Configure el túnel VPN de administración de AnyConnect en ASA

Contenido

Introducción

Este documento describe cómo configurar un ASA cuando el gateway VPN acepta conexiones de Cisco AnyConnect Secure Mobility Client a través del túnel VPN de administración.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de VPN mediante el administrador adaptable de dispositivos de seguridad (ASDM)
- Configuración de CLI del dispositivo de seguridad adaptable básico (ASA)
- Certificados X509

Componentes Utilizados

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

- Software Cisco ASA versión 9.12(3)9
- Software Cisco ASDM versión 7.12.2

- Windows 10 con Cisco AnyConnect Secure Mobility Client versión 4.8.03036

  Nota: Descargue el paquete de implementación Web de AnyConnect VPN (anyconnect-win*.pkg or anyconnect-macos*.pkg) en Cisco Software Download (sólo clientes registrados). Copie el cliente VPN AnyConnect en la memoria flash del ASA que se descargará a los equipos de los usuarios remotos para establecer la conexión VPN SSL con el ASA. Consulte la sección Instalación del cliente AnyConnect de la guía de configuración de ASA para obtener más información.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Un túnel VPN de gestión garantiza la conectividad a la red corporativa siempre que se encienda el sistema cliente, no solo cuando el usuario final establece una conexión VPN. Puede realizar la administración de parches en terminales fuera de la oficina, especialmente en dispositivos que el usuario no conecta con frecuencia, a través de VPN, a la red de la oficina. Los scripts de inicio de sesión de Endpoint OS que requieren conectividad de red corporativa también se benefician de esta función.

AnyConnect Management Tunnel permite a los administradores tener AnyConnect conectado sin la intervención del usuario antes de que este inicie sesión. El túnel de administración de AnyConnect puede funcionar junto con la detección de redes de confianza y, por lo tanto, solo se activa cuando el terminal está fuera de las instalaciones y desconectado de una VPN iniciada por el usuario. El túnel de administración de AnyConnect es transparente para el usuario final y se desconecta automáticamente cuando el usuario inicia la VPN.

SO/Aplicación	Requisitos de versión mínimos
ASA	9.0.1
ASDM	7.10.1
Versión de Windows AnyConnect	4.7.00136
Versión de macOS AnyConnect	4.7.01076
Linux	No admitido

Trabajo del Túnel de Gestión

El servicio de agente VPN de AnyConnect se inicia automáticamente al arrancar el sistema. Detecta que la función de túnel de gestión está activada (a través del perfil de VPN de gestión), por lo que inicia la aplicación cliente de gestión para iniciar una conexión de túnel de gestión. La aplicación cliente de administración utiliza la entrada de host del perfil VPN de administración para iniciar la conexión. A continuación, el túnel VPN se establece de la forma habitual, con una excepción: no se realiza ninguna actualización de software durante una conexión de túnel de gestión, ya que el túnel de gestión debe ser transparente para el usuario.

El usuario inicia un túnel VPN a través de la interfaz de usuario de AnyConnect, que activa la terminación del túnel de administración. Tras la terminación del túnel de administración, el establecimiento del túnel del usuario continúa de la forma habitual.

El usuario desconecta el túnel VPN, lo que activa el restablecimiento automático del túnel de gestión.

Limitaciones

- No se admite la interacción del usuario
- La autenticación basada en certificados a través del Almacén de certificados del equipo (Windows) sólo se admite
- Se aplica la comprobación estricta de certificados de servidor
- No se admite un proxy privado
- No se admite un proxy público (el valor ProxyNative se admite en plataformas en las que no se recupera la configuración del proxy nativo del explorador)
- No se admiten scripts de personalización de AnyConnect

Nota: Para obtener más información, consulte Acerca del Túnel VPN de Administración.

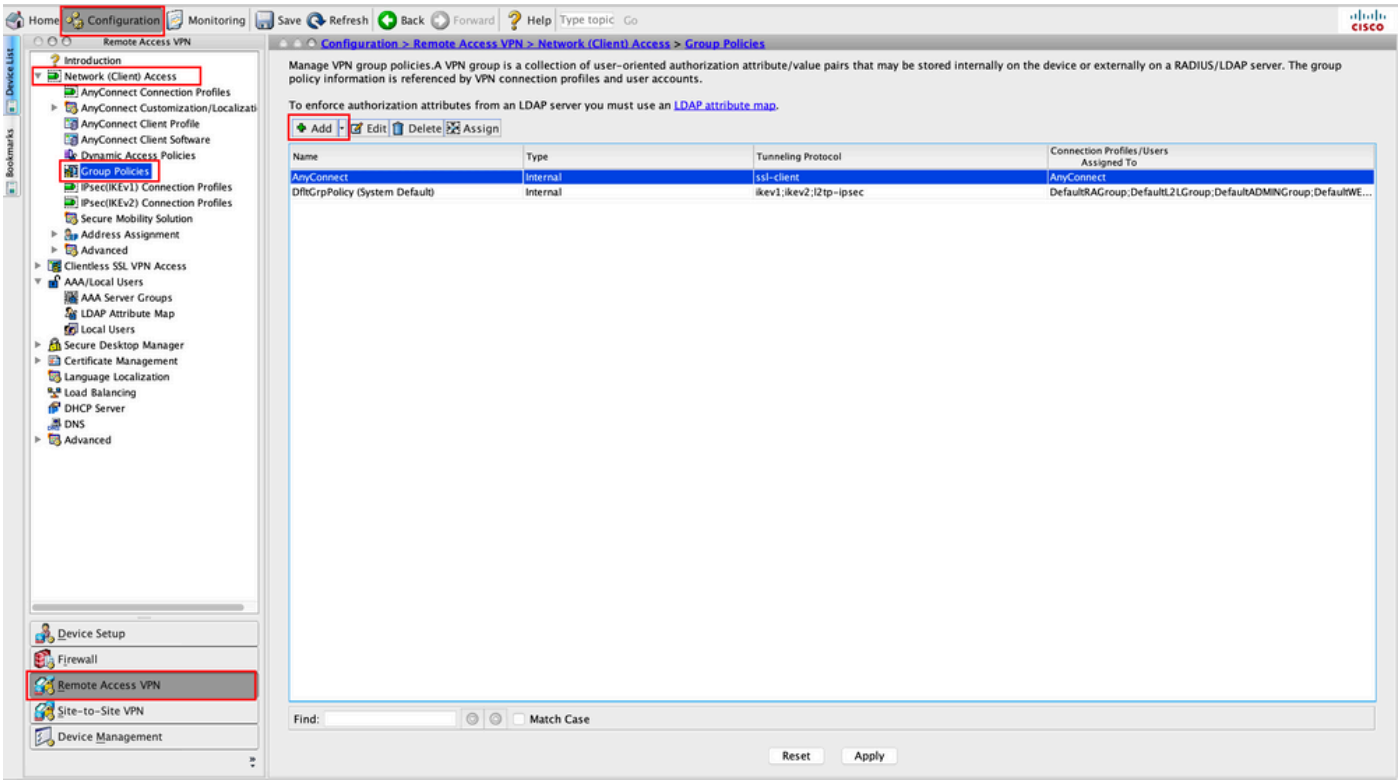
Configurar

En esta sección se describe cómo configurar Cisco ASA como gateway VPN para aceptar conexiones de clientes AnyConnect a través del túnel VPN de administración.

