ASA 8.X: Ejemplo de configuración de la inscripción SCEP de AnyConnect

Contenido

Introducción

La funcionalidad de inscripción SCEP se introduce en el cliente independiente AnyConnect 2.4. En este proceso, usted modifica el perfil de AnyConnect XML para incluir una configuración SCEP-relacionada y para crear una directiva y un perfil de la conexión específicos del grupo para la inscripción del certificado. Cuando un usuario de AnyConnect conecta con este grupo específico, AnyConnect envía una petición de la inscripción del certificado al servidor de CA, y el servidor de CA valida o niega automáticamente la petición.

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 2.4 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 meta de la inscripción SCEP automática para AnyConnect es publicar un certificado al cliente de una manera segura y scalable. Por ejemplo, los usuarios no necesitan pedir un certificado de un servidor de CA. Estas funciones se integran en el cliente de AnyConnect. Los Certificados se publican a los clientes basados en los parámetros del certificado mencionados en el archivo de perfil XML.

Descripción de los cambios requeridos

La característica de la inscripción SCEP de AnyConnect requiere ciertos parámetros del certificado ser definida en el perfil XML. Una directiva y un perfil de la conexión del grupo se crea en el ASA para la inscripción del certificado, y el perfil XML se asocia a esa directiva. El cliente de AnyConnect conecta con el perfil de la conexión que utiliza esta directiva específica y envía una petición un certificado con los parámetros que se definen en el archivo XML. El Certificate Authority (CA) valida o niega automáticamente la petición. El cliente de AnyConnect extrae los Certificados con el protocolo SCEP si el elemento del <CertificateSCEP> se define en un perfil del cliente.

La autenticación del certificado del cliente debe fallar antes de que los intentos de AnyConnect para extraer automáticamente los nuevos Certificados, así que si usted tengan ya un certificado válido instalado, no ocurre la inscripción.

Cuando los usuarios inician sesión al grupo específico, los alistan automáticamente. Hay también un método manual disponible para la recuperación de certificados en la cual presentan los usuarios con un botón del **certificado del conseguir**. Esto trabaja solamente cuando el cliente tiene acceso directo al servidor de CA, no a través del túnel.

Refiera al guía del administrador del Cliente Cisco AnyConnect VPN, libere 2.4 para más información.

Configuraciones XML para habilitar la característica de Anyconnect SCEP

Éstos son los elementos importantes que necesitan ser definidos en el archivo XML de AnyConnect. Refiera al guía del administrador del Cliente Cisco AnyConnect VPN, libere 2.4 para más información.

- <AutomaticSCEPHost> — Especifica el nombre del host y el perfil de la conexión (grupo de

túnel) ASA para los cuales se configura la recuperación de certificados SCEP. El valor necesita estar en el formato del Nombre de dominio totalmente calificado (FQDN) del nombre ASA \ del perfil de la conexión o de la dirección IP del nombre ASA \ del perfil de la conexión.
- **<**CAURL**>** — Identifica el servidor SCEP CA.
- **<**CertificateSCEP**>** — Define cómo el contenido del certificado se pide.
- **<**DisplayGetCertButton**>** — Determina si el AnyConnect GUI visualiza el botón del certificado del conseguir. Permite a los usuarios para pedir manualmente el renewal o el aprovisionamiento del certificado.

