ASA 8.X: Configuración de la función AnyConnect Start Before Logon

Contenido

Introducción

Con *Start Before Logon* (SBL) habilitado, el usuario ve el diálogo de inicio de sesión de la GUI de AnyConnect antes de que aparezca el cuadro de diálogo de inicio de sesión de Windows®. Esto establece primero la conexión VPN. Disponible solamente para las plataformas Windows, Start Before Logon permite al administrador controlar el uso de scripts de login, almacenamiento en caché de la contraseña, mapear controladores de red a unidades locales y mucho más. Puede utilizar la función SBL para activar la VPN como parte de la secuencia de inicio de sesión. SBL está inhabilitado de forma predeterminada.

Para obtener más información sobre la configuración de las funciones de AnyConnect VPN Client, refiérase a la sección Configuración de las Funciones de AnyConnect Client.

Nota: Dentro del cliente AnyConnect, la única configuración que realiza para SBL es habilitar la función. Los administradores de red gestionan el procesamiento que se realiza antes del inicio de sesión en función de los requisitos de su situación. Los scripts de inicio de sesión se pueden asignar a un dominio o a usuarios individuales. Generalmente, los administradores del dominio tienen archivos por lotes o similares definidos con usuarios o grupos en Active Directory. En cuanto el usuario inicia sesión, se ejecuta la secuencia de comandos de inicio de sesión.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ASA 5500 Series Adaptive Security Appliances que ejecutan la versión de software 8.x
- Cisco AnyConnect VPN versión 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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

El punto de SBL es que conecta un equipo remoto a la infraestructura de la empresa antes de iniciar sesión en el PC. Por ejemplo, un usuario puede estar fuera de la red corporativa física, sin poder acceder a los recursos corporativos hasta que su PC se haya unido a la red corporativa. Con SBL habilitado, el cliente AnyConnect se conecta antes de que el usuario vea la ventana de inicio de sesión de Microsoft. El usuario también debe iniciar sesión, como de costumbre, en Windows cuando aparezca la ventana de inicio de sesión de Microsoft.

Estas son varias razones para utilizar SBL:

- El equipo del usuario se une a una infraestructura de Active Directory.
- El usuario no puede tener credenciales almacenadas en caché en la PC, es decir, si la política de grupo no permite las credenciales almacenadas en caché.
- El usuario debe ejecutar secuencias de comandos de inicio de sesión que se ejecuten desde un recurso de red o que requieran acceso a un recurso de red.
- Un usuario tiene unidades asignadas a la red que requieren autenticación con la infraestructura de Active Directory.
- Los componentes de red, como MS NAP/CS NAC, pueden requerir conexión a la infraestructura.

SBL crea una red equivalente a la inclusión en la LAN corporativa local. Con SBL habilitado, dado que el usuario tiene acceso a la infraestructura local, los scripts de inicio de sesión que se ejecutan normalmente para un usuario en la oficina también están disponibles para el usuario remoto.

Para obtener información sobre cómo crear scripts de inicio de sesión, refiérase a este artículo de

Microsoft TechNet.

Para obtener información sobre cómo utilizar secuencias de comandos de inicio de sesión locales en Windows XP, refiérase a este artículo de Microsoft.

En otro ejemplo, se puede configurar un sistema para que no permita las credenciales almacenadas en caché para iniciar sesión en el equipo. En esta situación, los usuarios deben poder comunicarse con un controlador de dominio de la red corporativa para que sus credenciales se validen antes de acceder al PC. SBL requiere que una conexión de red esté presente en el momento en que se invoca. En algunos casos, esto no es posible porque una conexión inalámbrica puede depender de las credenciales del usuario para conectarse a la infraestructura inalámbrica. Dado que el modo SBL precede a la fase de credenciales de un inicio de sesión, una conexión no está disponible en este escenario. En este caso, la conexión inalámbrica debe configurarse para almacenar en caché las credenciales a través del login, o bien debe configurarse otra autenticación inalámbrica para que SBL funcione.

Instalar componentes Start Before Logon (sólo Windows)

Los componentes Start Before Logon deben instalarse después de que se haya instalado el cliente principal. Además, los componentes de AnyConnect 2.2 Start Before Logon requieren que se instale la versión 2.2 o posterior del software de cliente AnyConnect principal. Si implementa previamente el cliente AnyConnect y los componentes Start Before Logon con los archivos MSI (por ejemplo, se encuentra en una gran empresa que tiene su propia implementación de software (Altiris, Active Directory o SMS), debe obtener el pedido correctamente. El orden de la instalación se controla automáticamente cuando el administrador carga AnyConnect si se implementa en la Web o se actualiza en la Web. Para obtener información completa sobre la instalación, consulte Release Notes for Cisco AnyConnect VPN Client, Release 2.2.

Diferencias entre Windows-Vista\Windows 7 y Pre-Vista Start antes de iniciar sesión

Los procedimientos para habilitar SBL difieren ligeramente en los sistemas Windows Vista y Windows 7. Los sistemas anteriores a Vista utilizan un componente denominado autenticación e identificación gráfica de red privada virtual (VPNGINA) para implementar SBL. Los sistemas Vista y Windows 7 utilizan un componente llamado PLAP para implementar SBL.

En el cliente AnyConnect, la función Inicio antes de inicio de sesión de Windows Vista se conoce como Proveedor de acceso previo a inicio de sesión (PLAP), que es un proveedor de credenciales conectable. Esta función permite a los administradores de red realizar tareas específicas, como la recopilación de credenciales o la conexión a los recursos de red, antes del inicio de sesión. PLAP proporciona las funciones Start Before Logon en Windows Vista, Windows 7 y Windows 2008 Server. PLAP admite versiones de 32 y 64 bits del sistema operativo con vpnplap.dll y vpnplap64.dll, respectivamente. La función PLAP admite las versiones x86 y x64 de Windows Vista.

Nota: En esta sección, VPNGINA hace referencia a la función Start Before Logon para las plataformas anteriores a Vista y PLAP hace referencia a la función Start Before Logon para los sistemas Windows Vista y Windows 7.

En los sistemas anteriores a Vista, Start Before Logon utiliza un componente conocido como la biblioteca de vínculos dinámicos de identificación gráfica y autenticación (vpngina.dll) de VPN

para proporcionar las funciones Start Before Logon (Inicio antes del inicio de sesión). El componente PLAP de Windows, que forma parte de Windows Vista, reemplaza el componente GINA de Windows.

