# ASA 8.X: Comienzo de AnyConnect antes de la configuración de la característica del inicio

## Contenido



## Introducción

Con el *comienzo antes del inicio* (SBL) habilitó, el usuario ve el diálogo de inicio de AnyConnect GUI antes de que aparezca el cuadro de diálogo del inicio del ® 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 más información sobre configurar las características del cliente VPN de AnyConnect, refiera a la sección que configura las funciones de cliente de AnyConnect.

**Nota:** Dentro del cliente de AnyConnect, la única configuración que usted hace para SBL es habilitar la característica. Los administradores de la red manejan el proceso eso van encendido antes del inicio basado sobre los requisitos de su situación. Las secuencias de comandos de inicio se pueden asignar a un dominio o a los usuarios individuales. Generalmente, los administradores del dominio tienen los archivos por lote o similares definido con los usuarios o los grupos en el Active Directory. Tan pronto como el usuario abra una sesión, se ejecuta el script del login.

# prerrequisitos

## Requisitos

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.

- Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 esa versión de software 8.x del funcionamiento
- VPN versión 2.0 de Cisco AnyConnect

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Convenciones

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

# Antecedentes

La punta de SBL es que conecta una computadora remota con la infraestructura de la compañía antes del inicio con el PC. Por ejemplo, un usuario puede estar fuera de la red corporativa física, incapaz de acceder a los recursos corporativos hasta que su PC se haya unido a la red corporativa. Con SBL habilitado, el cliente de AnyConnect conecta antes de que el usuario vea la ventana del login de Microsoft. El usuario debe también iniciar sesión, como de costumbre, a Windows cuando aparece la ventana del login de Microsoft.

Éstas son varias razones para utilizar SBL:

- El PC del usuario se une a una infraestructura del Active Directory.
- El usuario no puede haber ocultado las credenciales en el PC, es decir, si la directiva del grupo rechaza las credenciales ocultadas.
- El usuario debe funcionar con los scripts del login que ejecutan de un recurso de red o que requieren el acceso a un recurso de red.
- Un usuario red-ha asociado las unidades que requieren la autenticación con la infraestructura del Active Directory.
- Los componentes de interconexión de redes, tales como NAC MS NAP/CS, pueden requerir la conexión a la infraestructura.

SBL crea una red que sea equivalente a la inclusión en el LAN corporativo local. Con SBL habilitado, puesto que el usuario tiene acceso a la infraestructura local, las secuencias de comandos de inicio que se ejecutan normalmente para un usuario en la oficina están también disponibles para el usuario remoto.

Para la información sobre cómo crear las secuencias de comandos de inicio, refiera a este artículo del TechNet de Microsoft .

Para la información sobre cómo utilizar las secuencias de comandos de inicio locales en Windows XP, refiera a este artículo de Microsoft .

En otro ejemplo, un sistema se puede configurar para rechazar las credenciales ocultadas para el inicio al PC. En este escenario, los usuarios deben poder comunicar con un controlador de dominio en la red corporativa para que sus credenciales sean validadas antes del acceso al PC. SBL requiere una conexión de red estar presente cuando se invoca. En algunos casos, esto no es posible porque una conexión de red inalámbrica puede depender de los credenciales de usuario para conectar con la infraestructura de red inalámbrica. Puesto que el modo SBL precede la fase credencial de un login, una conexión no está disponible en este escenario. En este caso, la conexión de red inalámbrica necesita ser configurada para ocultar las credenciales a través del login, u otra autenticación inalámbrica necesita ser configurada para que SBL trabaje.

## Instale el comienzo antes de los componentes del inicio (Windows solamente)

El comienzo antes de que los componentes del inicio deban ser instalados después de que el cliente de la base haya estado instalado. Además, el comienzo de AnyConnect 2.2 antes de que los componentes del inicio requieran esa versión 2.2, o más adelante, del software de cliente de AnyConnect de la base esté instalado. Si usted predespliega el cliente de AnyConnect y el comienzo antes de los componentes del inicio con los archivos MSI (por ejemplo, usted está en una compañía grande que tenga su propio despliegue del software (Altiris, Active Directory, o SMS), usted debe conseguir la derecha de la orden. La pedido de la instalación se maneja automáticamente cuando el administrador carga AnyConnect si es red desplegada y/o la red actualizada. Para la información de la instalación completa, refiera a los Release Note para el Cliente Cisco AnyConnect VPN, la versión 2.2.

### Las diferencias entre Windows Vista \ Windows 7 y PRE-Vista comienzan antes del inicio

Los procedimientos para habilitar SBL diferencian levemente en los sistemas de Windows Vista y de Windows 7. Los sistemas de PRE-Vista utilizan un componente llamado la identificación y la autenticación gráficas (VPNGINA) de la Red privada virtual para implementar SBL. Vista y Windows 7 sistemas utilizan un componente llamado PLAP para implementar SBL.

En el cliente de AnyConnect, el comienzo de Windows Vista antes de que la característica del inicio se conozca como el proveedor de acceso del PRE-login (PLAP), que es proveedor credencial conectable. Esta característica deja a los administradores de la red realizar las tareas específicas, tales como la colección de credenciales o de conexión a los recursos de red, antes del login. PLAP proporciona el comienzo antes de las funciones del inicio en Windows Vista, Windows 7 y el servidor de Windows 2008. PLAP soporta las versiones de 32 bits y 64-bit del sistema operativo con vpnplap.dll y vpnplap64.dll, respectivamente. La función PLAP soporta el x86 de Windows Vista y las versiones x64.

**Nota:** En esta sección, VPNGINA refiere al comienzo antes de la característica del inicio para las Plataformas de PRE-Vista, y PLAP refiere al comienzo antes de la característica del inicio para los sistemas de Windows Vista y de Windows 7.

En los sistemas de PRE-Vista, comience antes del inicio utiliza un componente conocido como la biblioteca con link dinámico gráfica de la identificación y de la autenticación VPN (vpngina.dll) para proporcionar el comienzo antes de las capacidades del inicio. El componente de Windows PLAP, que es parte de Windows Vista, substituye el componente de Windows GINA.

Activan A UNA GINA cuando un usuario presiona la combinación de claves Ctrl+Alt+Del. Con PLAP, la combinación de claves Ctrl+Alt+Del abre una ventana donde el usuario puede elegir iniciar sesión al sistema o activar cualquier conexión de red (componentes PLAP) con el botón connect de la red en la esquina inferior derecha de la ventana.