Aquí está un perfil del ejemplo:

```
<?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 UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AutoConnectOnStart UserControllable="true">true</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">
     ReconnectAfterResume
   </AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">
    Automatic
  </RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Automatic
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<CertificateEnrollment>
<AutomaticSCEPHost>asa2.cisco.com/certenroll</AutomaticSCEPHost>
<CAURL PromptForChallengePW="false">
     http://10.11.11.1/certsrv/mscep/mscep.dll
   </CAURL>
<CertificateSCEP>
<Name_CN>cisco</Name_CN>
<Company_O>Cisco</Company_O>
<DisplayGetCertButton>true</DisplayGetCertButton>
</CertificateSCEP>
</CertificateEnrollment>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>asa2.cisco.com</HostName>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

Configure el ASA para soportar el protocolo SCEP para AnyConnect

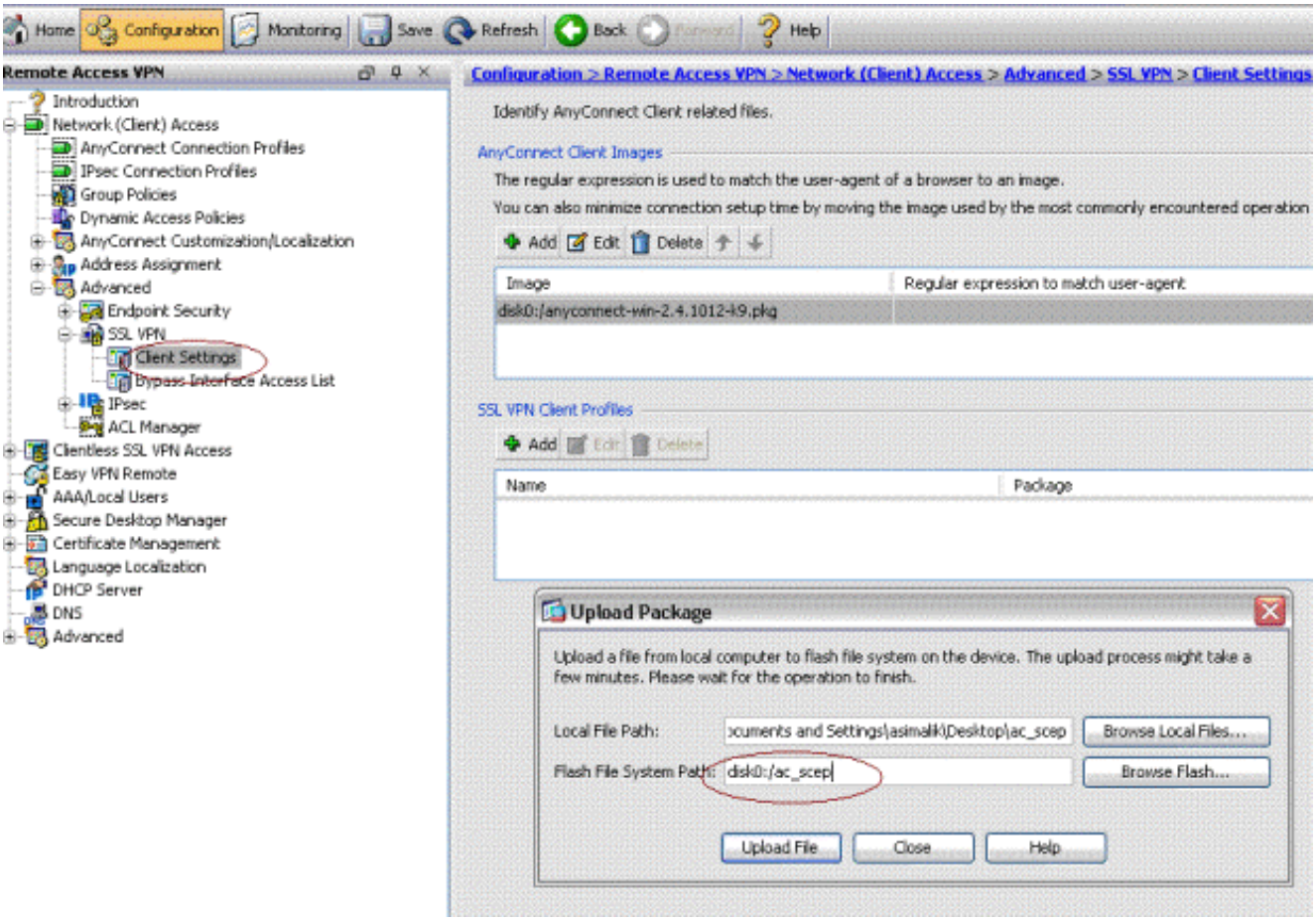
Para proporcionar el acceso a un registration authority (RA) privado, el administrador ASA debe crear un alias que tenga un ACL que restrinja la conectividad de red lateral del soldado al RA deseado. Para extraer automáticamente un certificado, los usuarios conectan y autentican a este alias.

Complete estos pasos:

1. Cree un alias en el ASA para señalar al grupo configurado específico.
2. Especifique el alias en el elemento del <AutomaticSCEPHost> en el perfil del cliente del usuario.
3. Asocie el perfil del cliente que contiene la sección del <CertificateEnrollment> al grupo configurado específico.
4. Fije un ACL para que el grupo configurado específico restrinja el tráfico al lado privado RA.

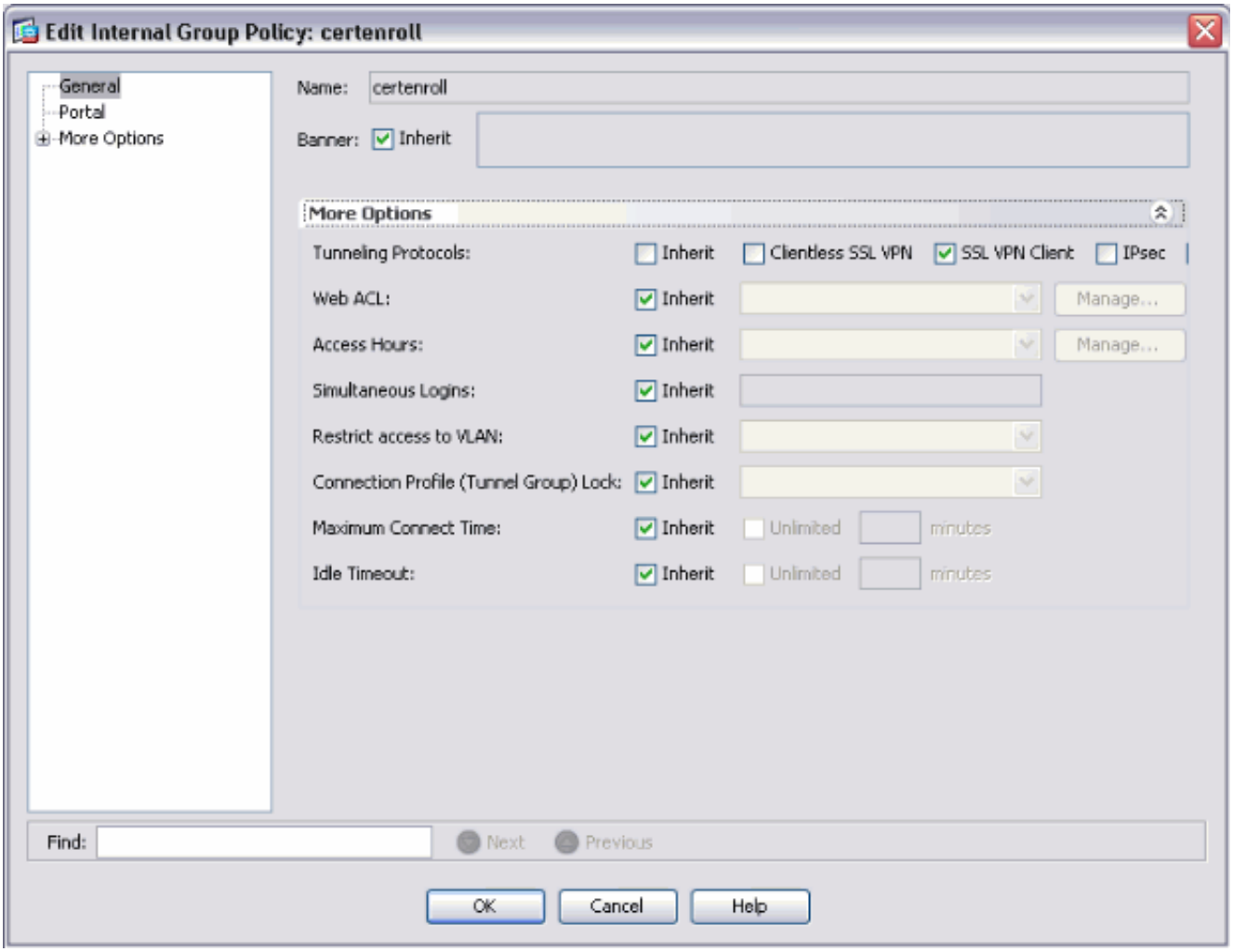
Complete estos pasos:

1. Cargue el perfil XML al ASA.Elija el **acceso del VPN de acceso remoto > de la red (cliente) > avanzó > SSL VPN > las configuraciones del cliente**.Bajo perfiles