Una GINA se activa cuando un usuario presiona la combinación de teclas Ctrl+Alt+Del. Con PLAP, la combinación de teclas Ctrl+Alt+Del abre una ventana en la que el usuario puede elegir iniciar sesión en el sistema o activar cualquier conexión de red (componentes PLAP) con el botón Network Connect en la esquina inferior derecha de la ventana.

Las secciones que siguen inmediatamente describen la configuración y los procedimientos para VPNGINA y PLAP SBL. Para obtener una descripción completa de la habilitación y el uso de la función SBL (PLAP) en una plataforma de Windows Vista, consulte Configuración de Inicio antes de Inicio de Sesión (PLAP) en sistemas de Windows Vista.

Configuración XML para Habilitar SBL

El valor de elemento de UseStartBeforeLogon permite activar (true) o desactivar (false) esta característica. Si establece este valor en **true** en el perfil, el procesamiento adicional se produce como parte de la secuencia de inicio de sesión. Consulte la descripción de Inicio antes del inicio de sesión para obtener más información. Establezca el valor <UseStartBefore Logon> del archivo CiscoAnyConnect.xml en **true** para habilitar SBL:

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

Para inhabilitar SBL, establezca el mismo valor en **false**.

Para habilitar la función UserControablable, utilice esta instrucción cuando habilite SBL:

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

Cualquier configuración de usuario asociada a este atributo se almacena en otra parte.

Habilitar SBL

Para minimizar el tiempo de descarga, el cliente AnyConnect solicita descargas (desde el dispositivo de seguridad) sólo de los módulos principales que necesita para cada función que soporta. Para habilitar nuevas funciones, como SBL, debe especificar el nombre del módulo con el comando **svc module** desde el modo de configuración de WebVPN de política de grupo o del nombre de usuario WebVPN:

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

El valor de cadena para SBL es **vpngina**.

En este ejemplo, el administrador de red ingresa en el modo de atributos de política de grupo para los teletrabajadores de políticas de grupo; ingresa en el modo de configuración de WebVPN para la política de grupo; y especifica la cadena VPNGINA para habilitar SBL:

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

Además, el administrador debe asegurarse de que el archivo <profile.xml> de AnyConnect, donde <profile.xml> es el nombre que el administrador de red ha asignado al archivo XML, tenga la instrucción <UseStartBeforeLogon> establecida en **true**, por ejemplo:

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

El sistema debe reiniciarse antes de que se inicie el inicio de sesión. También debe especificar en el dispositivo de seguridad que desea permitir SBL o cualquier otro módulo para funciones adicionales. Refiérase a la descripción de la sección Habilitación de Módulos para Funciones Adicionales de AnyConnect, página 2-5 (ASDM) o Habilitación de Módulos para Funciones Adicionales de AnyConnect, página 3-4 (CLI) para obtener más información.

Inicio de la configuración antes de iniciar sesión con CLI

Este escenario muestra cómo configurar el archivo XML con CLI:

1. Cree un perfil que se enviará a los PC clientes que tengan un aspecto similar al siguiente:
```
<?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. Copie el archivo en la memoria Flash del dispositivo de seguridad:
```
Copy tftp://x.x.x.x/AnyConnectProfile.xml AnyConnectProfile.xml
```
3. En el dispositivo de seguridad, agregue el perfil como un perfil disponible a la sección global de WebVPN, siempre y cuando todo lo demás esté configurado correctamente para las conexiones de AnyConnect:
```
hostname(config-group-policy)# webvpn
```

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

4. Edite la política de grupo que utilice y agregue los comandos **svc module** y **svc profile**:

```
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
```

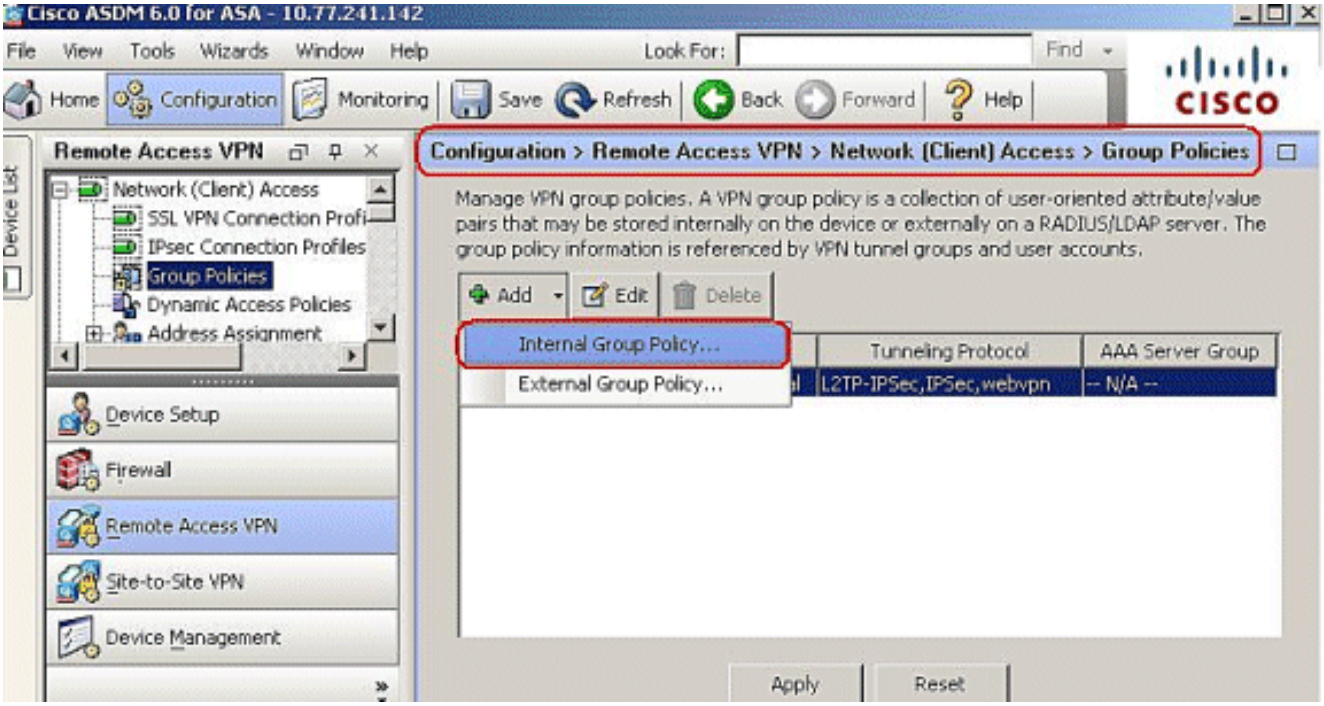
Inicio antes de la configuración de inicio de sesión con ASDM

Complete estos pasos para configurar SBL con ASDM:

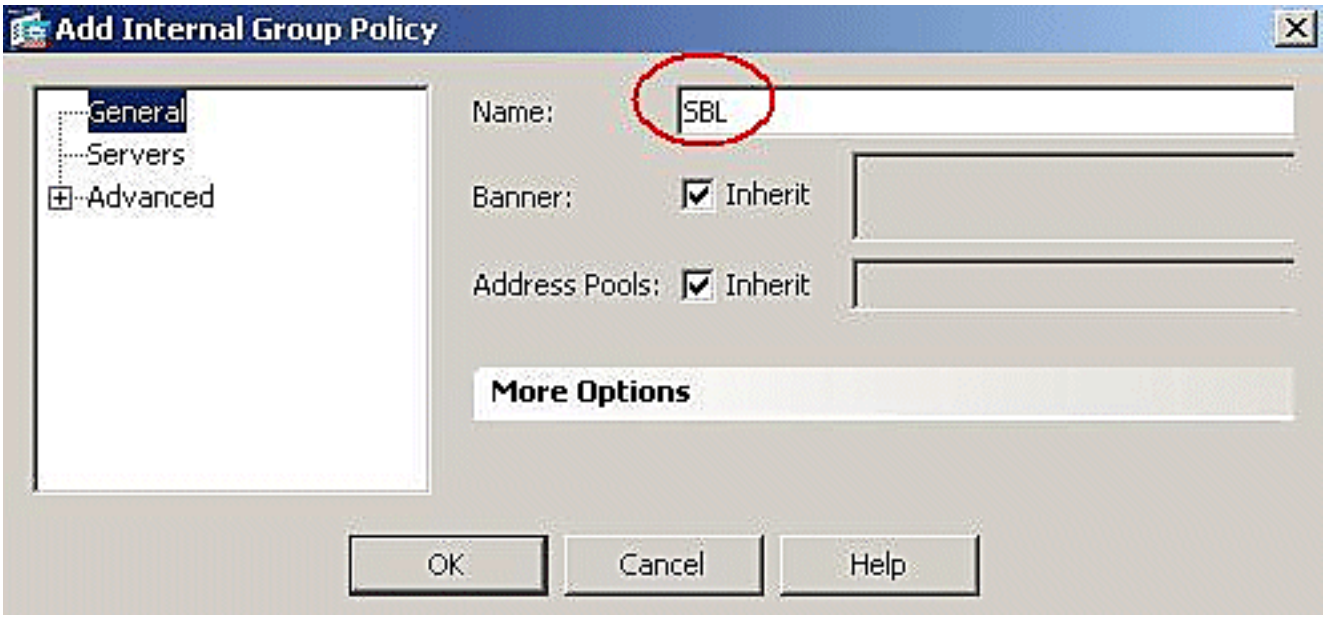
1. Cree un perfil que se enviará a los PC clientes que tengan un aspecto similar al siguiente:

```
<?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>
```

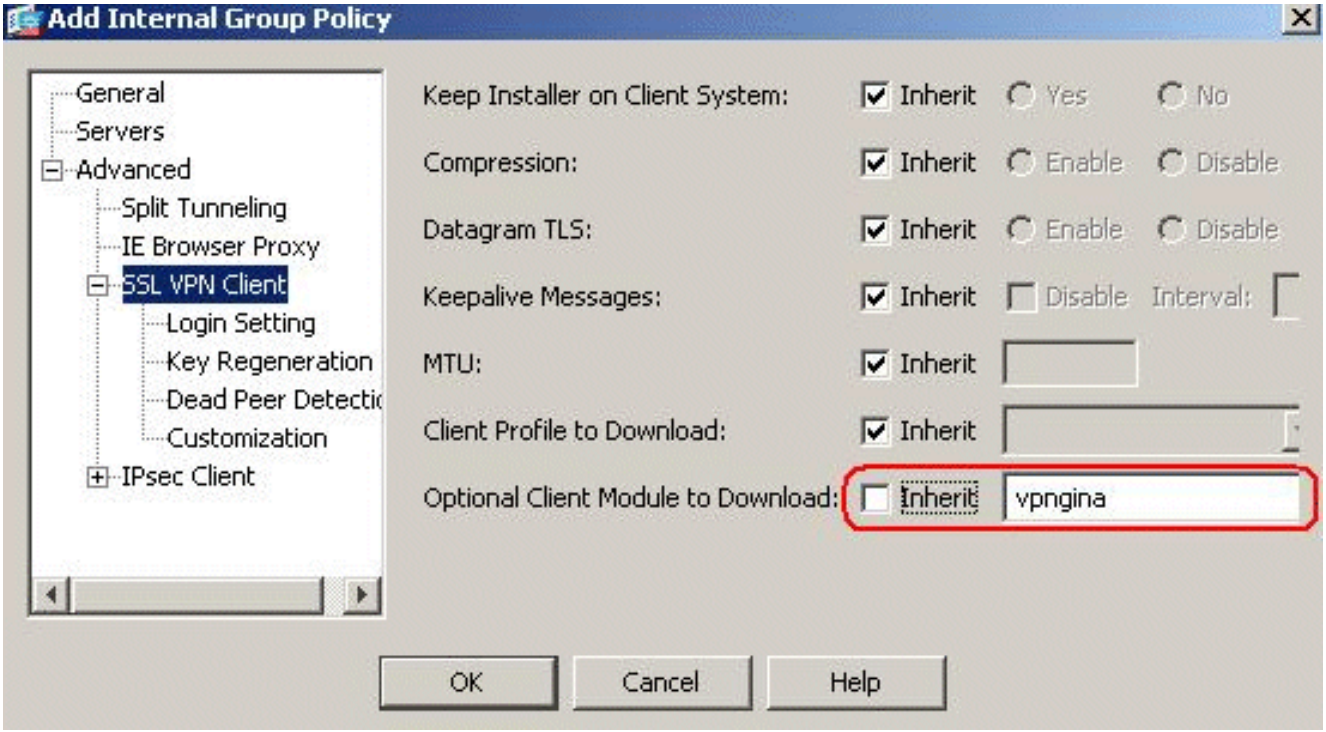
2. Guarde el perfil como **AnyConnectProfile.xml** en el equipo local.
3. Inicie el ASDM y vaya a la página de inicio.
4. Vaya a **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add** , y haga clic en la **Internal Group Policy**.



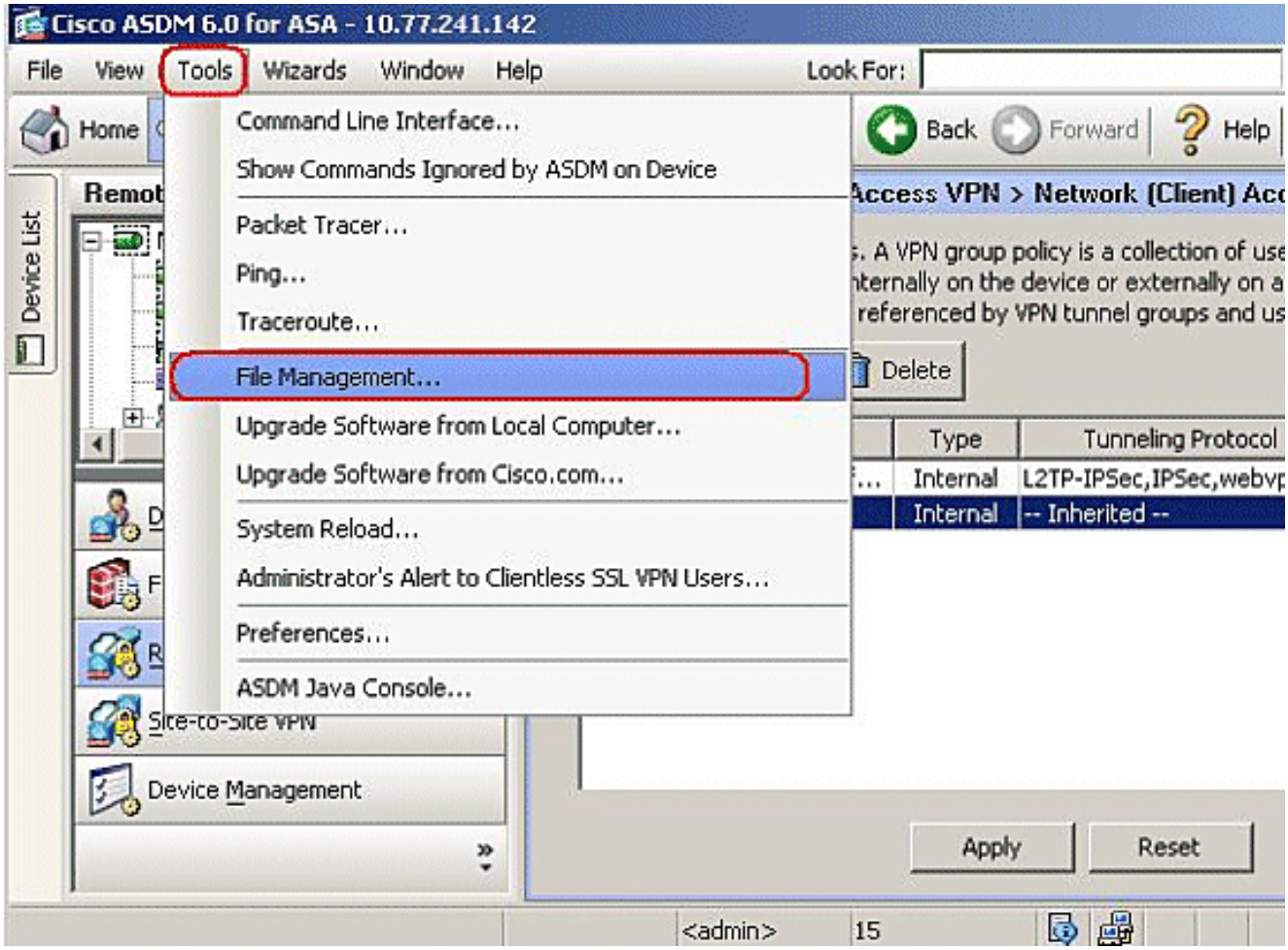
5. Introduzca el nombre de la política de grupo; por ejemplo, **SBL**.



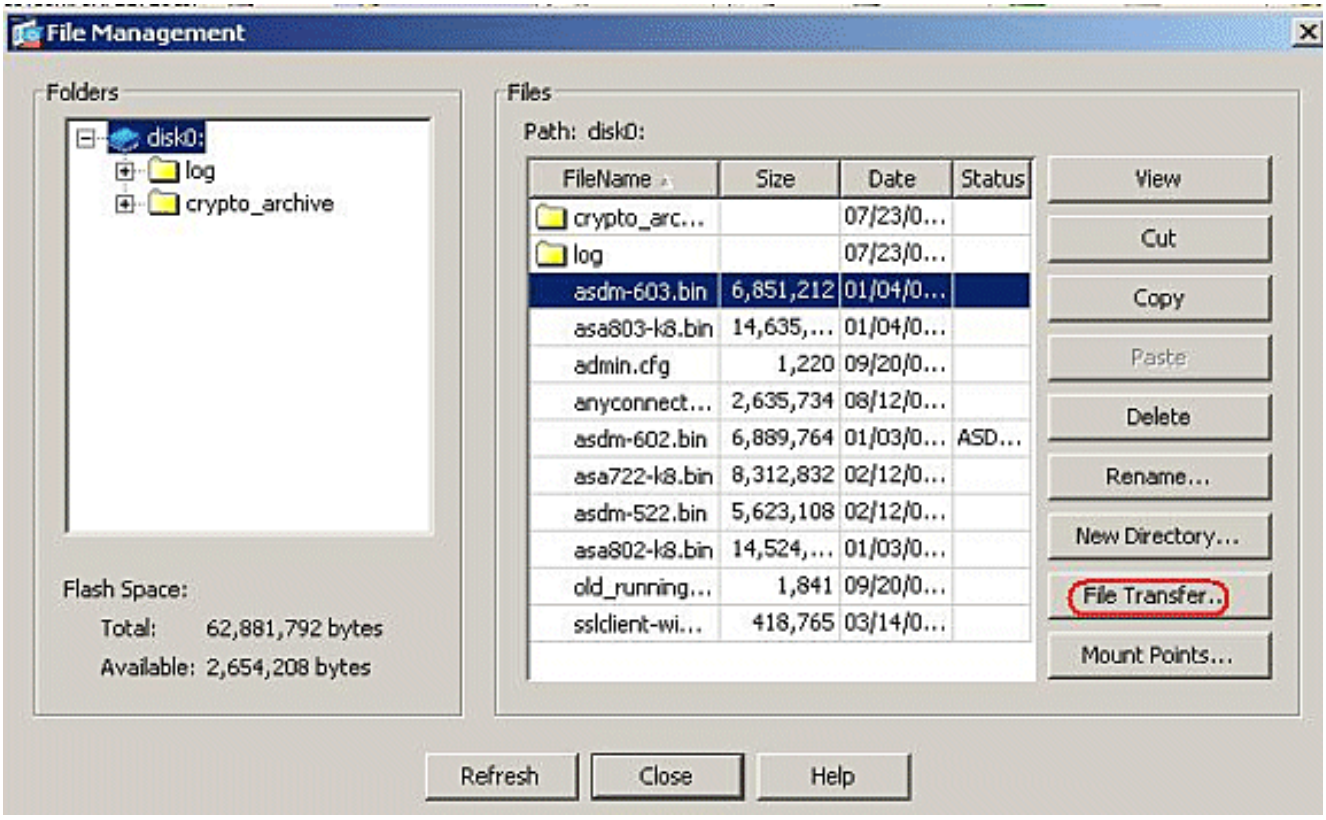
6. Vaya a **Advanced > SSL VPN Client**. Quite la marca de verificación Heredar en el **Módulo cliente opcional para descargar** y elija **vpngina** en el cuadro desplegable.



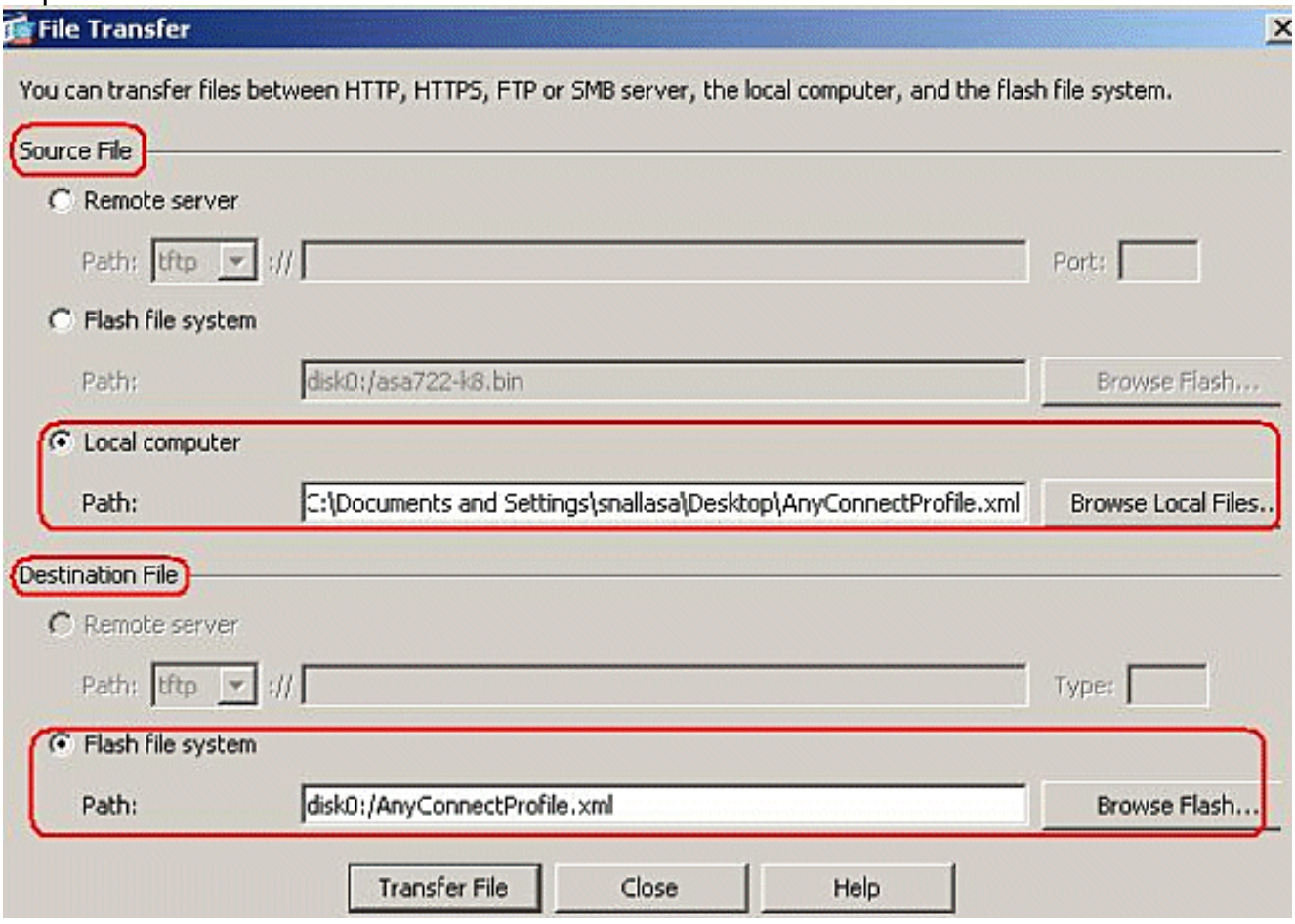
7. Para transferir el perfil **AnyConnectProfile.xml** del equipo local a Flash, vaya a **Herramientas** y haga clic en **Administración de archivos**.



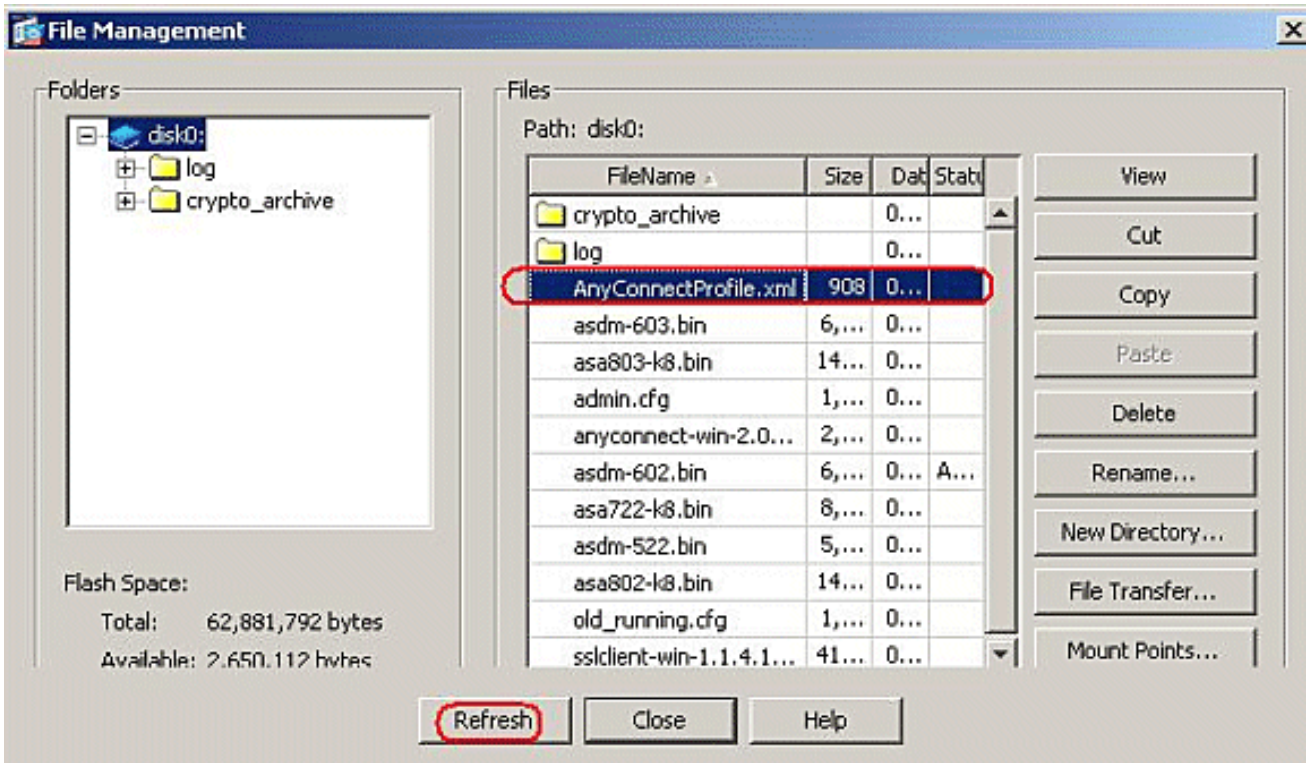
8. Haga clic en el botón **Transferencia de archivos**.



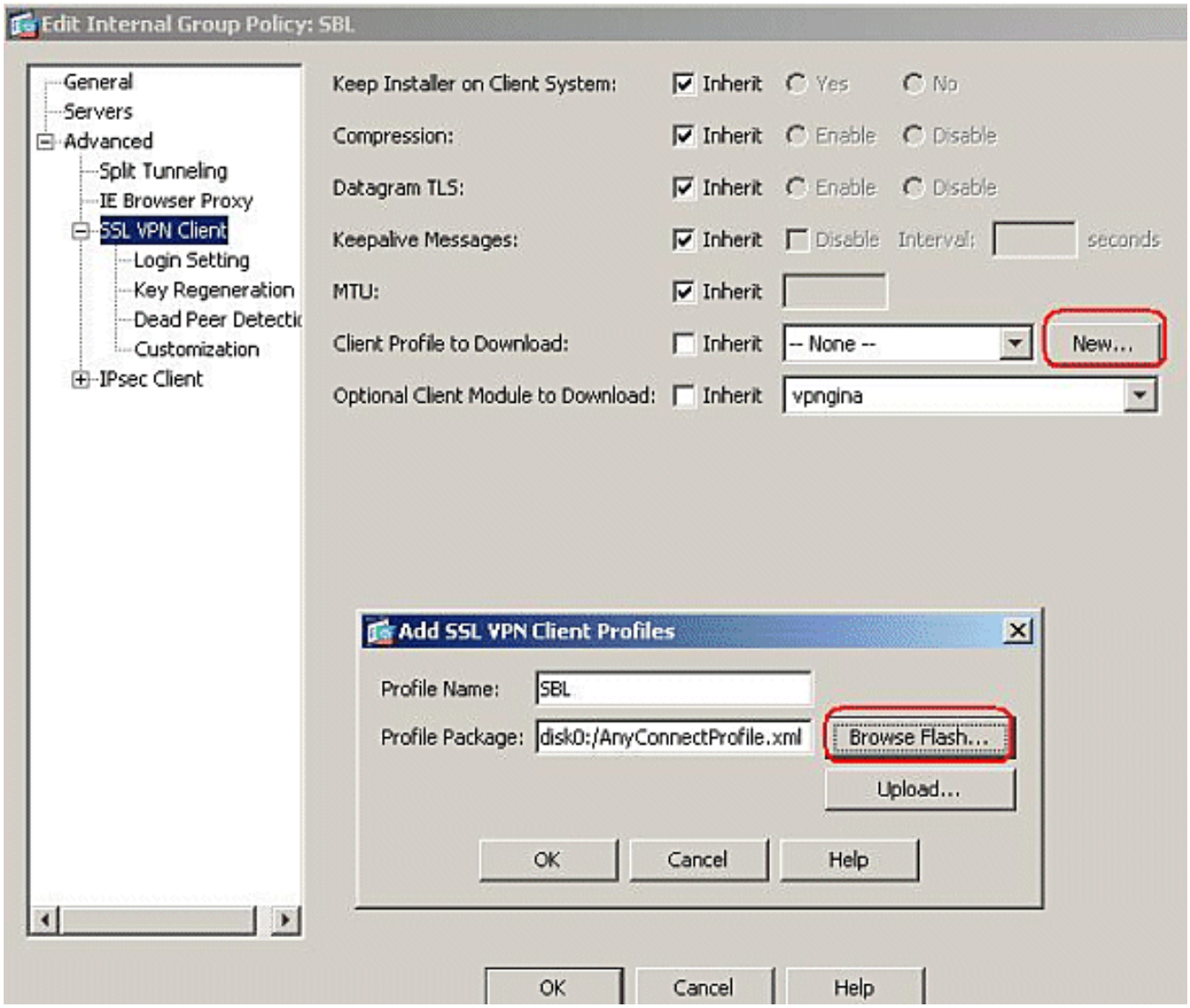
9. Para transferir el perfil desde el equipo local a la memoria Flash ASA, elija el **archivo de origen**, la ruta del archivo XML (equipo local) y la **ruta de acceso del archivo de destino** según sus