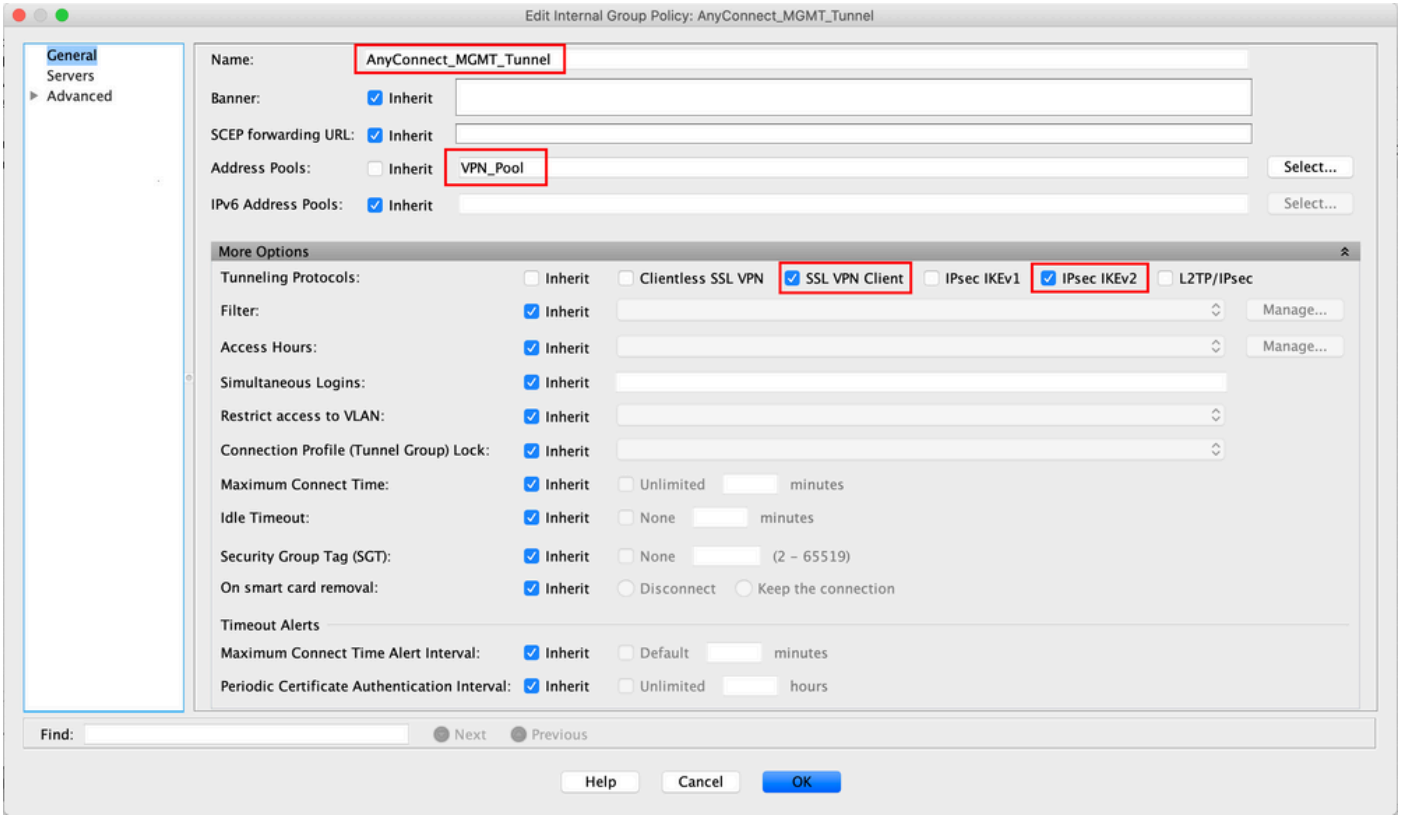
Configuración en ASA mediante ASDM/CLI

Paso 1. Cree la directiva de grupo de AnyConnect. Desplácese hasta Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Haga clic en Add.

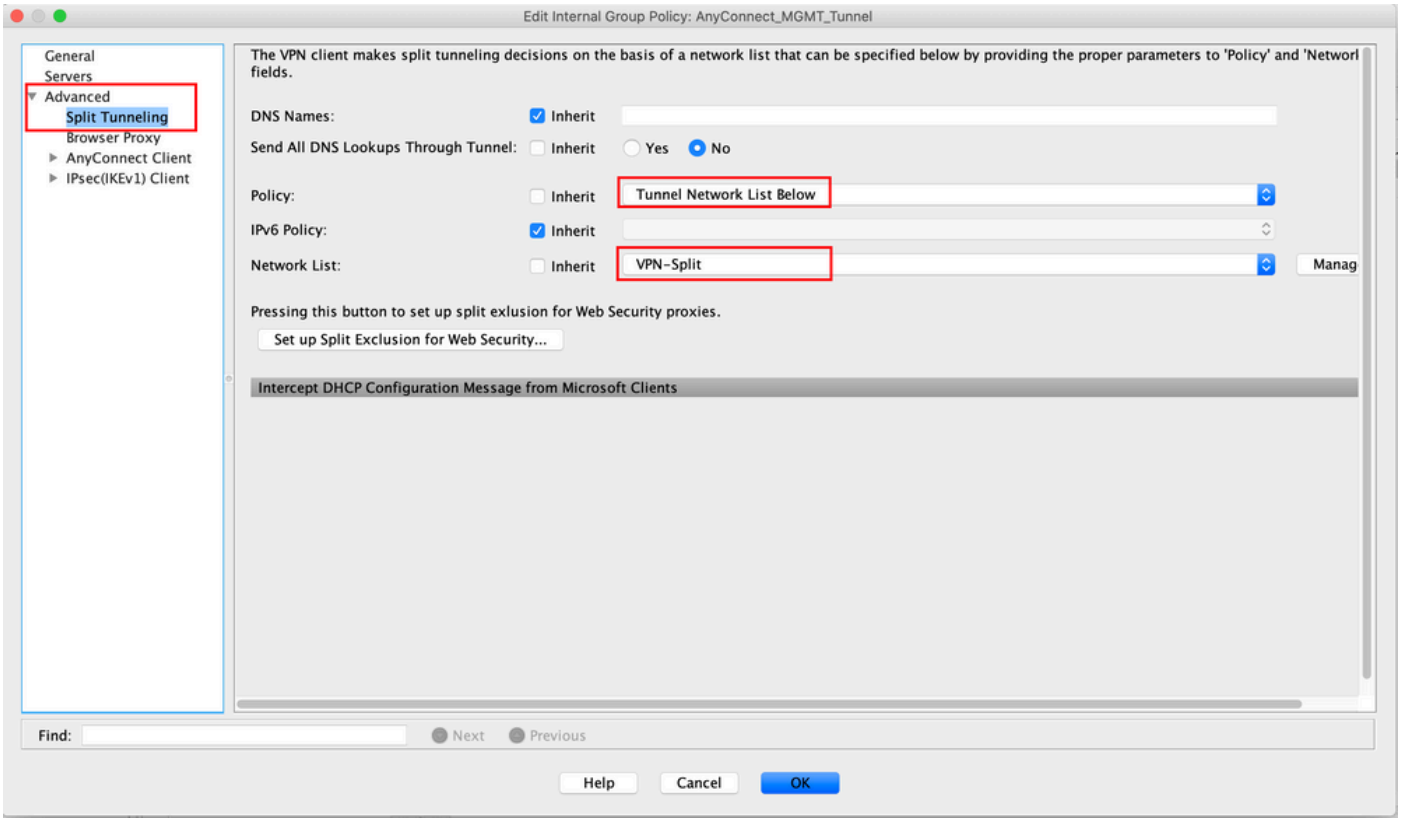
Nota: se recomienda crear una nueva política de grupo de AnyConnect que se utilice solo para el túnel de administración de AnyConnect.



Paso 2. Proporcionar una Name para la Directiva de grupo. Asignar/crear un Address Pool. Elegir Tunneling Protocols como SSL VPN Client y/o IPsec IKEv2, como se muestra en la imagen.

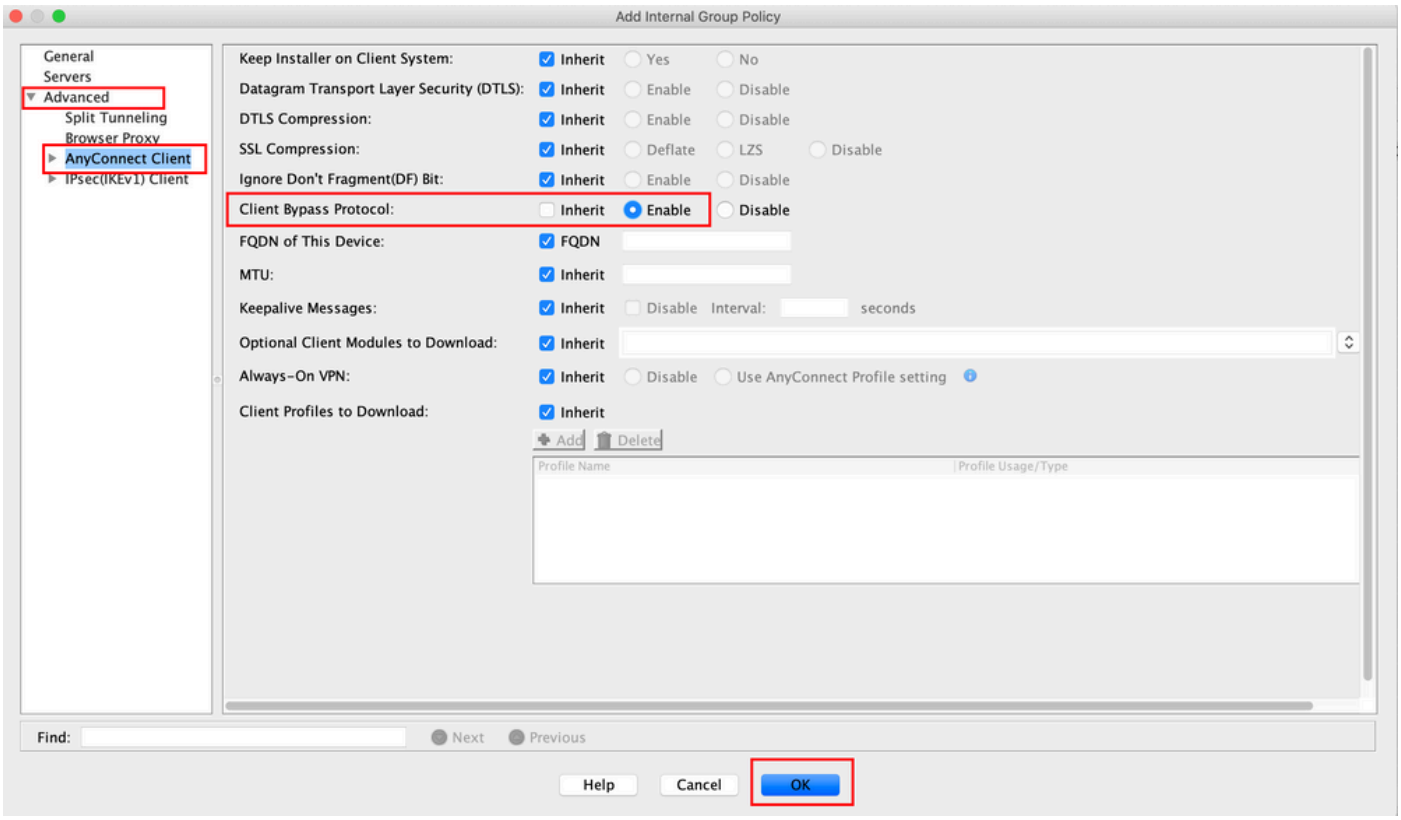


Paso 3. Desplácese hasta Advanced > Split Tunneling. Configure el Policy como Tunnel Network List Below y seleccione la Network List, como se muestra en la imagen.