del cliente VPN SSL, haga click en AddEl tecleo **hojea los archivos locales** para seleccionar el archivo de perfil, y el tecleo **hojea el Flash** para especificar el nombre del archivo de destello.**Archivo de la carga del**
tecleo.

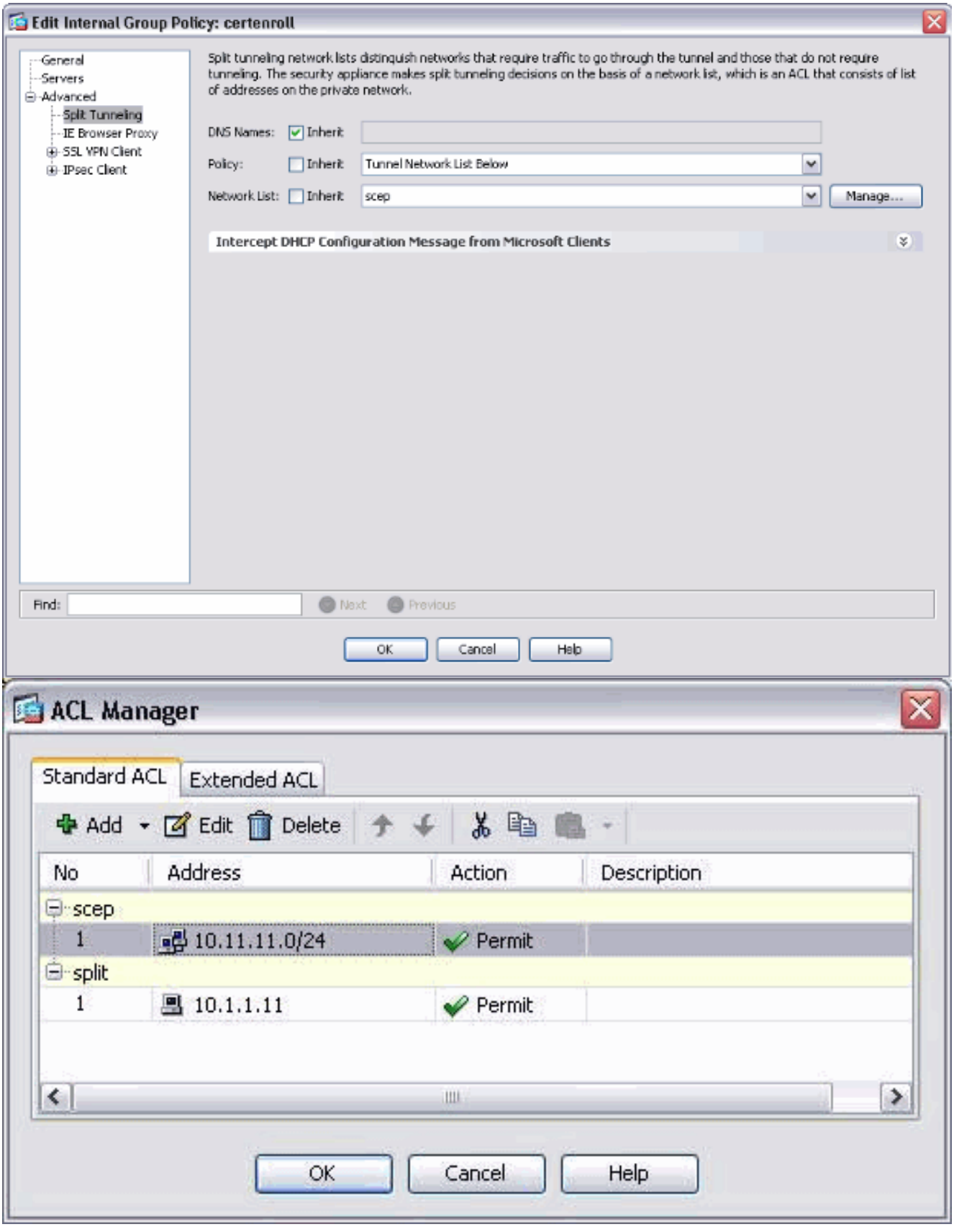


2. Configure una directiva del grupo del **certenroll** para la inscripción del certificado.Elija el **acceso del VPN de acceso remoto > de cliente de red > la directiva del grupo**, y el haga click

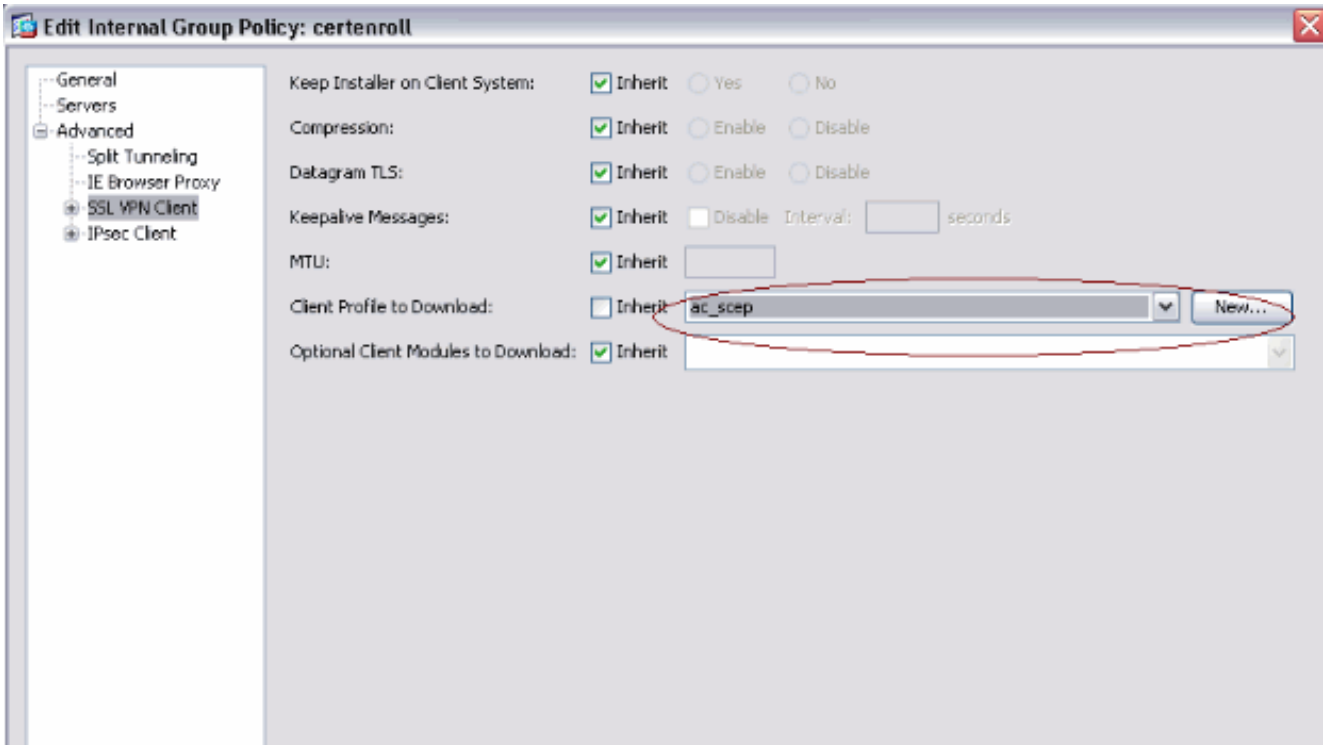
en
Add



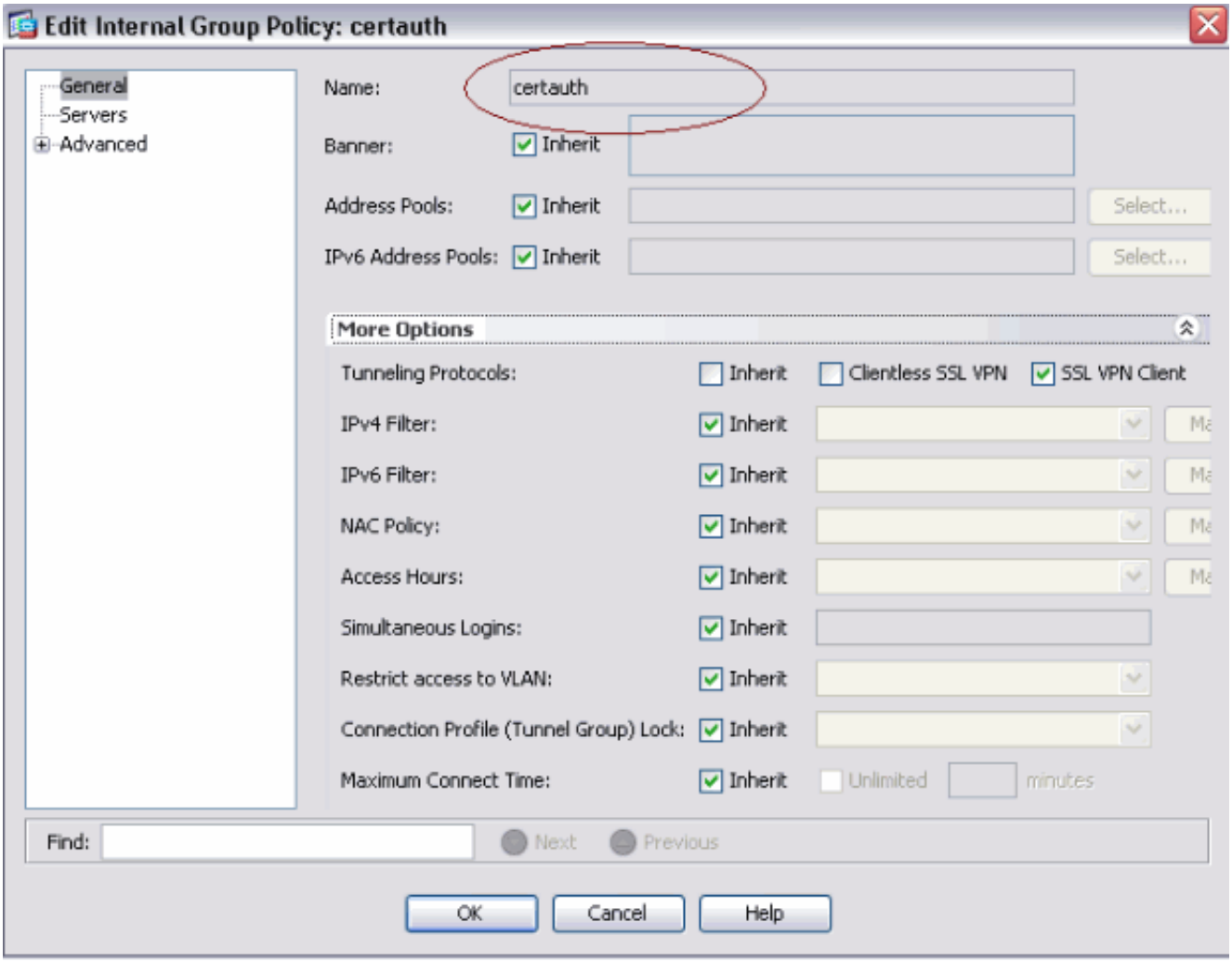
Agregue un túnel dividido para el servidor de CA.Amplíe **avanzado**, y después seleccione el **Túnel dividido**.Elija la **lista de la red de túneles abajo del** menú de la directiva, y el tecleo **maneja** para agregar el Access Control
List.



Seleccione al **cliente VPN SSL**, y elija el perfil para el certenroll del **perfil del cliente para descargar el**
menú.

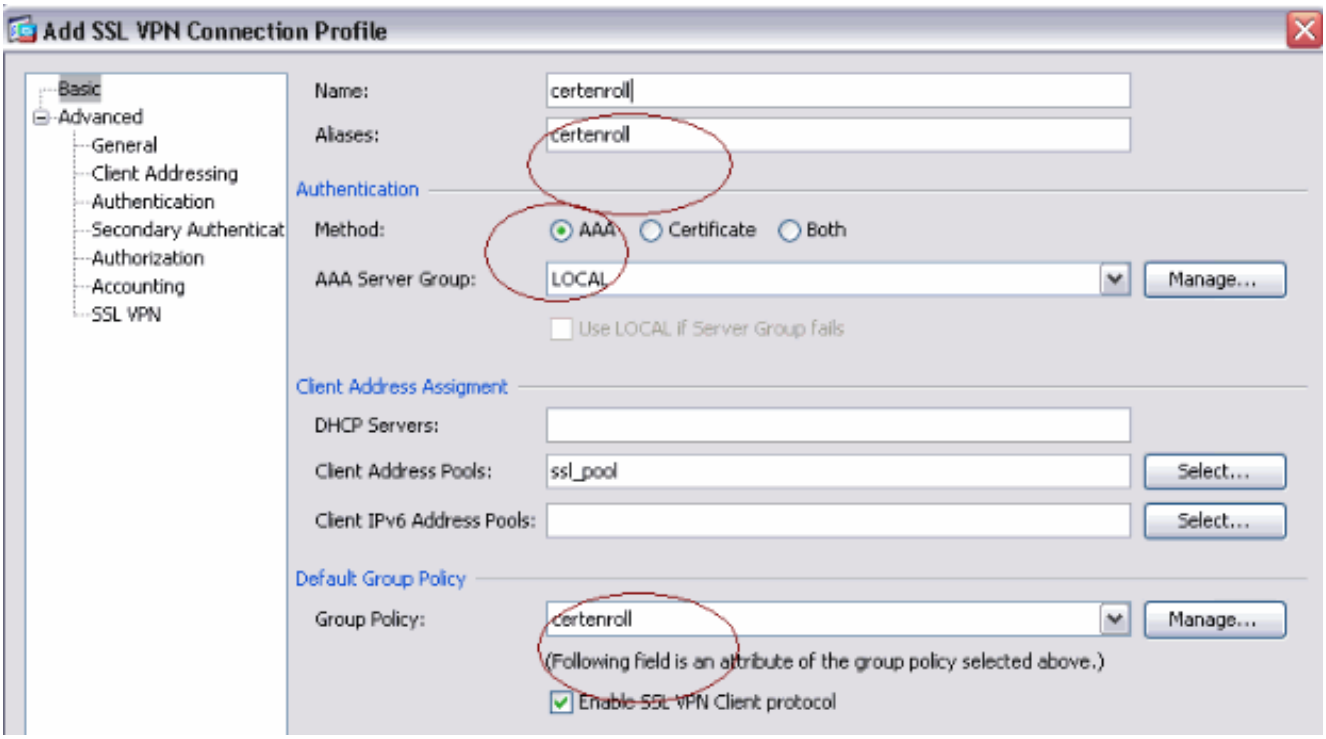