Las secciones que siguen inmediatamente describen las configuraciones y los procedimientos para VPNGINA y PLAP SBL. Para una descripción completa de la habilitación y el uso de la característica SBL (PLAP) en una plataforma de Windows Vista, refiera a configurar el comienzo antes del inicio (PLAP) en los sistemas de Windows Vista.

## Configuraciones XML para habilitar SBL

El valor del elemento para UseStartBeforeLogon permite que esta característica sea dada vuelta en (verdad) o apagado (falso). Si usted fija este valor **para verdad** en el perfil, el proceso adicional ocurre como parte de la secuencia del inicio. Vea el comienzo antes de la descripción del inicio para los detalles adicionales. Fije el valor de Logon> del <UseStartBefore en el archivo CiscoAnyConnect.xml al permiso SBL del trueto:

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

Para inhabilitar SBL, fije el mismo valor a **falso**.

Para habilitar la característica de UserControllable, utilice esta declaración cuando usted habilita SBL:

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

Cualquier ajustes de usuario asociado a este atributo se salva a otra parte.

## Permiso SBL

Para minimizar el tiempo de descarga, los pedidos de cliente de AnyConnect descargan (del dispositivo de seguridad) solamente de los módulos del núcleo eso que necesita para cada característica que soporte. Para habilitar las nuevas funciones, tales como SBL, usted debe especificar el nombre del módulo con los **módulos svc** ordena del WebVPN de la directiva del grupo o del modo de configuración del WebVPN del nombre de usuario:

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

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

En este ejemplo, el administrador de la red ingresa el modo de los atributos de la grupo-directiva para el telecommuters de la directiva del grupo; ingresa al modo de configuración del WebVPN para la directiva del 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 de AnyConnect <profile.xml>, donde está el nombre <profile.xml> que el administrador de la red ha asignado al archivo XML, tenga la declaración del <UseStartBeforeLogon> fijada para verdad, **por ejemplo**:

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

El sistema debe ser reiniciado antes de que el comienzo antes del inicio tome el efecto. Usted debe también especificar en el dispositivo de seguridad que usted quiere permitir SBL, o cualquier otro módulo para las características adicionales. Refiera a la descripción en los módulos que habilitan para las características adicionales de AnyConnect, pagine la sección 2-5 (del ASDM) o habilitando los módulos para las características adicionales de AnyConnect, pagine 3-4 (CLI) para más información.

## Comience antes de la configuración del inicio con el CLI

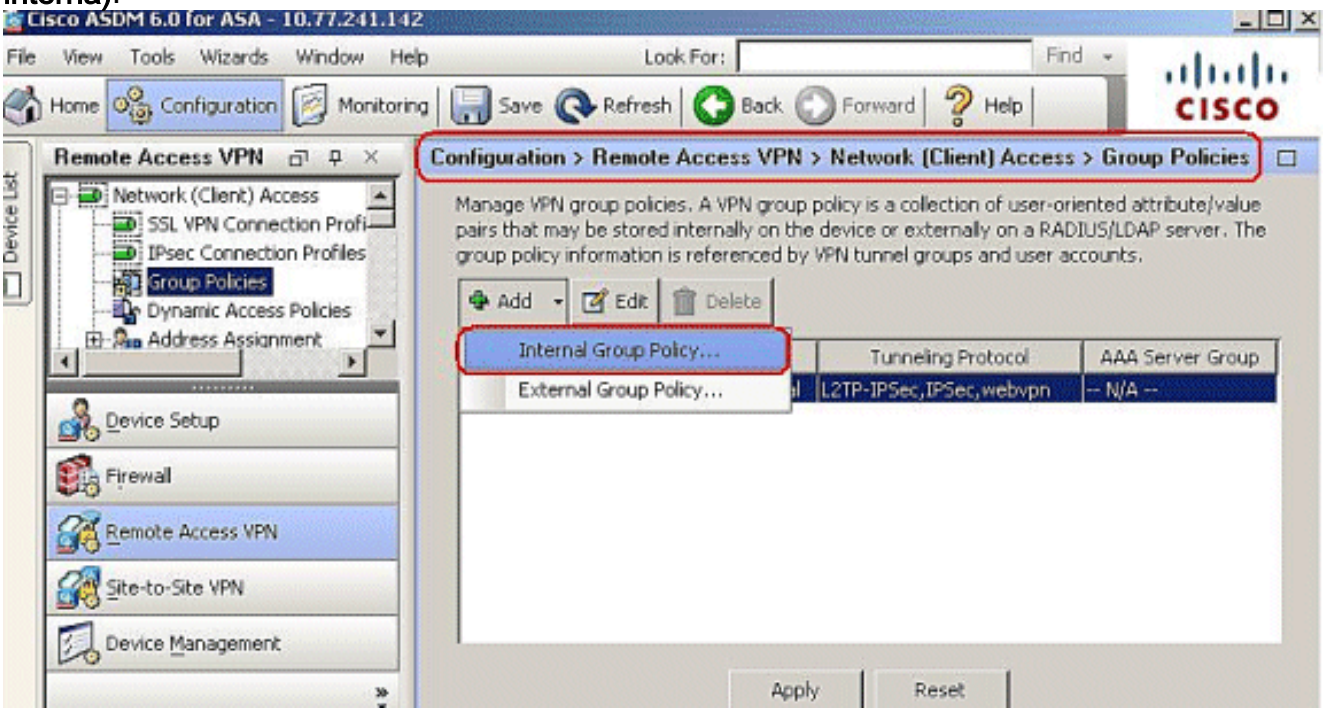
Este escenario le muestra cómo configurar el archivo XML con el CLI:

1. Cree un perfil que se empujará hacia abajo al cliente PC que parece similar a esto:
```
<?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 al Flash en el dispositivo de seguridad:
```
Copy tftp://x.x.x.x/AnyConnectProfile.xml AnyConnectProfile.xml
```
3. En el dispositivo de seguridad, agregue el perfil como perfil disponible a la sección global del WebVPN, mientras todo lo demás se configure correctamente para las conexiones de AnyConnect:
```
hostname(config-group-policy)# webvpn hostame(config-group-webvpn)# svc
profiles ReallyNewProfile disk0:/AnyConnectProfile.xml
```
4. Edite la directiva del grupo que usted uso, y agrega los **módulos svc** y los **comandos profile 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
```