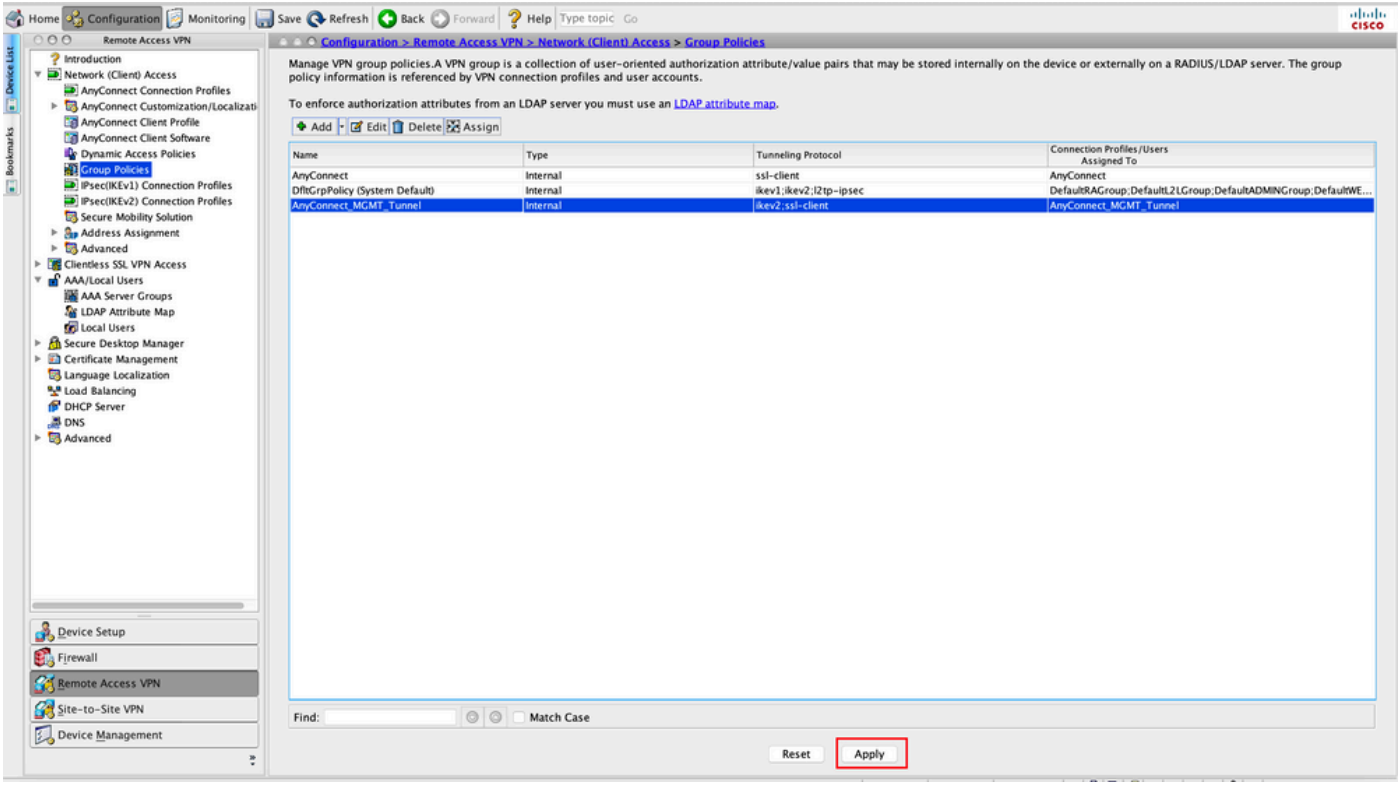


Nota: Si no se introduce una dirección de cliente para ambos protocolos IP (IPv4 e IPv6), el **Client Bypass Protocol** la configuración debe ser enabled para que el tráfico correspondiente no se vea interrumpido por el túnel de gestión. Para realizar la configuración, consulte el paso 4.

Paso 4. Desplácese hasta Advanced > AnyConnect Client. Set Client Bypass Protocol a Enable. Haga clic en OK para guardar, como se muestra en la imagen.



Paso 5. Como se muestra en esta imagen, haga clic en Apply para enviar la configuración al ASA.

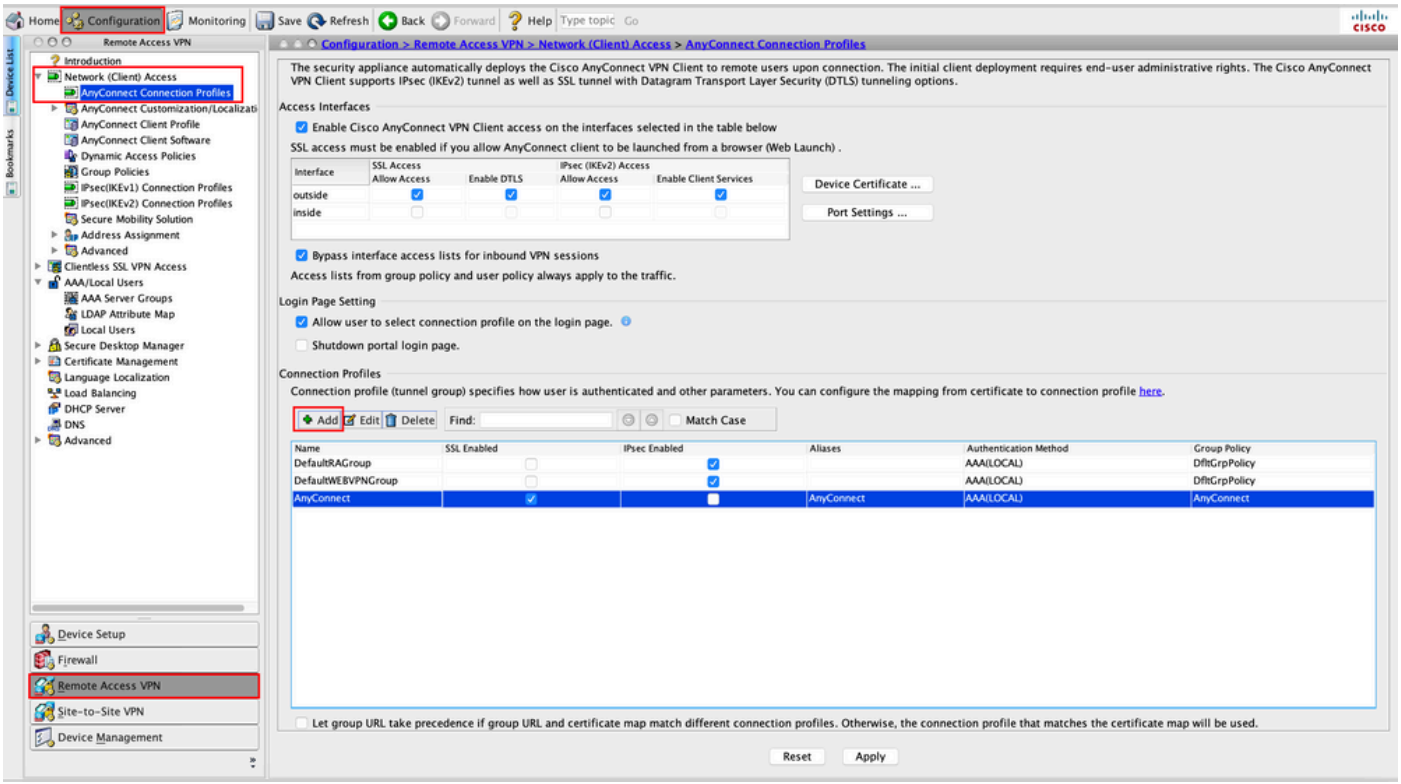


Configuración CLI para la directiva de grupo:

