zum Abschließen auf
OK.



12. Deaktivieren Sie das Kontrollkästchen Vererbung, und wählen Sie im Feld **Client Profile to Download** (Zu **downloadendes Clientprofil) SBL aus**. Klicken Sie auf **OK**.



13. Klicken Sie auf **Apply**, um den Vorgang abzuschließen.



Verwenden der Manifestdatei

Das auf der Sicherheits-Appliance hochgeladene AnyConnect-Paket enthält die Datei VPNManifest.xml. Dieses Beispiel zeigt einen Beispielinhalt dieser Datei:

```
<?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>
```

Die Sicherheits-Appliance hat, wie in Schritt 1 erläutert, konfigurierte Profile gespeichert und speichert außerdem ein oder mehrere AnyConnect-Pakete, die den AnyConnect-Client selbst, das Download-Dienstprogramm, die Manifestdatei und alle anderen optionalen Module oder Support-Dateien enthalten.

Wenn ein Remote-Benutzer über WebLaunch oder einen aktuellen Standalone-Client eine Verbindung zur Sicherheits-Appliance herstellt, wird der Downloader zuerst heruntergeladen und ausgeführt. Mithilfe der Manifestdatei wird ermittelt, ob auf dem PC des Remote-Benutzers ein aktueller Client aktualisiert werden muss oder eine Neuinstallation erforderlich ist. Die Manifestdatei enthält außerdem Informationen darüber, ob optionale Module zum Herunterladen und Installieren der VPNGINA vorhanden sind. Das Clientprofil wird auch von der Sicherheits-Appliance heruntergefahren. Die Installation von VPNGINA wird mithilfe des Befehls **svc modules value vpngina** aktiviert, der im Befehlsmodus für die **Gruppenrichtlinie (webvpn)** konfiguriert wurde, wie in Schritt 4 beschrieben. Der AnyConnect-Client und VPNGINA werden installiert, und der Benutzer sieht den AnyConnect-Client beim nächsten Neustart vor der Anmeldung bei der Windows-Domäne.

Wenn der Benutzer eine Verbindung herstellt, werden der Client und das Profil an den Benutzer-PC weitergeleitet. der Client und VPNGINA installiert sind; und der Benutzer sieht den AnyConnect-Client beim nächsten Neustart vor der Anmeldung.

Ein Beispielprofil wird auf dem Client-PC bereitgestellt, wenn AnyConnect installiert ist: **C:\Documents and Settings\All Users\Application Data\Cisco\Cisco\AnyConnect VPN Client\Profile\AnyConnectProfile**.

Fehlerbehebung SBL

Gehen Sie folgendermaßen vor, wenn ein Problem mit SBL auftritt:

1. Stellen Sie sicher, dass das Profil gedrückt wird.
2. Löschen Sie vorherige Profile. Suchen Sie auf der Festplatte nach diesen, um den Speicherort zu finden: *.xml
3. Verfügen Sie beim Öffnen der Software über eine AnyConnect-Installation und eine AnyConnect VPNGINA-Installation?
4. Deinstallieren Sie den AnyConnect-Client.
5. Löschen Sie das AnyConnect-Protokoll des Benutzers in der Ereignisanzeige, und testen Sie es erneut.
6. Surfen Sie im Internet wieder zur Sicherheits-Appliance, um den Client neu zu installieren.
7. Stellen Sie sicher, dass das Profil auch angezeigt wird.
8. Einmal neu starten. Beim nächsten Neustart wird die Aufforderung Start Before Logon (Vor Anmeldung starten) angezeigt.
9. Senden Sie das AnyConnect-Ereignisprotokoll im EVT-Format an Cisco.
10. Wenn Sie diesen Fehler sehen, löschen Sie das Benutzerprofil, und verwenden Sie das

Standardprofil:

```
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.
```

Problem 1

Diese Fehlermeldung wird beim Upload des AnyConnect-Profils angezeigt: `Fehler bei der Validierung der XML-Datei anhand des aktuellen Schemas`. Wie wird dieser Fehler behoben?

Lösung 1

Diese Fehlermeldung tritt hauptsächlich aufgrund der Syntax- oder Konfigurationsprobleme im AnyConnect-Profil auf. Um dieses Problem zu beheben, stellen Sie sicher, dass das konfigurierte AnyConnect-Profil dem AnyConnect-Beispielprofil im Abschnitt Beispiel für ein AnyConnect-Profil und XML-Schema im Administratorhandbuch für den Cisco AnyConnect VPN-Client ähnelt.

Zugehörige Informationen

- Administratoranleitung für den Cisco AnyConnect VPN Client, Version 2.0
- Erstellen von Anmeldeskripts - Windows TechNet
- Konfigurieren von Start Before Logon (PLAP) auf Windows Vista-Systemen
- ASA 8.x-VPN-Zugriff mit dem AnyConnect SSL VPN-Client - Konfigurationsbeispiel
- Cisco AnyConnect VPN-Client
- Cisco Adaptive Security Appliances der Serie ASA 5500
- Technischer Support und Dokumentation - Cisco Systems