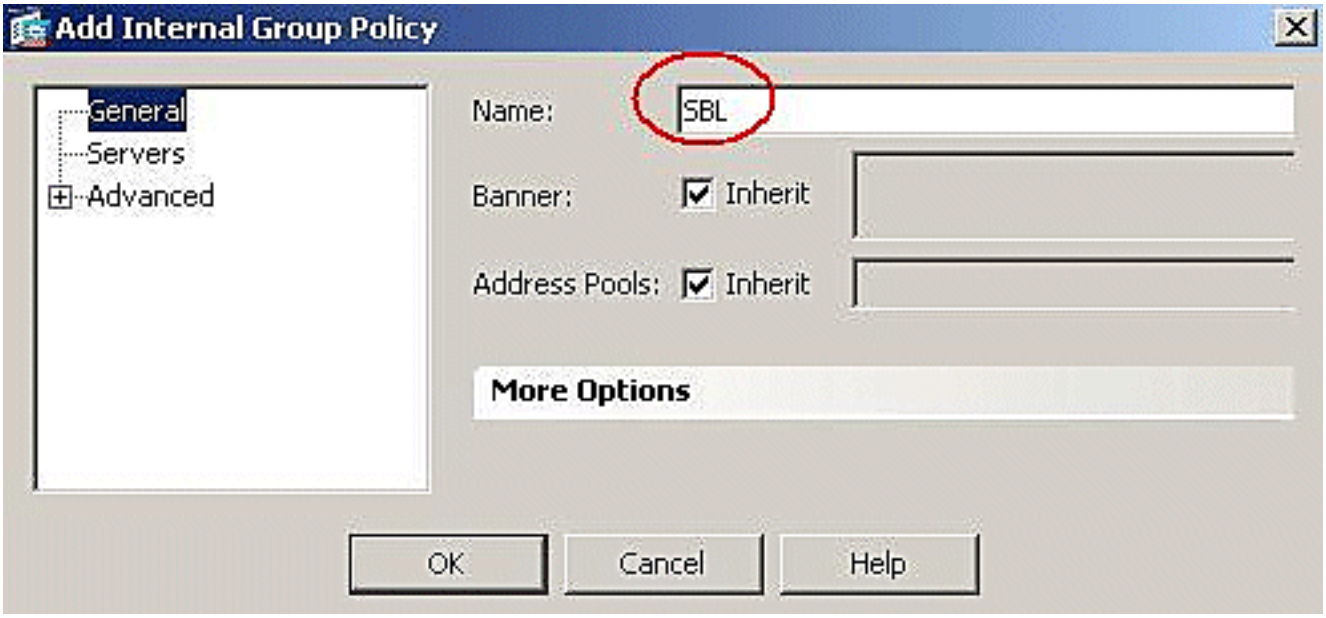
## Comience antes de la configuración del inicio con el ASDM

Complete estos pasos para configurar el SBL con el ASDM:

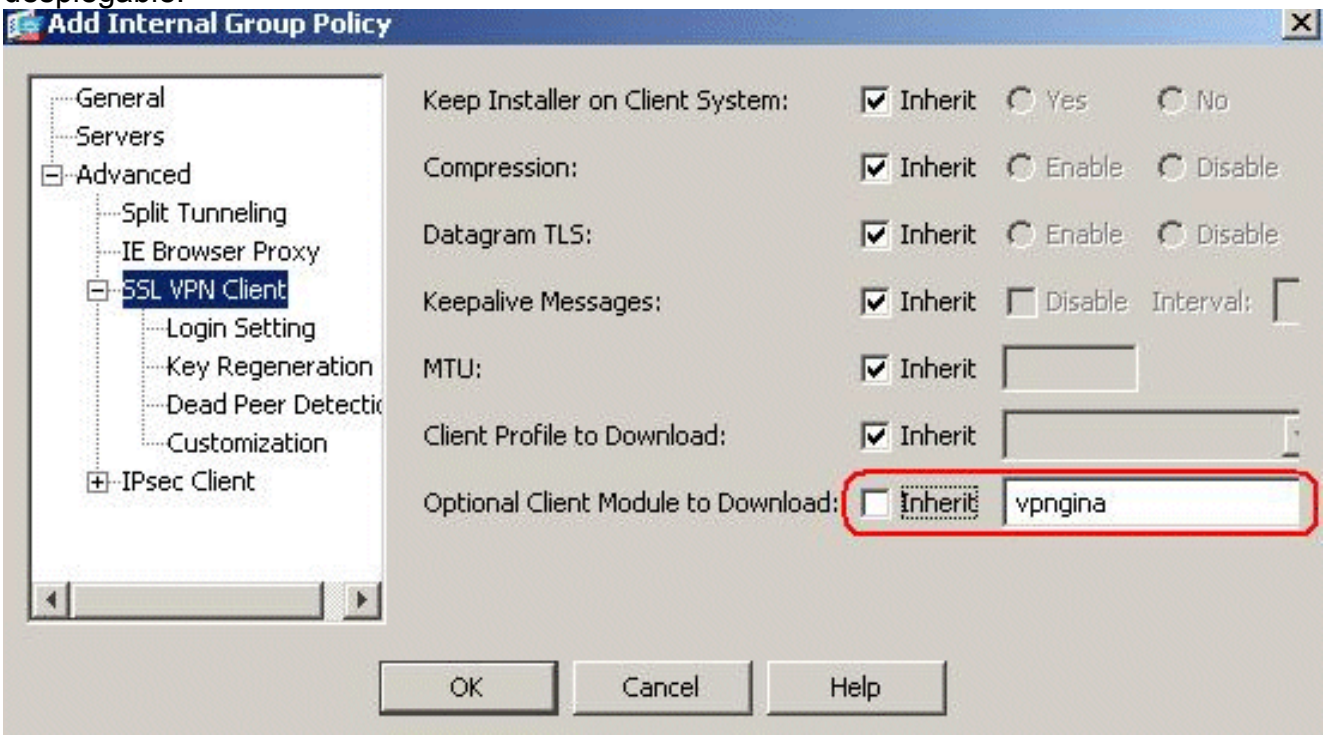
1. Cree un perfil que se empujará hacia abajo al cliente PC que parece similar a esto:
```
<?xml
version="1.0" encoding="UTF-8" ?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi :schemaLocation=
   "http://schemas.xmlsoap.org/encoding/ 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. Salve el perfil como **AnyConnectProfile.xml en la** computadora local.
3. Inicie el ASDM, y vaya al Home Page.
4. Van a la **configuración > al VPN de acceso remoto > las directivas al acceso > al grupo de la red (cliente) > Add**, y hacen clic el **Internal group policy (política grupal interna)**.



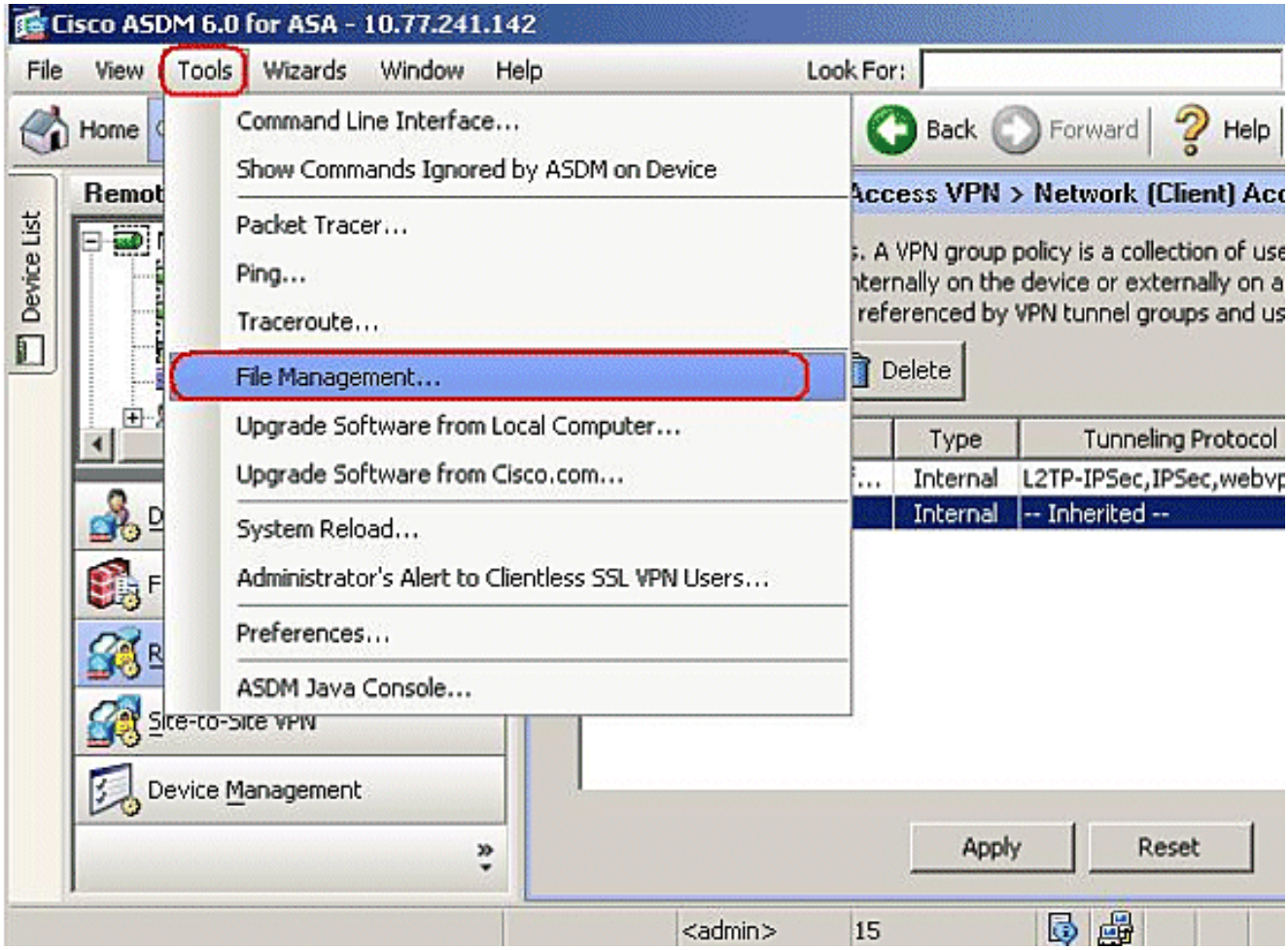

5. Ingrese el nombre de la directiva del grupo, por ejemplo, **SBL**.



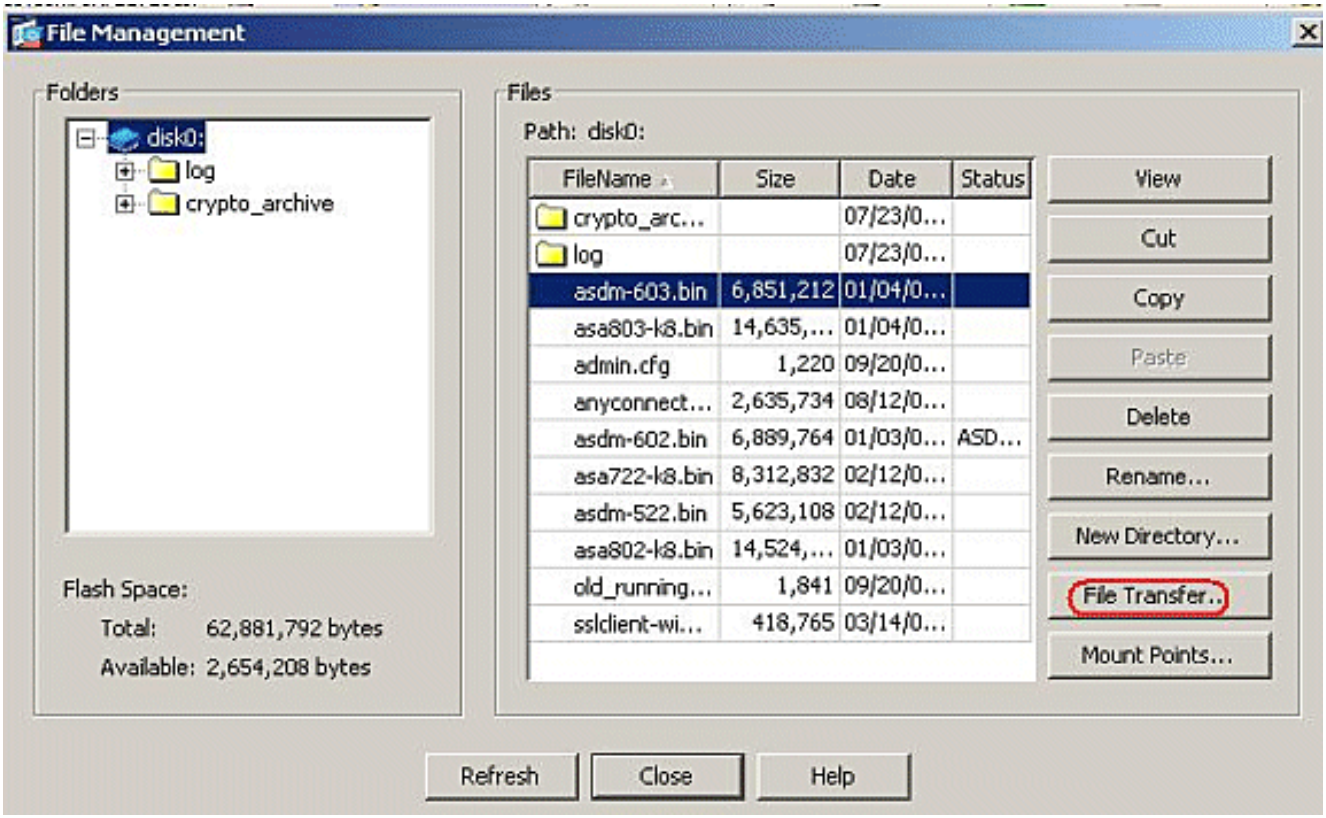

6. Va a **avanzado > el cliente VPN SSL**. Quite la marca de tilde de la herencia en el **módulo cliente opcional para descargar**, y elija el **vpngina de la** casilla desplegable.



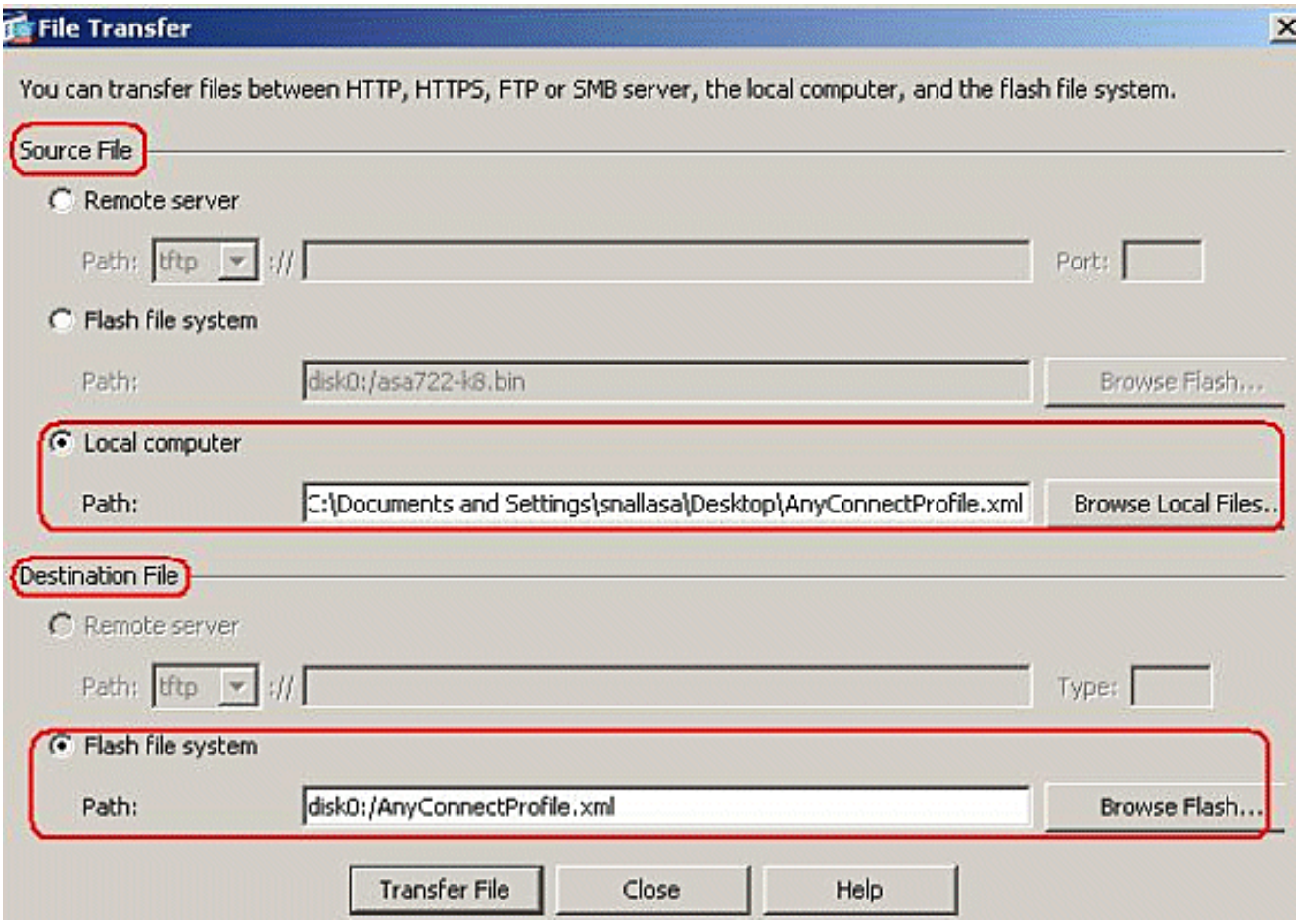

7. Para transferir el perfil **AnyConnectProfile.xml de la** computadora local para contellear, vaya a las herramientas**, y** haga clic FileManagement**.**



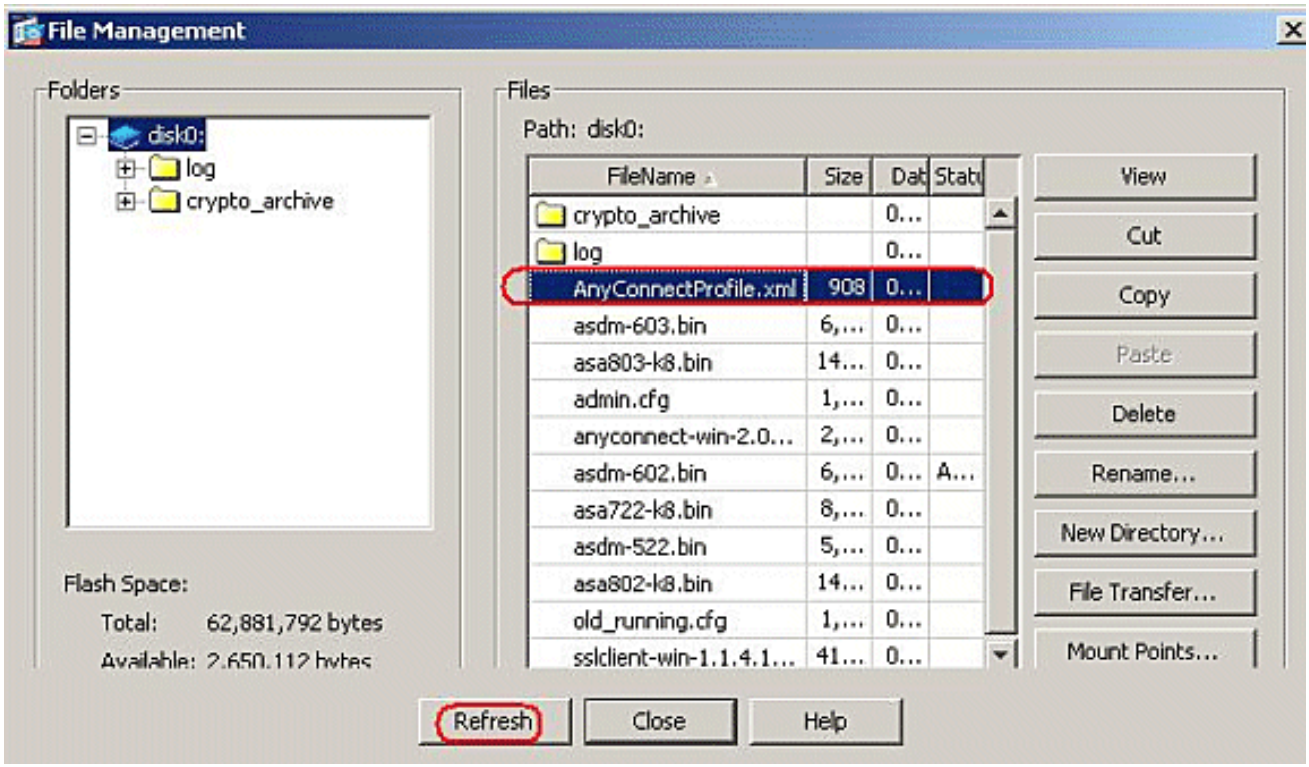

8. Haga clic el botón de la **transferencia de archivos**.