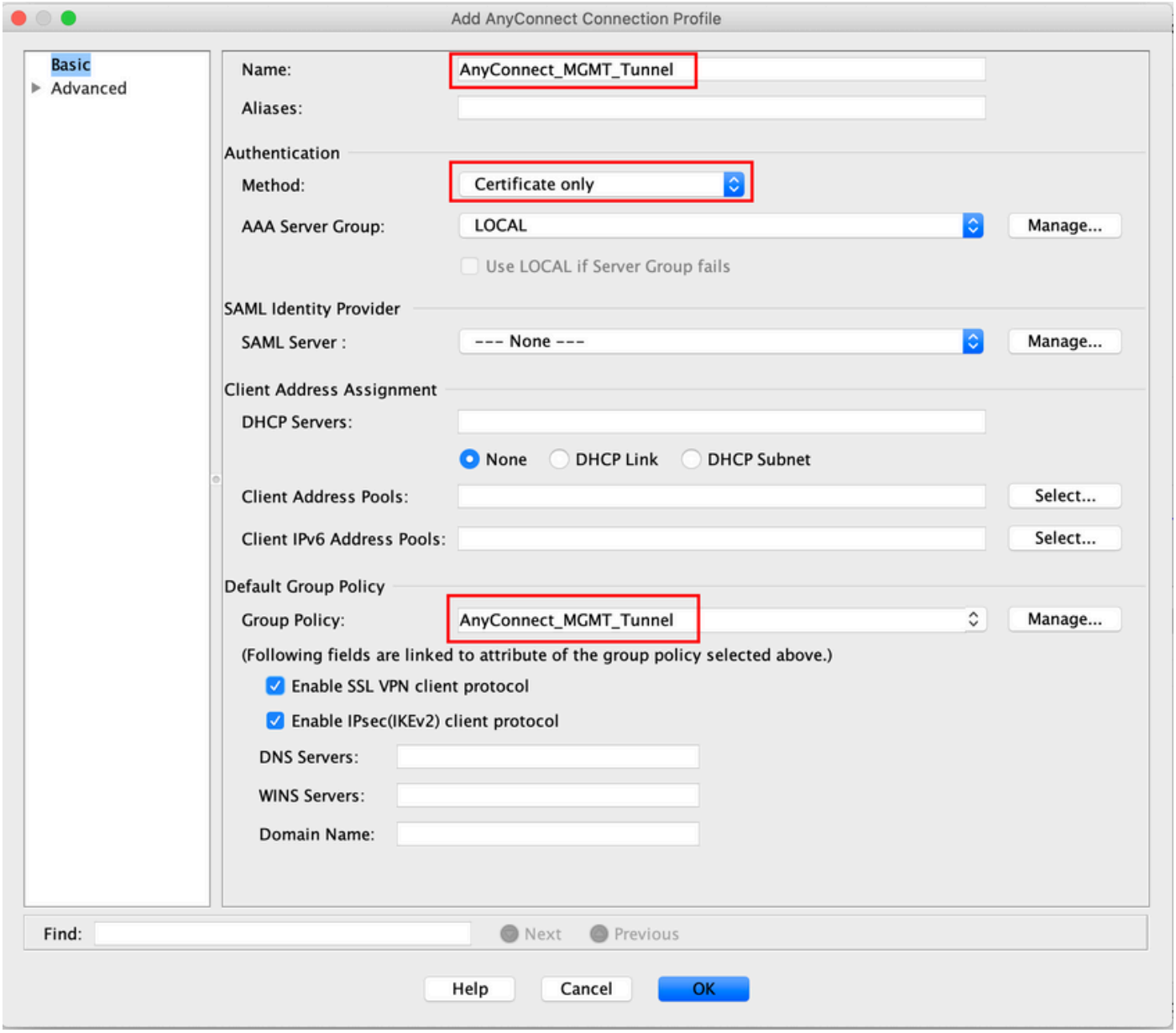
```
ip local pool VPN_Pool 192.168.10.1-192.168.10.100 mask 255.255.255.0
! access-list VPN-Split standard permit 172.16.0.0 255.255.0.0
! group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-network-list value VPN-Split
 client-bypass-protocol enable
 address-pools value VPN_Pool
```

Paso 6. Cree el perfil de conexión de AnyConnect. Desplácese hasta Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. Haga clic en Add.

> **Nota:** se recomienda crear un nuevo perfil de conexión de AnyConnect que se utilice solo para el túnel de administración de AnyConnect.



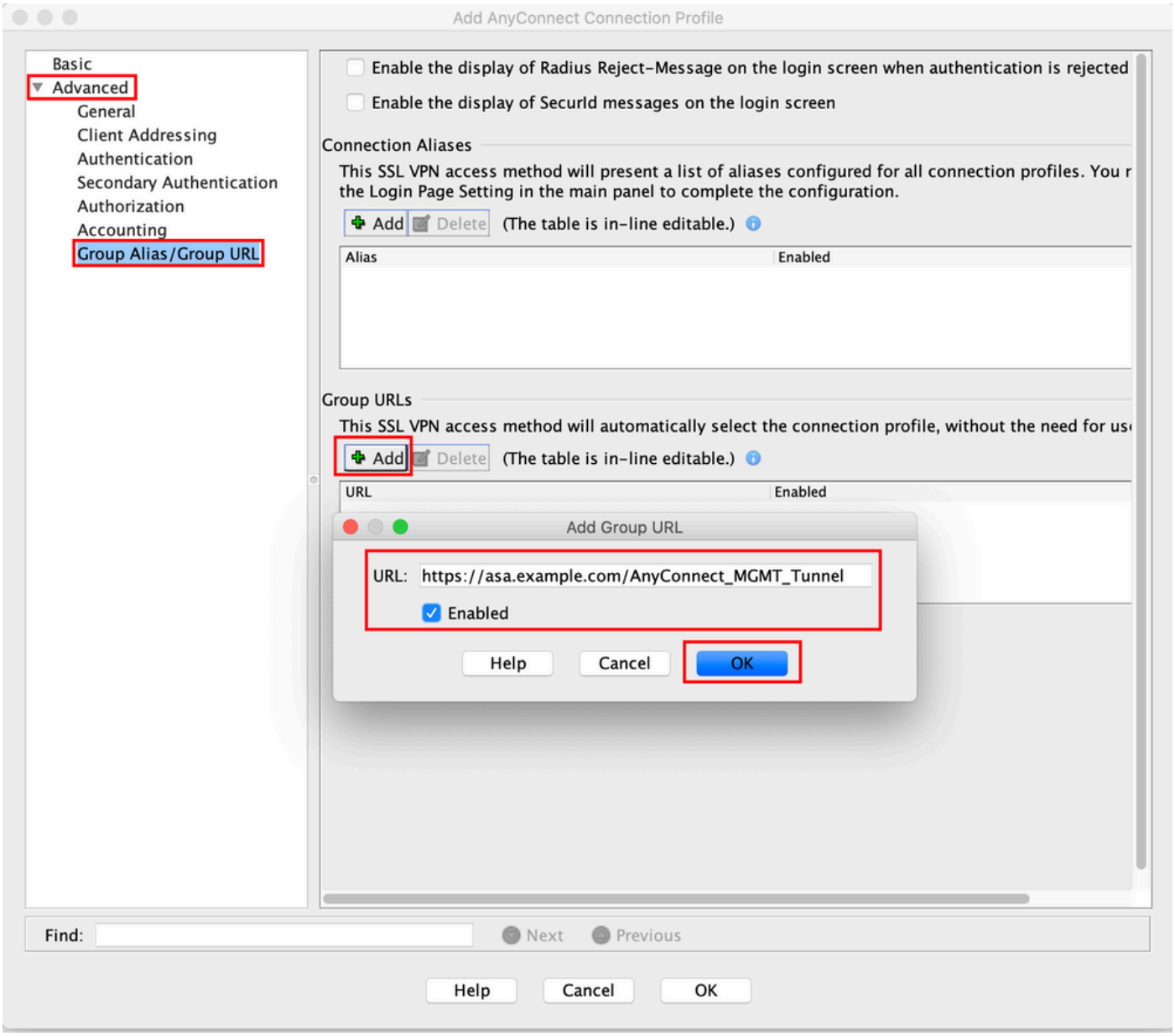
Paso 7. Proporcionar una Name para el perfil de conexión y establezca Authentication Method como Certificate only. Elija el Group Policy como el creado en el Paso 1.



Nota: Asegúrese de que el certificado raíz de la CA local esté presente en el ASA. Desplácese hasta Configuration > Remote Access VPN > Certificate Management > CA Certificates para agregar o ver el certificado.