3. Cree a otro grupo llamado **certauth** para la autenticación certificada.

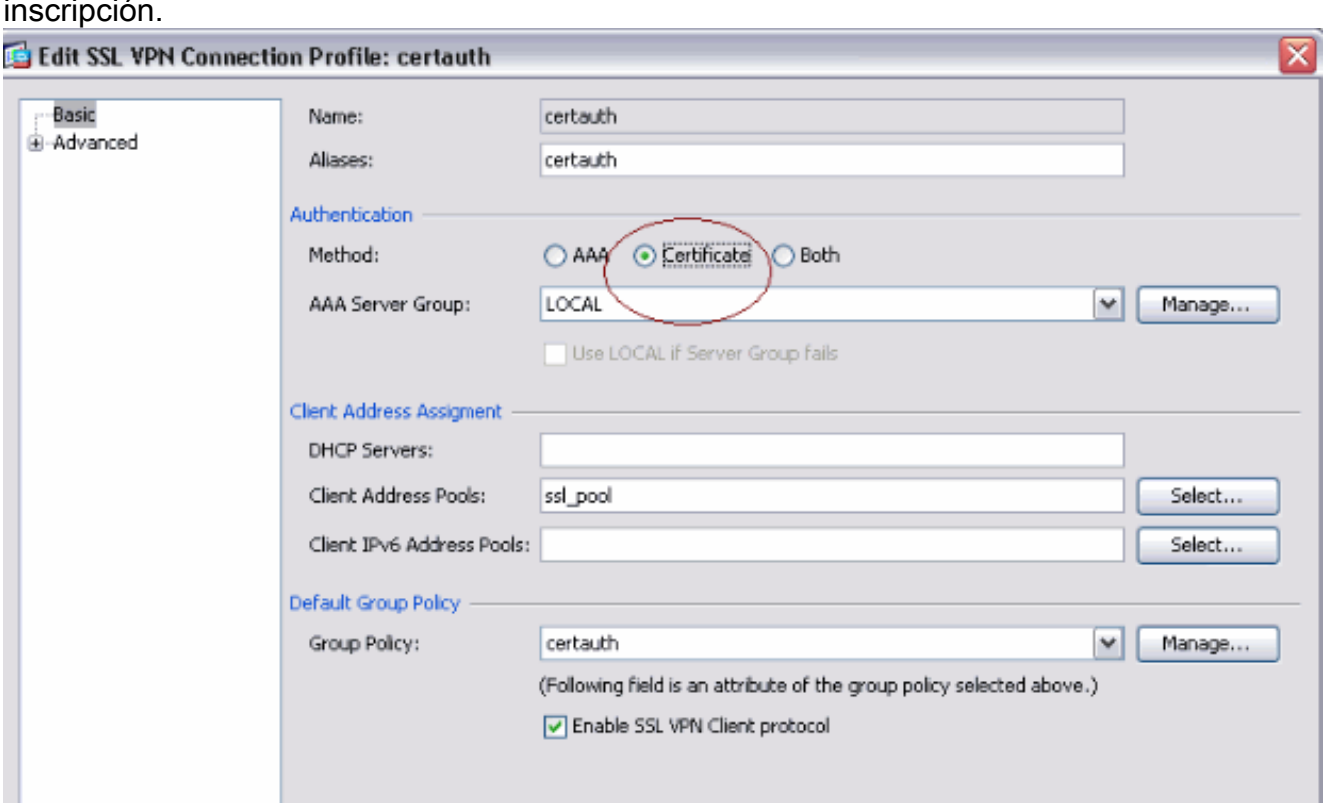


4. Cree un perfil de la conexión del certenroll.Elija el **acceso del VPN de acceso remoto > de cliente de red > los perfiles de la conexión de AnyConnect**, y el haga click en AddIngrese el grupo del **certenroll** en el campo de los alias.**Nota:** El nombre de alias debe hacer juego el valor usado en el perfil de AnyConnect bajo

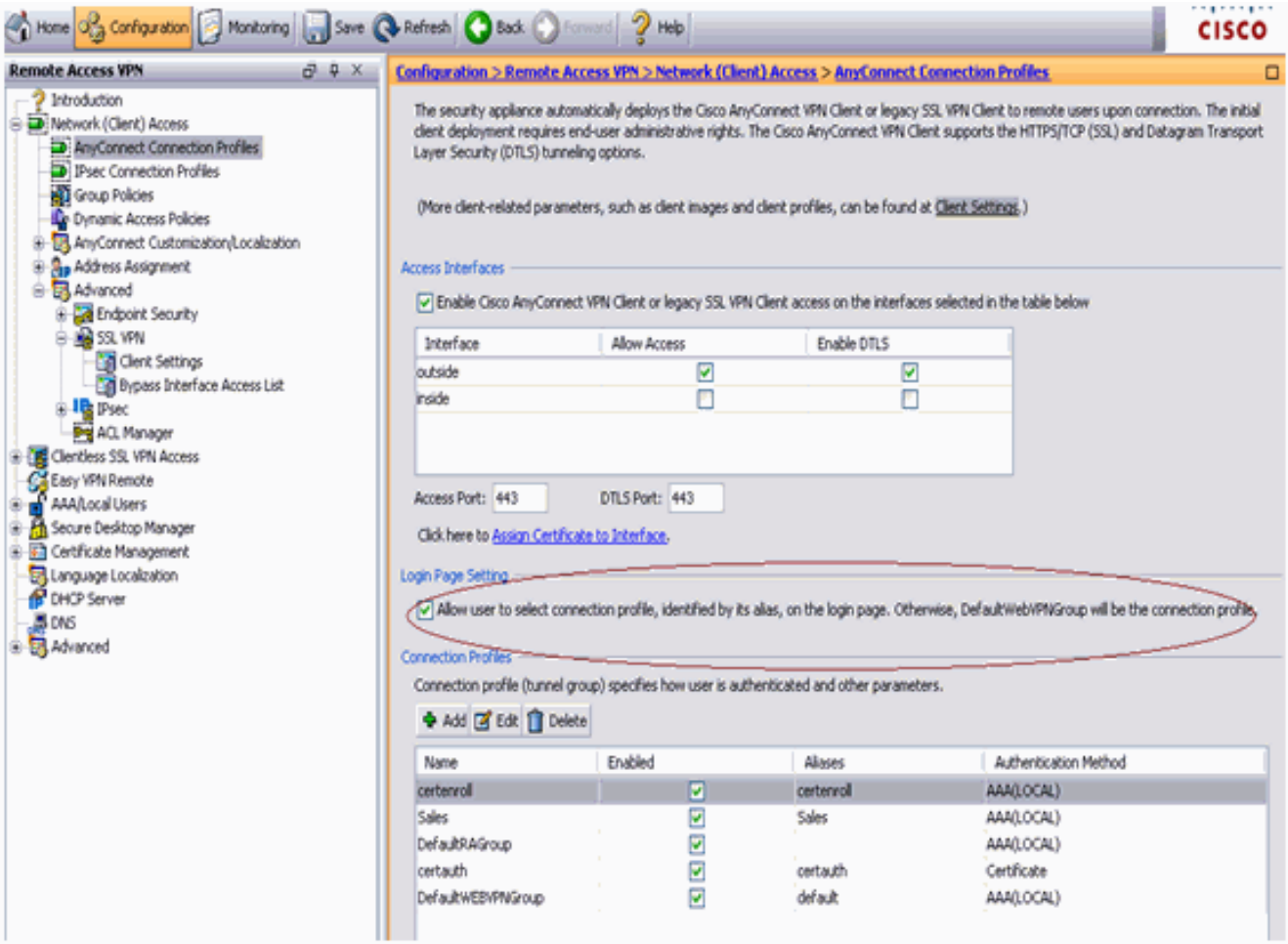
AutomaticSCEPHost.



5. Haga otro perfil de la conexión llamado **certauth** con la autenticación certificada. Éste es el perfil de la conexión real que se utiliza después de la inscripción.



6. Para se habilita aseegurarse el uso del alias, control **permite que el usuario seleccione el perfil de la conexión, identificado por su alias, en la página de registro. Si no, DefaultWebVPNGroup es el perfil de la conexión.**



Pruebe AnyConnect SCEP

Utilize esta sección para confirmar que su configuración funcione correctamente.