9. Para transferir el perfil de la computadora local a memoria flash ASA, elija el **archivo de origen**, la trayectoria del archivo XML (computadora local), y la trayectoria del **archivo de destino** según su
requisito.

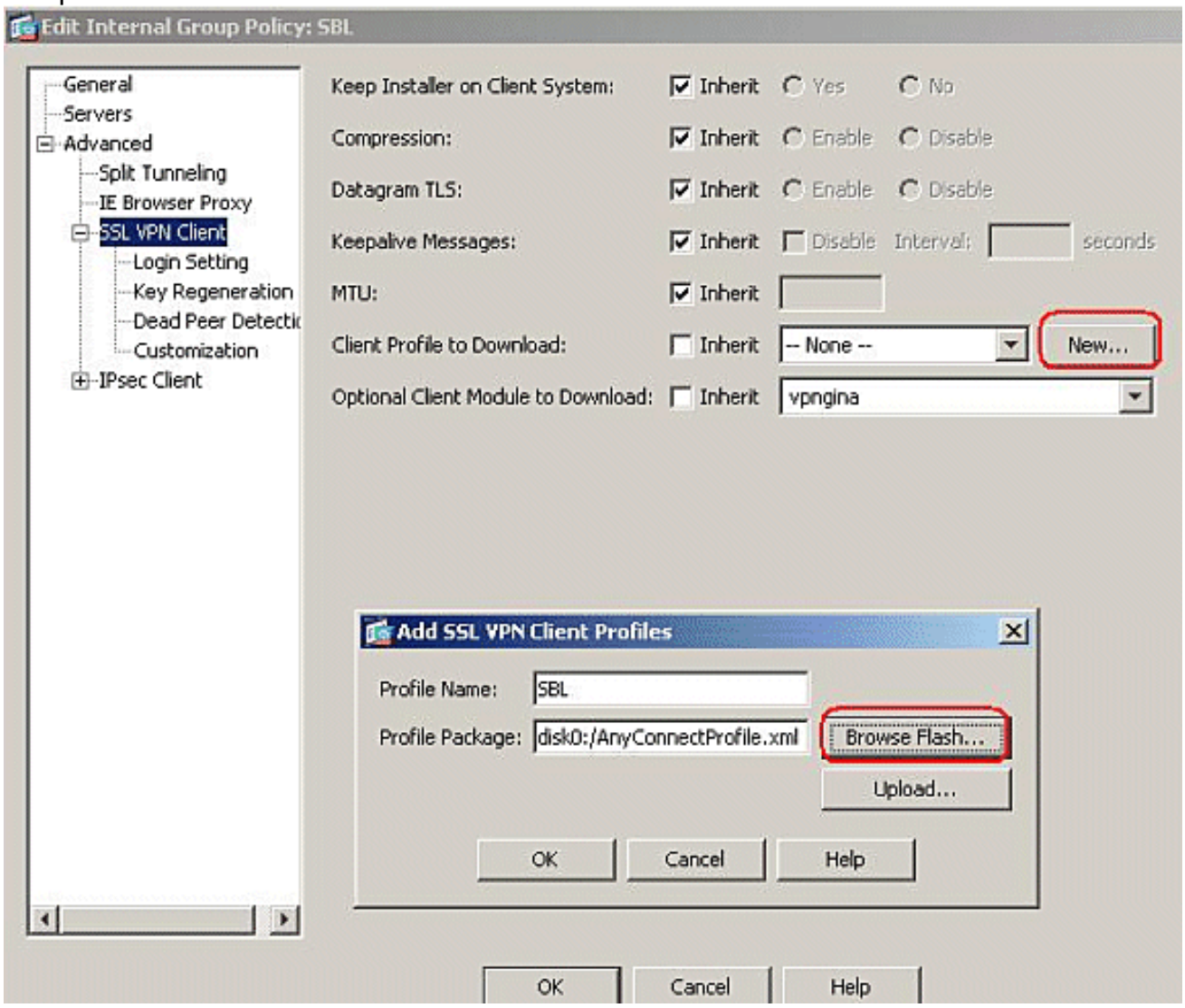



10. Después de que la transferencia, haga clic el **botón Refresh Button** para verificar si el archivo de perfil está en memoria flash.

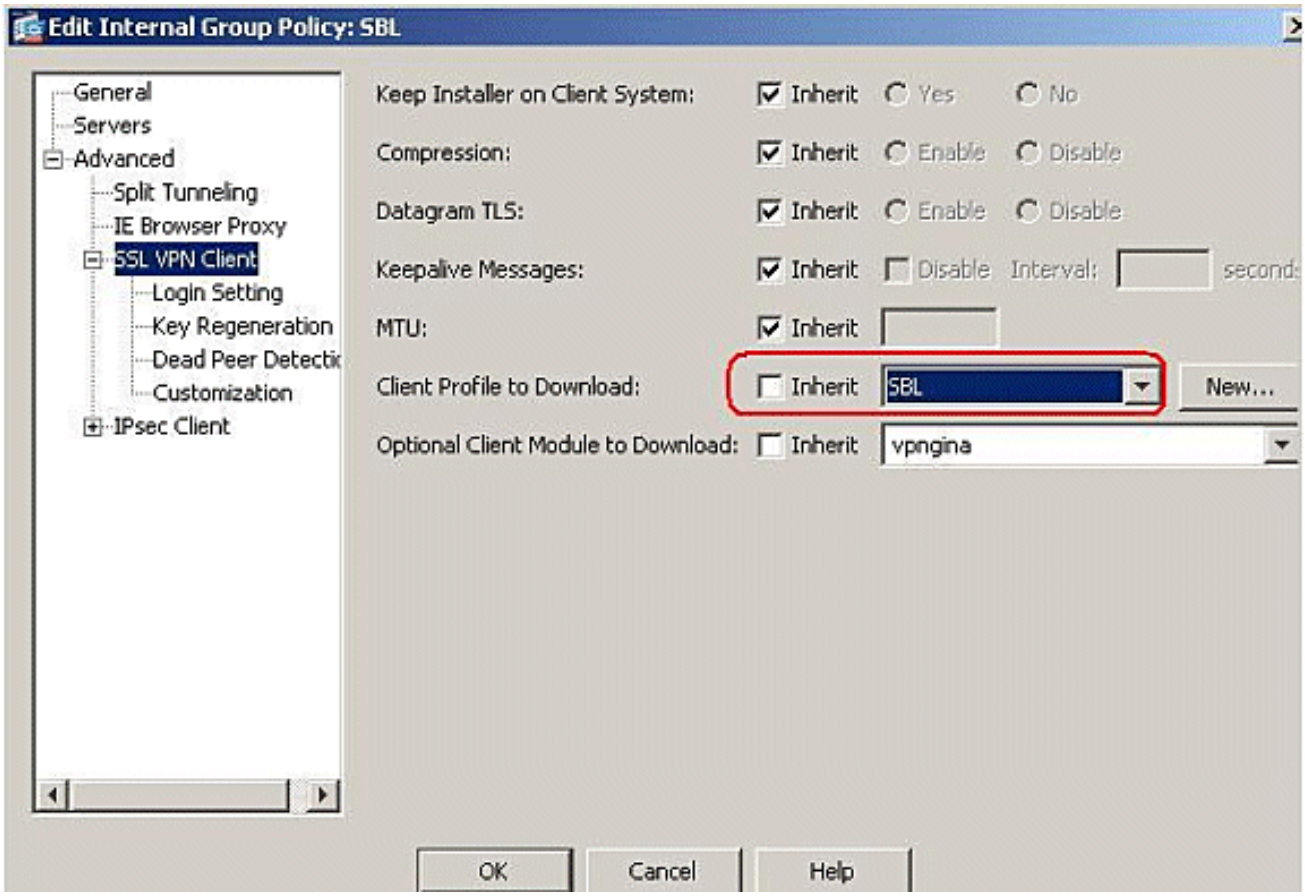



11. Asigne el perfil a la directiva interna del grupo (**SBL**).Siga esta trayectoria, la **configuración > el VPN de acceso remoto > las directivas del acceso > del grupo de la red (cliente) > editan SBL (Internal group policy (política grupal interna)) > avanzaron > perfil del cliente VPN > del cliente SSL a descargar**, y hacen clic el **nuevo** botón.En los **perfiles del cliente VPN del agregar SSL**, haga clic el **botón Browse** para elegir la ubicación del

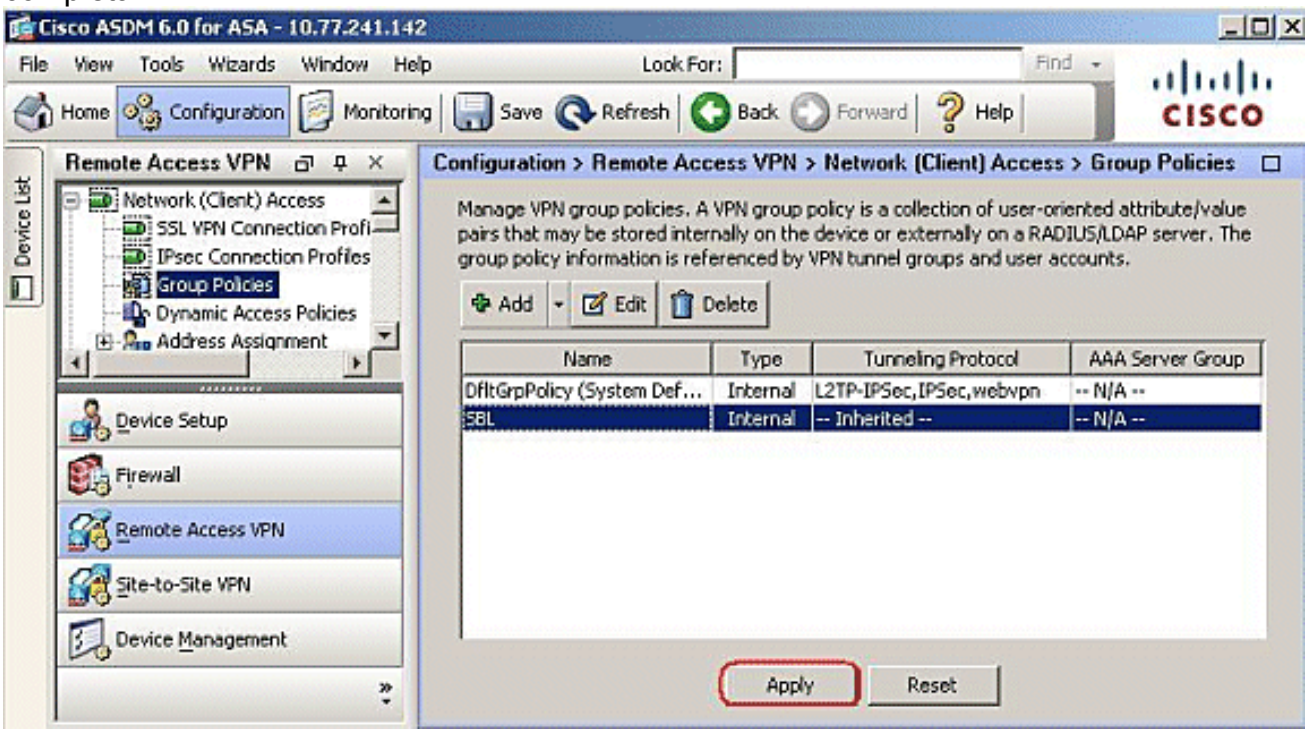
profile(AnyConnectProfile.xml) **salvada** en memoria flash ASA. Asigne a Namefor el perfil, por ejemplo, SBL**. El tecleo** OKTO
completa.




12. Quite la casilla de verificación de la herencia y elija **SBL** en el **perfil del cliente para descargar el** campo. Haga clic en
OK.




13. El tecleo **se aplica** para completar.