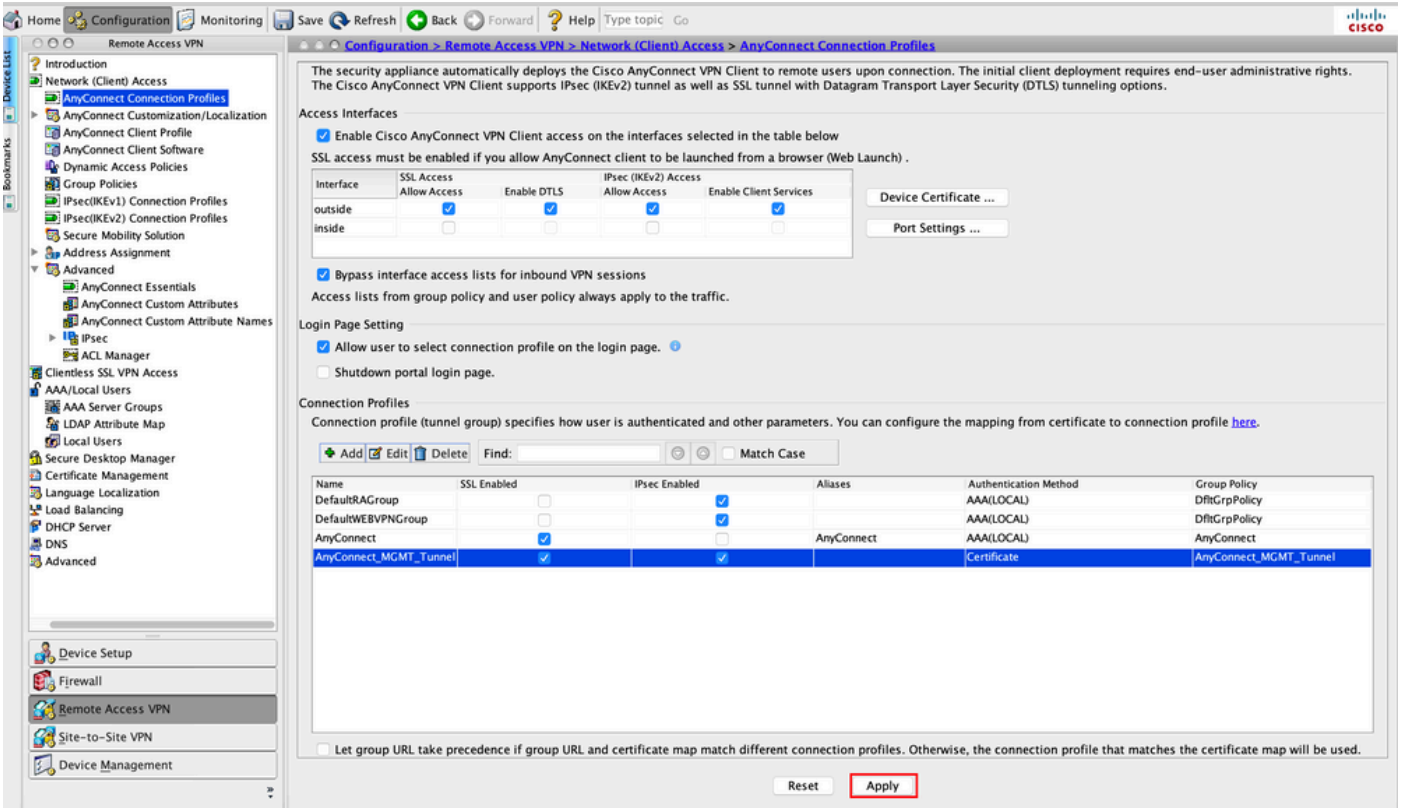
Nota: Asegúrese de que existe un certificado de identidad emitido por la misma CA local en el Almacén de certificados del equipo (para Windows) y/o en Cadena de claves del sistema (para macOS).

Paso 8. Desplácese hasta Advanced > Group Alias/Group URL. Haga clic en Add bajo Group URLs y añada un URL. Garantizar Enabled está activado. Haga clic en OK para guardar, como se muestra en la imagen.



Si se utiliza IKEv2, asegúrese de IPsec (IKEv2) Access está habilitado en la interfaz utilizada para AnyConnect.

Paso 9. Haga clic en Apply para enviar la configuración al ASA.

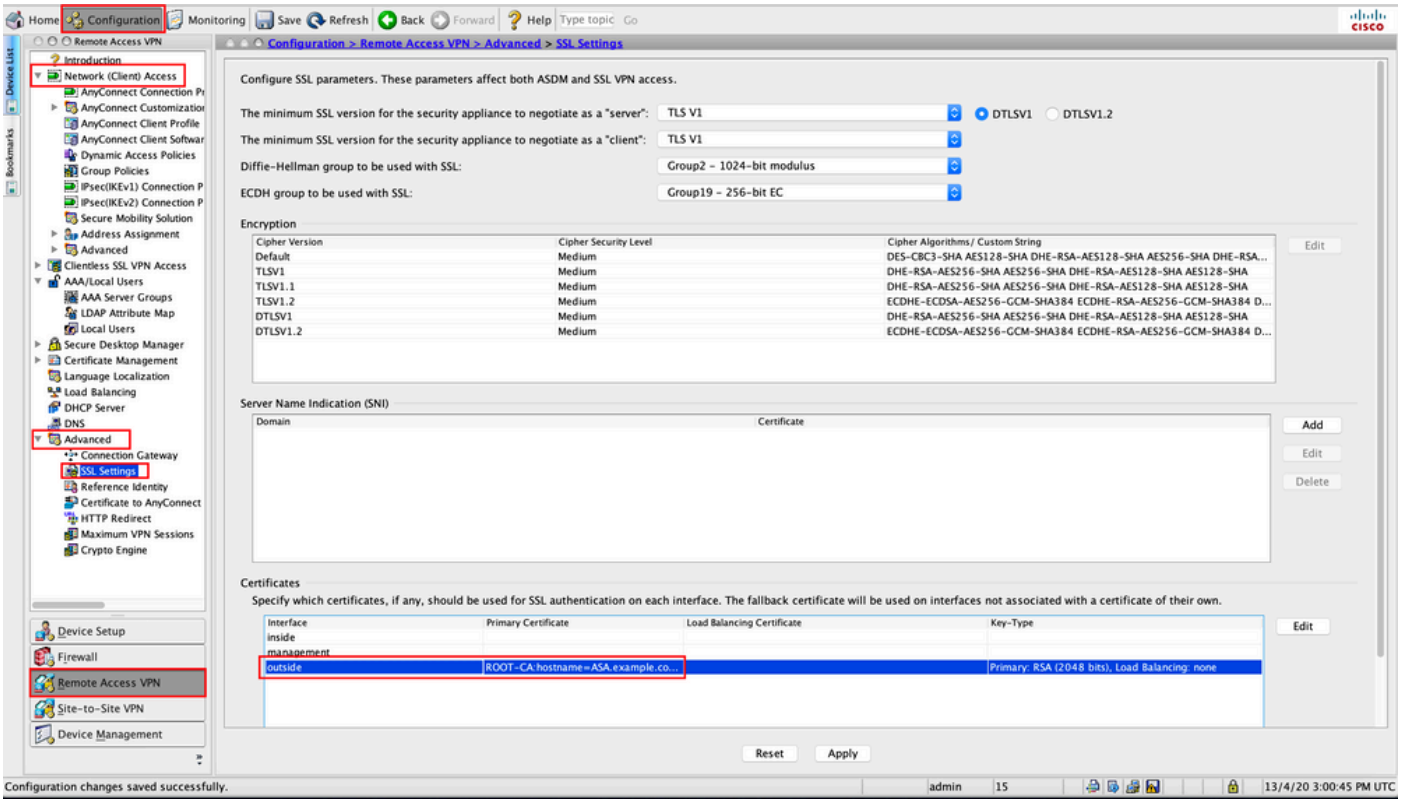


Configuración CLI para el perfil de conexión (grupo de túnel):

```
tunnel-group AnyConnect_MGMT_Tunnel type remote-access
tunnel-group AnyConnect_MGMT_Tunnel general-attributes
 default-group-policy AnyConnect_MGMT_Tunnel
tunnel-group AnyConnect_MGMT_Tunnel webvpn-attributes
 authentication certificate
 group-url https://asa.example.com/AnyConnect_MGMT_Tunnel enable
```

Paso 10. Asegúrese de que un certificado de confianza esté instalado en el ASA y enlazado a la interfaz utilizada para las conexiones de AnyConnect. Desplácese hasta Configuration > Remote Access VPN > Advanced > SSL Settings para agregar o ver esta configuración.

Nota: Refiérase a Instalación del Certificado de Identidad en ASA.