requerimientos.



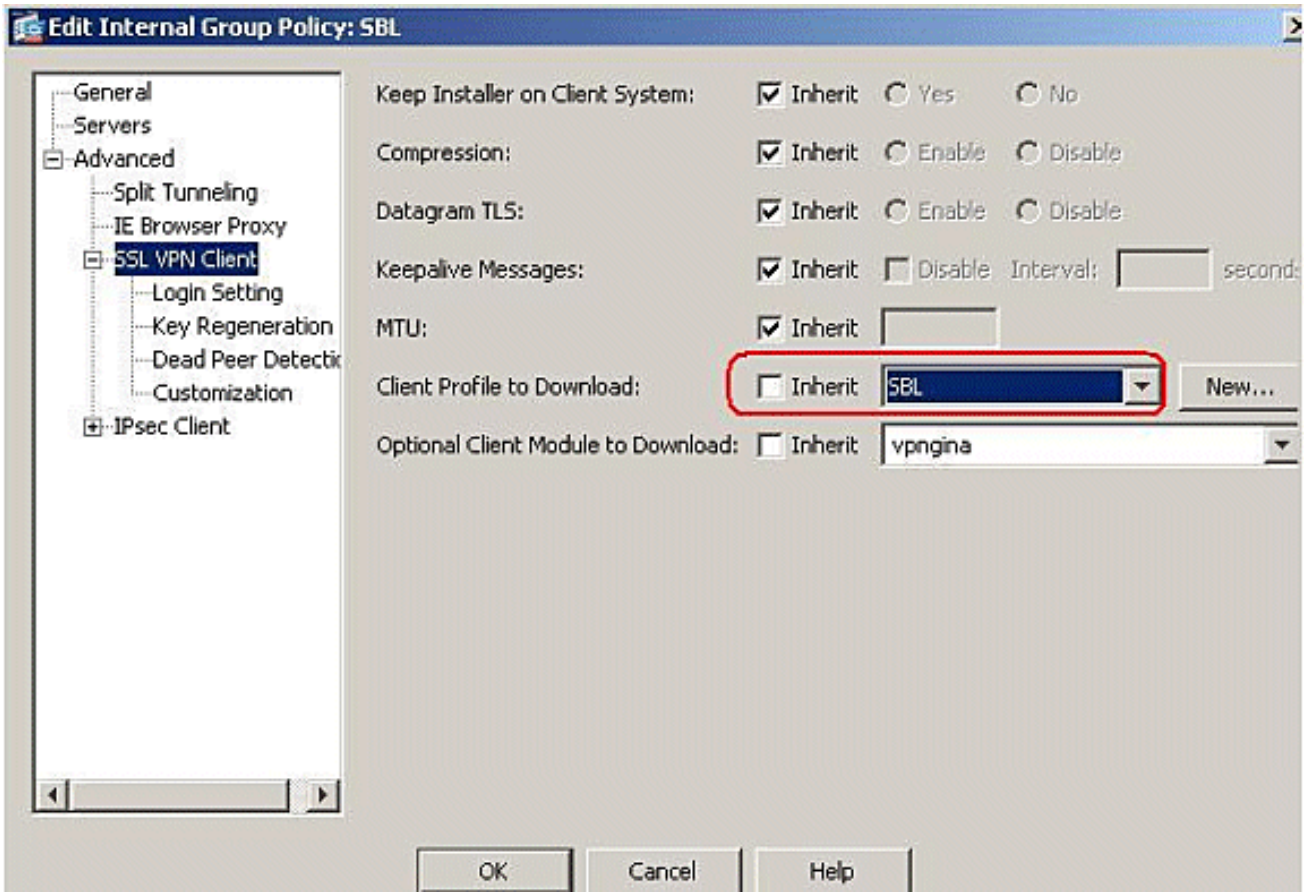
10. Después de la transferencia, haga clic en el botón **Refresh** para verificar si el archivo de perfil está en la memoria
Flash.



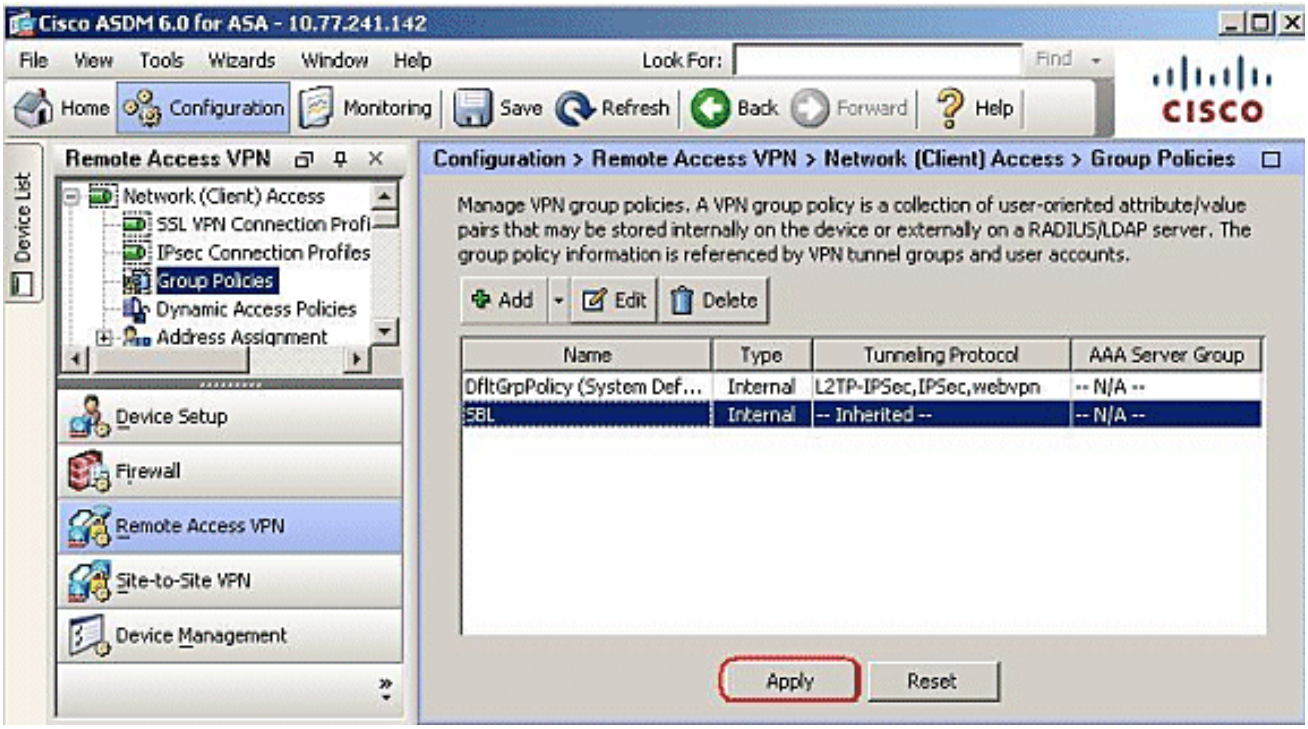
11. Asigne el perfil a la política de grupo interna (**SBL**).Siga esta ruta, **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Edit SBL (Internal Group Policy) > Advanced > SSL VPN Client > Client Profile to Download**, y haga clic en el botón **New**.En **Add SSL VPN Client Profiles**, haga clic en el botón **Browse** para elegir la ubicación del perfil (**AnyConnectProfile.xml**) almacenado en la memoria Flash ASA. Asigne el **Nombre** para el perfil, por ejemplo, **SBL**. Haga clic en **Aceptar** para completarlo.



12. Quite la casilla de verificación Heredar y elija **SBL** en el **campo Perfil de cliente para descargar**. Click
OK.



13. Haga clic en **Aplicar** para finalizar.



Utilizar el archivo Manifest

El paquete de AnyConnect que se carga en el dispositivo de seguridad contiene un archivo llamado VPNManifest.xml. Este ejemplo muestra un contenido de ejemplo de este archivo:

```
<?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>
```

El dispositivo de seguridad ha almacenado en él los perfiles configurados, como se explica en el paso 1, y también almacena uno o varios paquetes AnyConnect que contienen el propio cliente AnyConnect, la utilidad del descargador, el archivo de manifiesto y cualquier otro módulo opcional o archivos de soporte.

Cuando un usuario remoto se conecta al dispositivo de seguridad con WebLaunch o con un cliente independiente actual, el descargador se descarga primero y se ejecuta. Utiliza el archivo de manifiesto para determinar si hay un cliente actual en el equipo del usuario remoto que debe actualizarse o si se requiere una instalación nueva. El archivo de manifiesto también contiene información sobre si hay algún módulo opcional que se debe descargar e instalar, en este caso, el VPNGINA. El perfil del cliente también se envía desde el dispositivo de seguridad. La instalación de VPNGINA se activa mediante el comando **svc module value vpngina** configurado en el **modo de comando group-policy (webvpn)** como se explica en el Paso 4. Se instalan el cliente AnyConnect y VPNGINA, y el usuario ve el cliente AnyConnect en el siguiente reinicio, antes del inicio de sesión en Windows Domain.

Cuando el usuario se conecta, el cliente y el perfil se transmiten al equipo del usuario; el cliente y VPNGINA están instalados; y el usuario ve el cliente AnyConnect en el siguiente reinicio, antes del inicio de sesión.

Se proporciona un perfil de ejemplo en el equipo cliente cuando se instala AnyConnect: **C:\Documents and Settings\All Users\Application Data\Cisco\Cisco\AnyConnect VPN Client\Profile\AnyConnectProfile**.

Troubleshooting de SBL

Utilice este procedimiento si encuentra un problema con SBL:

1. Asegúrese de que el perfil está presionado.
2. Eliminar perfiles anteriores; busque en el disco duro para encontrar la ubicación: *.xml.
3. Cuando vaya a los programas Add/Remove, ¿dispone de una instalación AnyConnect y de AnyConnect VPNGINA?
4. Desinstale el cliente AnyConnect.
5. Borre el registro de AnyConnect del usuario en el Visor de eventos y vuelva a probar.
6. La Web vuelve al dispositivo de seguridad para reinstalar el cliente.
7. Asegúrese de que el perfil también aparezca.
8. Reinicie una vez. En el siguiente reinicio, se le solicitará el mensaje Start Before Logon (Iniciar antes de iniciar sesión).
9. Envíe el registro de eventos de AnyConnect a Cisco en formato .evt .
10. Si ve este error, elimine el perfil de usuario y utilice el perfil predeterminado:

```
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.
```

Problema 1

Este mensaje de error aparece al intentar cargar el perfil de AnyConnect: `Error al validar el archivo XML con el esquema más reciente.` ¿Cómo se resuelve este error?

Solución 1

Este mensaje de error se produce principalmente debido a problemas de sintaxis o configuración en el perfil de AnyConnect. Para resolver este problema, asegúrese de que el perfil de AnyConnect configurado sea similar al perfil de AnyConnect de ejemplo presente en la sección Perfil de AnyConnect y Esquema XML de ejemplo de la Guía del Administrador de Cisco AnyConnect VPN Client.

Información Relacionada

- Guía del administrador de Cisco AnyConnect VPN Client, versión 2.0
- Creación de scripts de inicio de sesión: Windows TechNet
- Configuración de Start Before Logon (PLAP) en sistemas Windows Vista
- Ejemplo de Configuración de ASA 8.x VPN Access con AnyConnect SSL VPN Client
- Cisco AnyConnect VPN Client
- Cisco ASA 5500 Series Adaptive Security Appliances
- Soporte Técnico y Documentación - Cisco Systems