## Utilice el archivo de manifiesto

El paquete de AnyConnect que está cargado en el dispositivo de seguridad contiene un archivo llamado VPNManifest.xml. Este ejemplo muestra un contenido de la muestra 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 salvado en él configuró los perfiles, como se explica en el paso 1, y también salva uno o los paquetes múltiples de AnyConnect que contengan al cliente sí mismo de AnyConnect, utilidad del descargador, archivo de manifiesto, y cualesquiera otros módulos opcionales o archivo del soporte.

Cuando un usuario remoto conecta con el dispositivo de seguridad con WebLaunch o un cliente independiente actual, el descargador se descarga primero y funcionamiento. Utiliza el archivo de manifiesto para comprobar si hay un cliente actual en el usuario remoto PC que necesita ser actualizado, o se requiere una instalación desde el inicio. El archivo de manifiesto también contiene la información sobre si hay algunos módulos opcionales que se deban descargar y instalar, en este caso, el VPNGINA. El perfil del cliente también se empuja hacia abajo del dispositivo de seguridad. La instalación de VPNGINA es activada por el **vpngina del valor de los módulos de** comando svc configurado bajo modo de comando de la grupo-**directiva (webvpn)** como se explica en el paso 4. El cliente de AnyConnect y los VPNGINA están instalados, y el usuario ve al cliente de AnyConnect en la reinicialización siguiente, antes del inicio del Dominio de Windows.