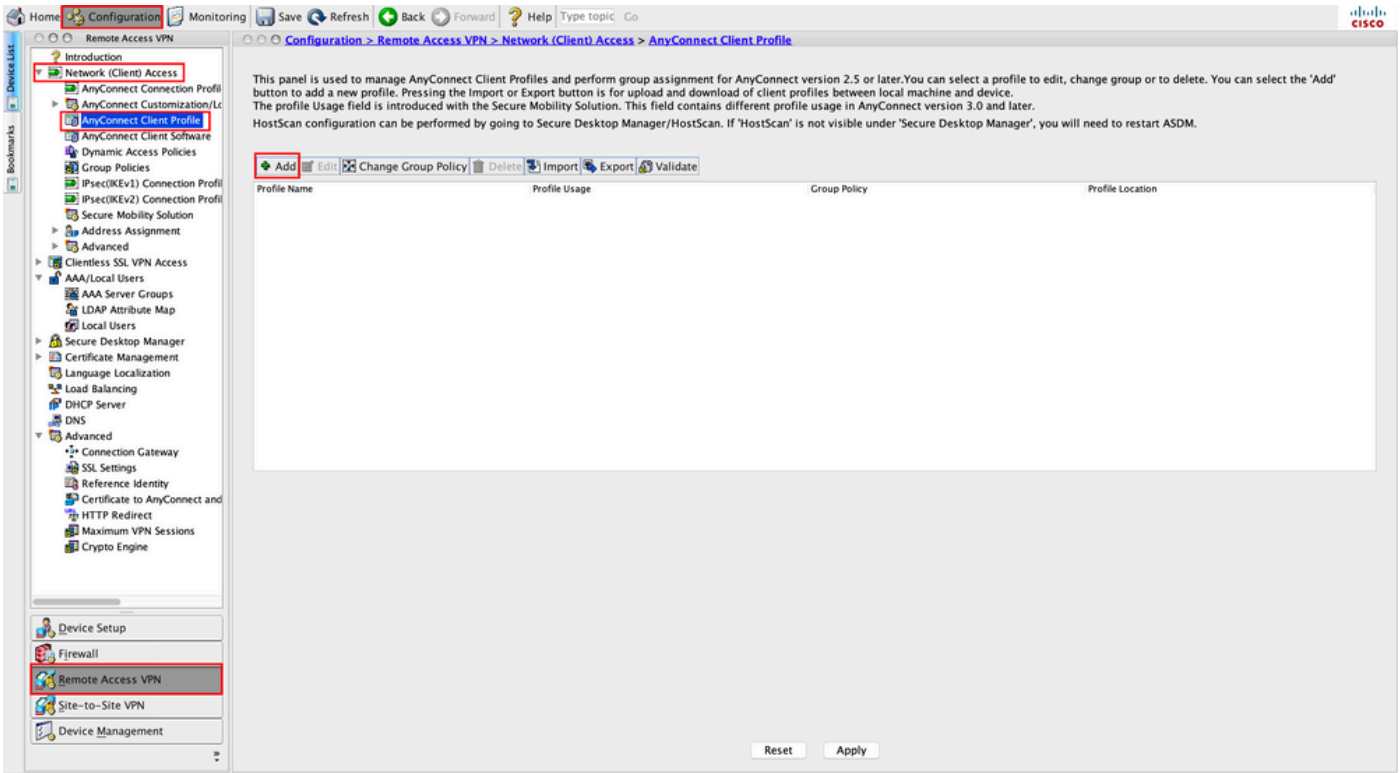


Configuración CLI para SSL Trustpoint:

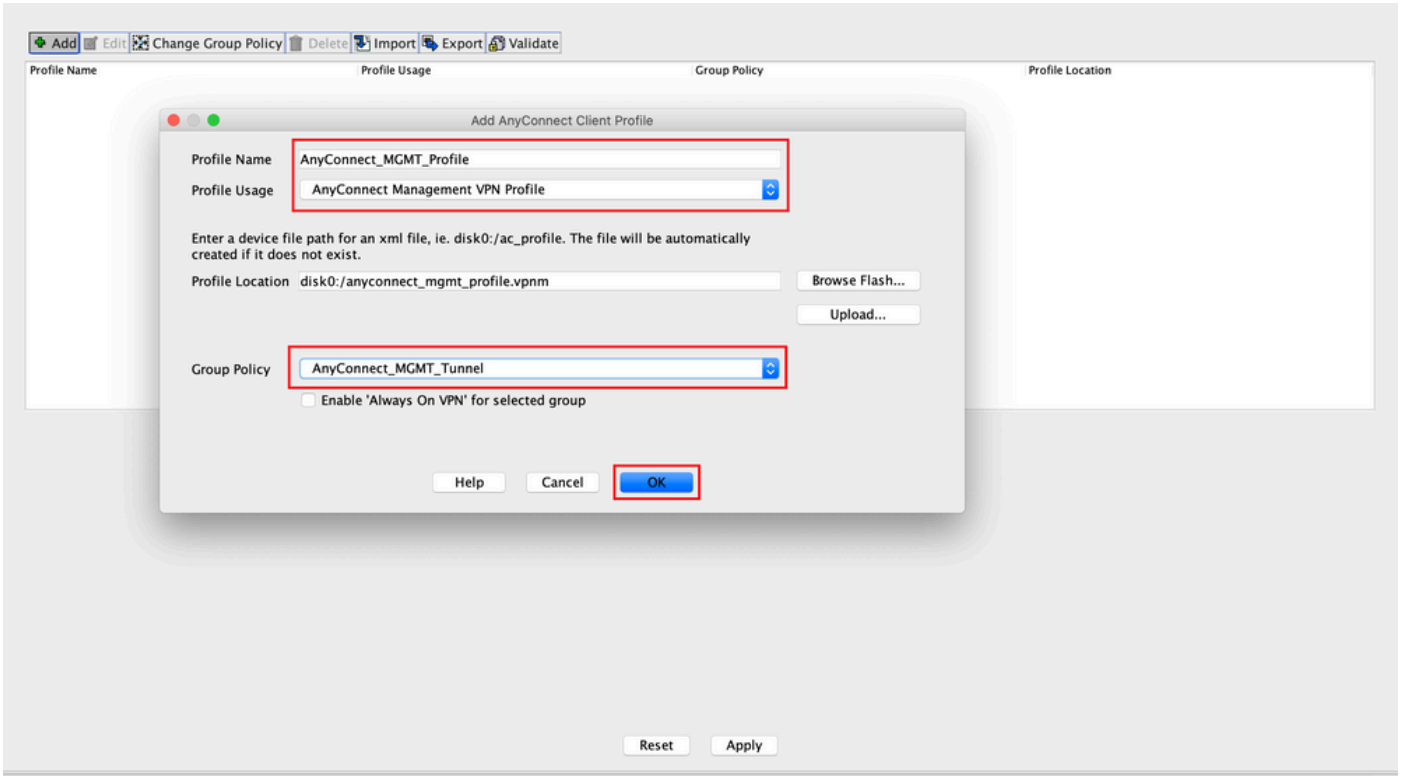
```
ssl trust-point ROOT-CA outside
```

Creación del perfil VPN de administración de AnyConnect

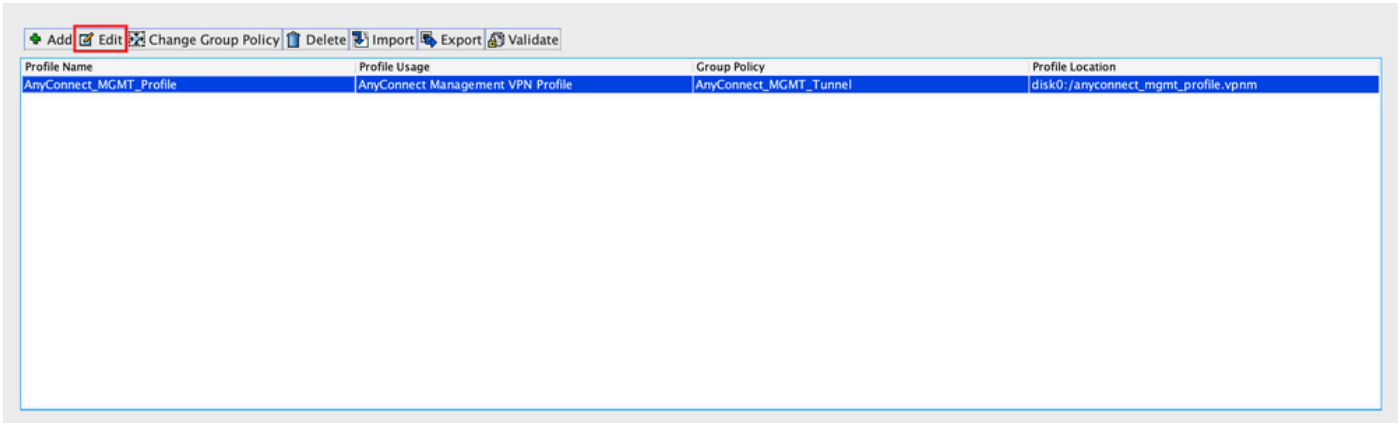
Paso 1. Cree el perfil de cliente de AnyConnect. Desplácese hasta Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. Haga clic en Add, como se muestra en la imagen.