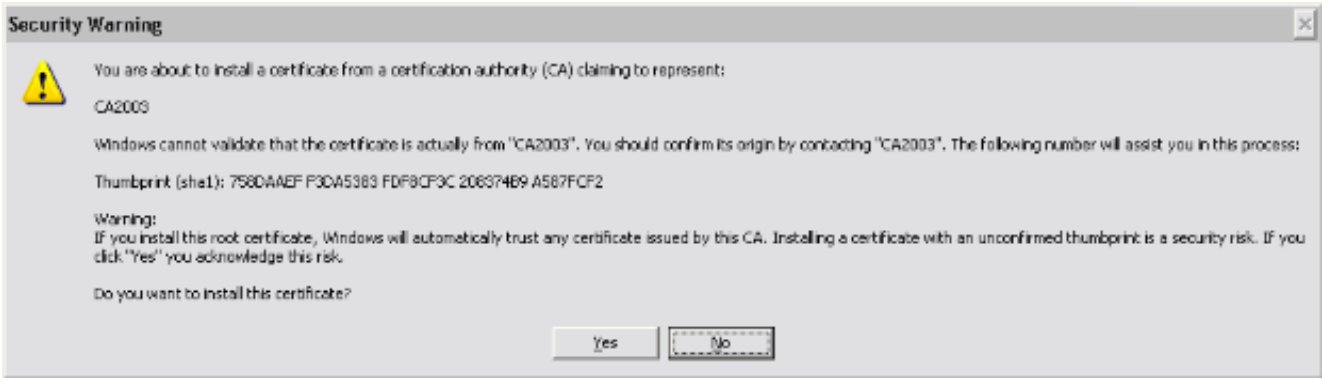
1. Inicie al cliente de AnyConnect, y conecte con el perfil del

certenroll. AnyConnect pasa la petición de la inscripción al servidor de CA con el

SCEP. AnyConnect pasa la petición de la inscripción directamente y no pasa a través del túnel, si se utiliza el botón del

certificado del conseguir.

2. Esta advertencia aparece. Haga clic **sí** para instalar el usuario y el certificado raíz del uso

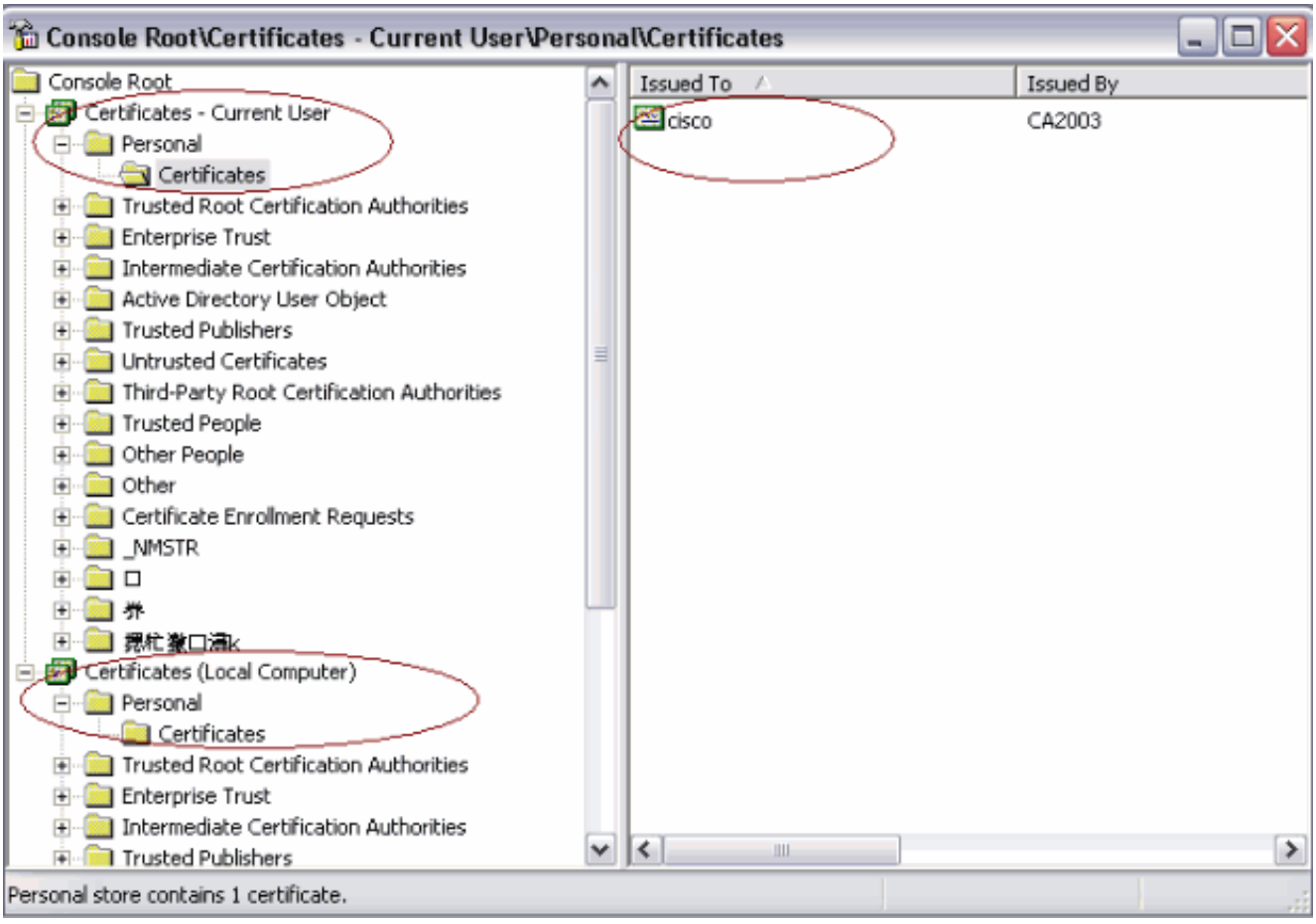


3. Una vez que se alista el certificado, conecte con el perfil del **certauth**.

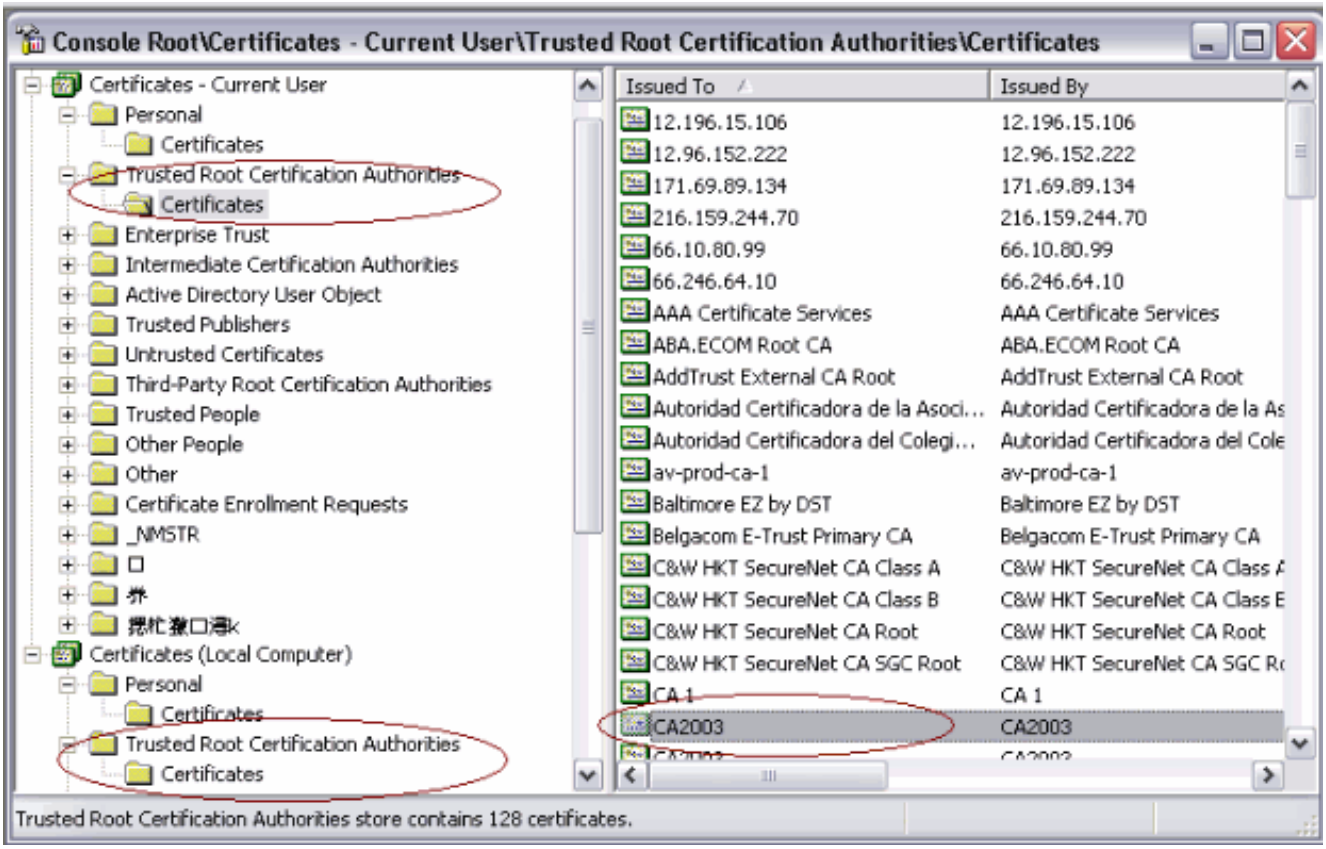
Certifique el almacenamiento en Microsoft Windows después de que petición SCEP

Complete estos pasos:

1. Haga clic el **Start (Inicio) > Run (Ejecutar) > el mmc**.
2. El tecleo **agrega/quita la broche adentro**.
3. Haga clic **agregan**, y eligen los **Certificados**.
4. Agregue los **mis** Certificados de la **cuenta de usuario** y de la **cuenta del ordenador**.Esta imagen muestra el Certificado de usuario instalado en el almacén de certificados de Windows:



Esta imagen muestra el certificado de CA instalado en el almacén de certificados de Windows:



Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

- Trabajos de la inscripción SCEP de AnyConnect solamente cuando la autenticación certificada falla. Si no está alistando, marque el almacén de certificados. Si los Certificados están instalados ya, borrelos y pruebe otra vez.
- La inscripción SCEP no trabaja a menos que se utilice el comando del **puerto externo 443 de la interfaz de la autenticación certificada SSL**.Refiera a este bug Cisco ID para más información:Id. de bug Cisco CSCtf06778 (clientes registrados solamente) — AnyConnect SCEP alista no trabaja con por el auth 2 CERT del grupoId. de bug Cisco CSCtf06844 (clientes registrados solamente) — Inscripción SCEP de AnyConnect que no trabaja con el ASA por el auth CERT del grupo
- Si el servidor de CA está en el exterior del ASA, aseegurese permitir la conexión mediante pines con el **comando intra-interface del permiso del trafico de seguridad igual**. También agregue el exterior y los comandos access-list nacionales tal y como se muestra en de este ejemplo:

```
nat (outside) 1
access-list natoutside extended permit ip 172.16.1.0 255.255.255.0 host 171.69.89.87
```

  Donde está 172.16.1.0 el pool y 171.69.89.87 de AnyConnect es el dirección IP del servidor de CA.
- Si el servidor de CA está en el interior, aseegurese incluirlo en la lista de acceso del túnel dividido para la directiva del grupo del **certenroll**. En este documento, se asume que el servidor de CA está en el interior.

```
group-policy certenroll attributes
split-tunnel-policy tunnelspecified
 split-tunnel-network-list value scep
```

```
access-list scep standard permit 171.69.89.0 255.255.255.0
```

Información Relacionada

- Guía del administrador del Cliente Cisco AnyConnect VPN, versión 2.4
- Soporte Técnico y Documentación - Cisco Systems