Cuando el usuario conecta, pasan el cliente y el perfil abajo al usuario PC; el cliente y los VPNGINA están instalados; y el usuario ve al cliente de AnyConnect en la reinicialización siguiente, antes del inicio.

Un ejemplo de perfil se proporciona en PC del cliente cuando AnyConnect está instalado: **Usuarios \ datos de aplicación \ Cisco \ Cisco de C:\Documents and Settings\All \ cliente VPN \ perfil \ AnyConnectProfile de AnyConnect**.

## Troubleshooting SBL

Utilice este procedimiento si usted encuentra un problema con SBL:

1. Asegúrese de que el perfil esté avanzado.
2. Borre los perfiles anteriores; busque para ellos en la unidad de disco duro para encontrar la ubicación: *.xml.
3. ¿Cuando usted va al agregar/quita los programas, usted tiene una instalación de AnyConnect e instalación de AnyConnect VPNGINA?
4. Desinstale al cliente de AnyConnect.
5. Borre el registro de AnyConnect del usuario en el visor de eventos y la contra-prueba.
6. La red hojea de nuevo al dispositivo de seguridad para reinstalar al cliente.
7. Aseegurese que aparece el perfil también.
8. Reinicie una vez. En la reinicialización siguiente, le indican con el comienzo antes del mensaje de conexión a la comunicación.
9. Envíe el registro de acontecimientos de AnyConnect a Cisco en el formato .evt.
10. Si usted ve este error, borre el perfil del 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

Se considera este mensaje de error mientras que intenta cargar el perfil de AnyConnect: `Error en validar el archivo XML contra el último esquema.` ¿Cómo se resuelve este error?

## Solución 1

Este mensaje de error ocurre sobre todo debido al sintaxis o a los problemas de configuración en el perfil de AnyConnect. Para resolver este problema, aseegurese que el perfil de AnyConnect configurado es similar al perfil de AnyConnect de la muestra presente en la sección del perfil y del esquema XML de AnyConnect de la muestra del guía del administrador del Cliente Cisco AnyConnect VPN.

# Información Relacionada

- Guía del administrador del Cliente Cisco AnyConnect VPN, versión 2.0
- Creando las secuencias de comandos de inicio - Windows TechNet
- Configurar el comienzo antes del inicio (PLAP) en los sistemas de Windows Vista
- Acceso ASA 8.x VPN con el ejemplo de configuración del cliente VPN de AnyConnect SSL
- Cisco AnyConnect VPN Client
- Cisco ASA 5500 Series Adaptive Security Appliances
- Soporte Técnico y Documentación - Cisco Systems