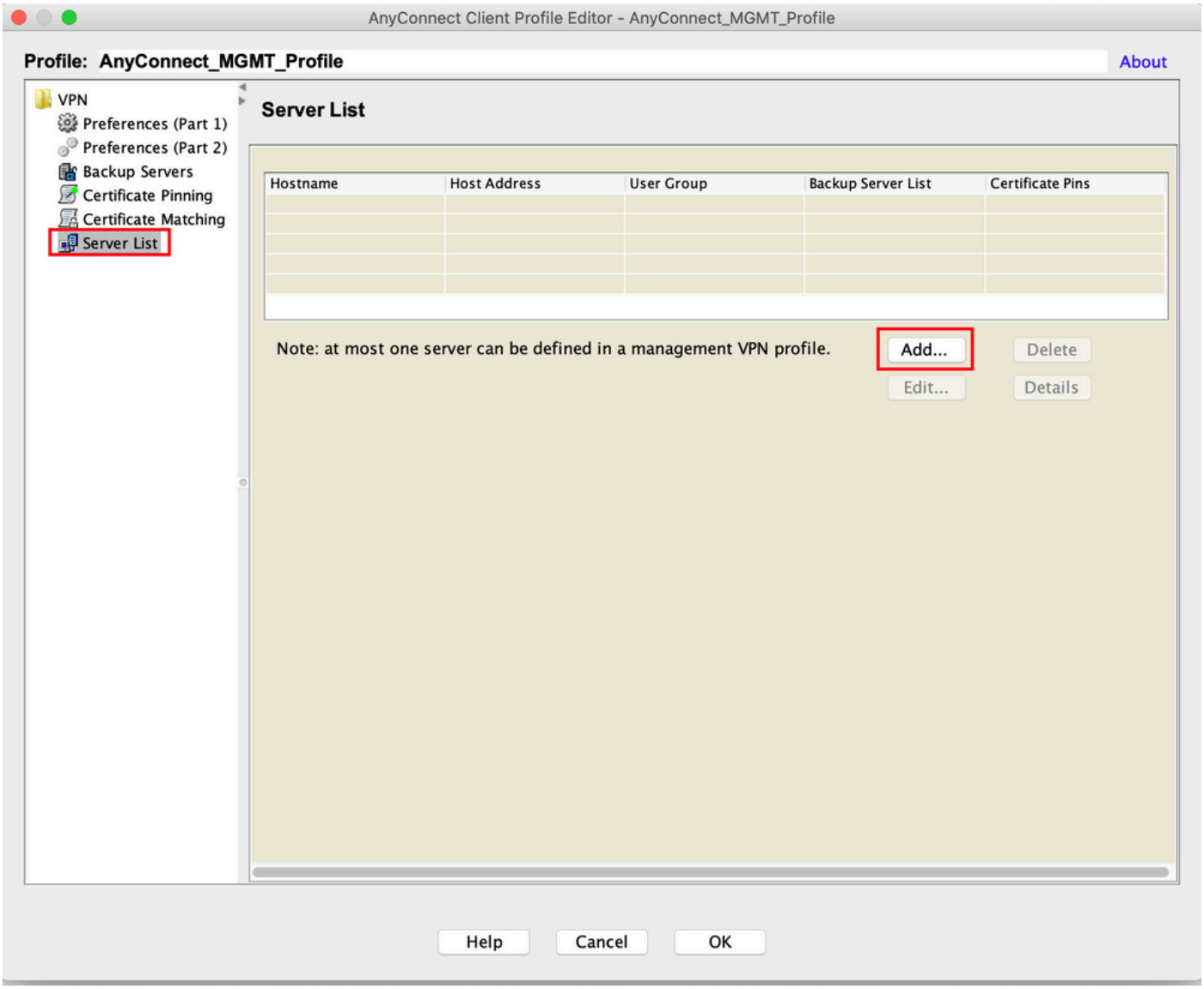
Paso 2. Proporcionar una Profile Name. Elija el Profile Usage como AnyConnect Management VPN profile. Elija el Group Policy creado en el Paso 1. Haga clic en OK , como se muestra en la imagen.



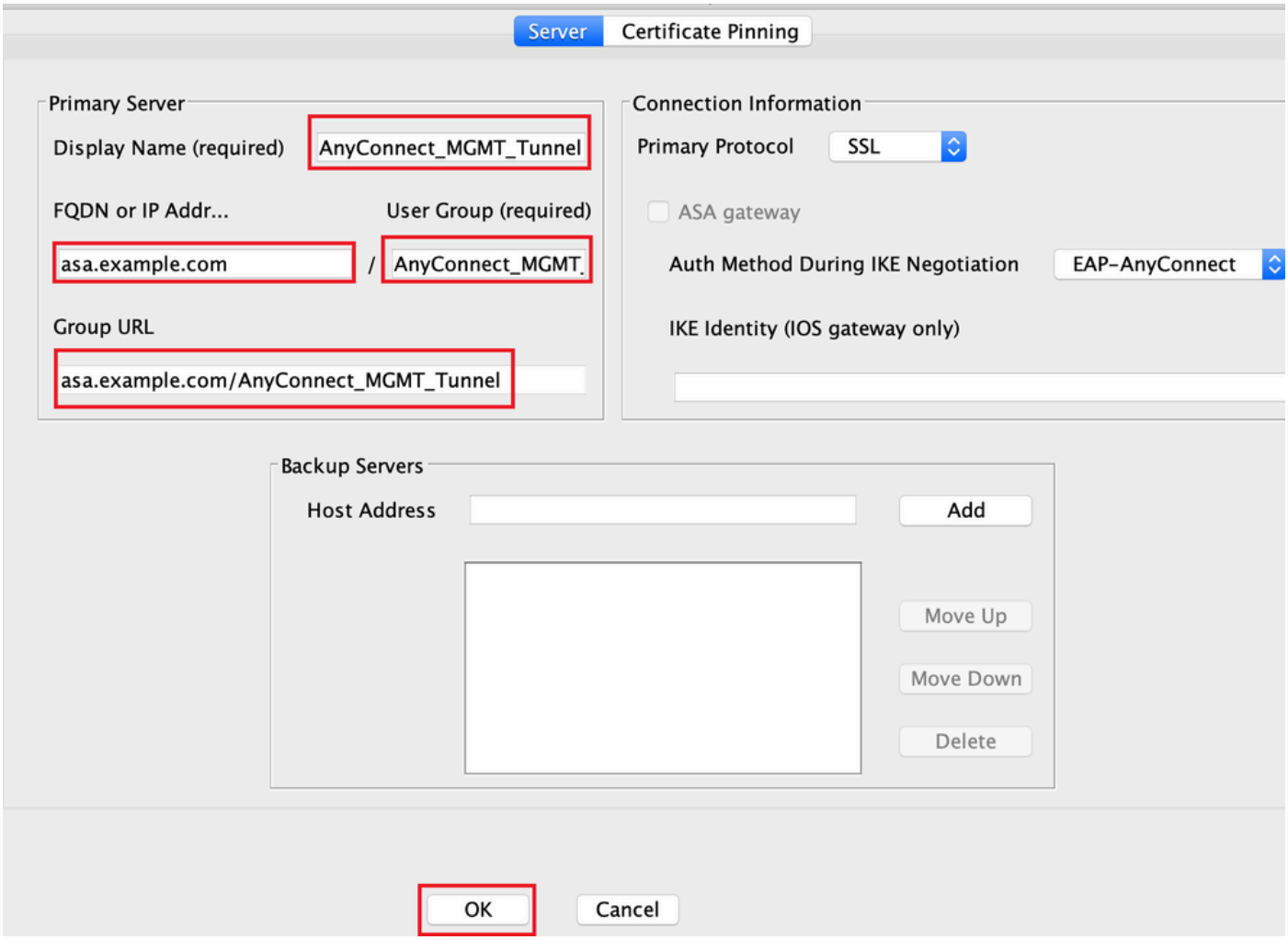
Paso 3. Elija el perfil creado y haga clic en Edit, como se muestra en la imagen.



Paso 4. Desplácese hasta Server List. Haga clic en Add para agregar una nueva entrada de la lista de servidores, como se muestra en la imagen.



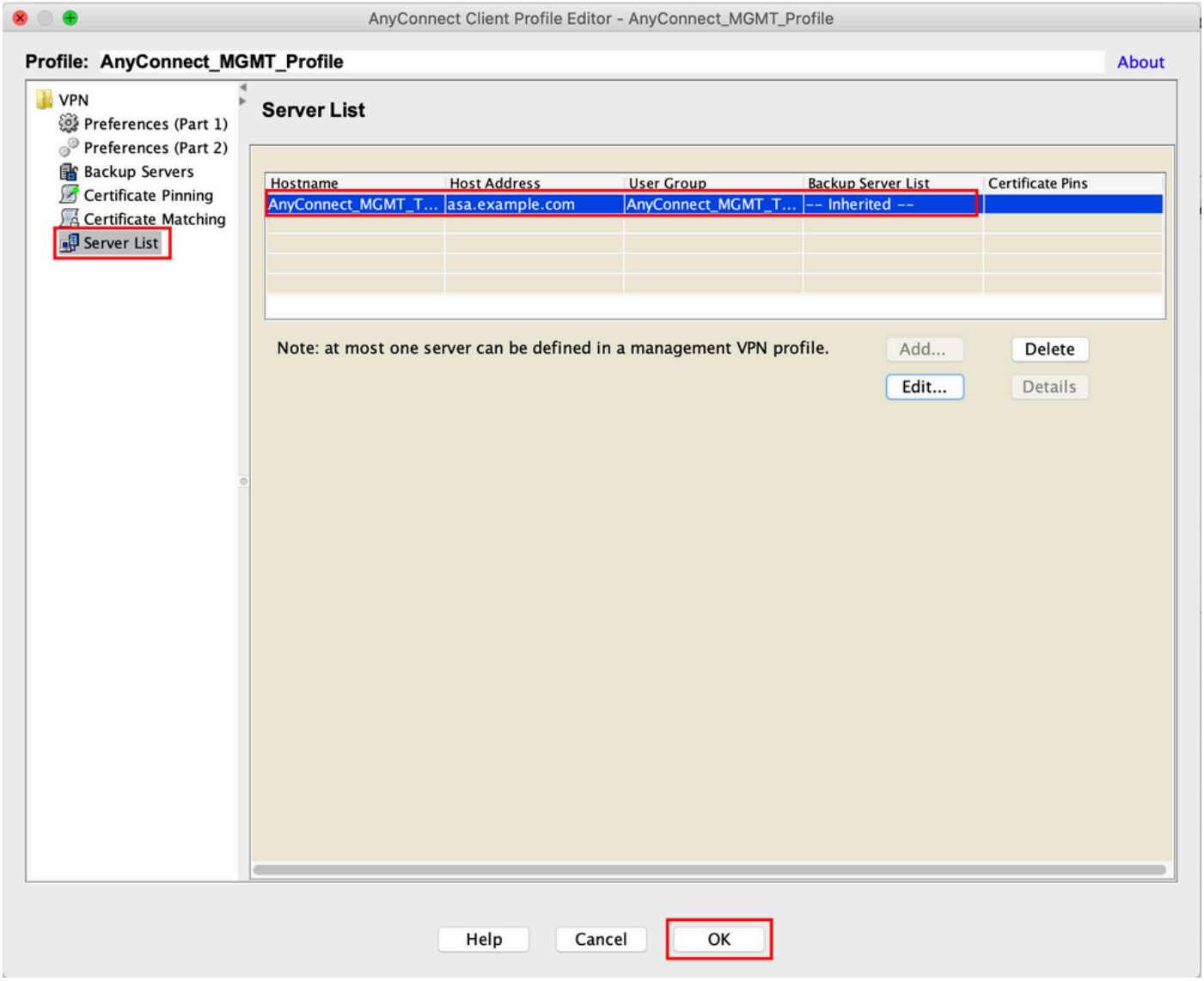
Paso 5. Proporcionar una Display Name. Agregue el FQDN/IP address del ASA. Proporcione la User Group como el nombre del grupo de túnel. Group URL se rellena automáticamente con el FQDN y User Group. Haga clic en OK.



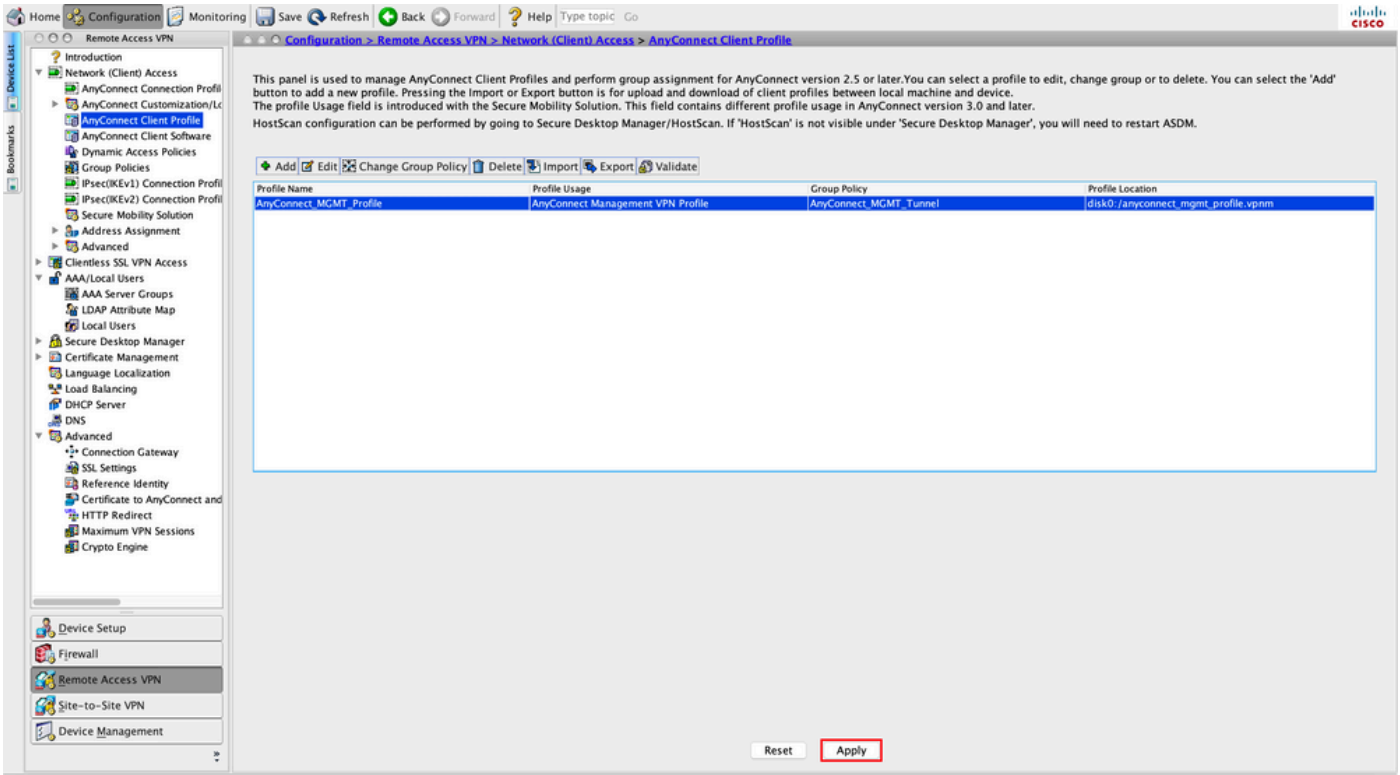
Nota: El FQDN, la dirección IP y el grupo de usuarios deben ser los mismos que la URL del grupo mencionada durante la configuración del perfil de conexión de AnyConnect en el paso 8.

Nota: AnyConnect con IKEv2 como protocolo también se puede utilizar para establecer una VPN de administración a ASA. Garantizar Primary Protocol se establece en IPsec en el paso 5.

Paso 6. Como se muestra en la imagen, haga clic en OK para guardar.



Paso 7. Haga clic en Apply tPara enviar la configuración al ASA, como se muestra en la imagen.



Configuración CLI tras la adición del perfil VPN de administración de AnyConnect.

```
webvpn
 enable outside
 hsts
  enable
  max-age 31536000
  include-sub-domains
  no preload
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
!
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-network-list value VPN-Split
 client-bypass-protocol enable
 address-pools value VPN_Pool
 webvpn
  anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

Perfil VPN de administración de AnyConnect en el equipo cliente de AnyConnect:

```
<?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="false">false</UseStartBeforeLogon>




        <ShowPreConnectMessage>false</ShowPreConnectMessage>




        <ProxySettings>IgnoreProxy</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>30</AuthenticationTimeout>

--- Output Omitted ---
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>false</AllowManualHostInput> </ClientInitialization>
```

```
</AnyConnectProfile>
```

Nota: Si se utiliza la detección de redes de confianza (TND) en el perfil VPN de AnyConnect del usuario, se recomienda que coincida con la misma configuración en el perfil VPN de gestión para que la experiencia del usuario sea coherente. El túnel VPN de administración se activa en función de la configuración de TND aplicada al perfil de túnel VPN de usuario. Además, la acción TND Connect en el perfil VPN de gestión (aplicada solo cuando el túnel VPN de gestión está activo), siempre se aplica al túnel VPN de usuario, para garantizar que el túnel VPN de gestión sea transparente para el usuario final.

Nota: En cualquier PC de usuario final, si el perfil VPN de gestión tiene la configuración de TND activada y falta el perfil VPN de usuario, tendrá en cuenta la configuración de preferencias predeterminada para TND (está desactivada en las preferencias predeterminadas de la aplicación cliente de CA) en lugar de perder el perfil VPN de usuario. Esta discordancia puede llevar a un comportamiento inesperado/indefinido.
De forma predeterminada, la configuración de TND está desactivada en las preferencias predeterminadas.
Para superar las preferencias predeterminadas y la configuración codificada en la aplicación AnyConnect Client, el equipo del usuario final debe tener dos perfiles VPN, un perfil VPN de usuario y un perfil VPN de administración de CA, y ambos deben tener la misma configuración TND.
La lógica detrás de la conexión y desconexión del túnel VPN de administración es que para establecer un túnel VPN de administración, el agente de CA utiliza la configuración de TND del perfil VPN del usuario y, para la desconexión del túnel VPN de administración, comprueba la configuración de TND del perfil VPN de administración.

Métodos de implementación para el perfil VPN de administración de AnyConnect

- Una conexión VPN de usuario exitosa se completa con el perfil de conexión de ASA para descargar el perfil VPN de administración de AnyConnect del gateway VPN.

  Nota: Si el protocolo utilizado para el túnel VPN de administración es IKEv2, la primera conexión debe establecerse a través de SSL (para descargar el perfil VPN de administración de AnyConnect del ASA).

- El perfil VPN de administración de AnyConnect se puede cargar manualmente en los equipos cliente mediante una inserción de GPO o mediante una instalación manual (asegúrese de que el nombre del perfil sea `VpnMgmtTunProfile.xml`).

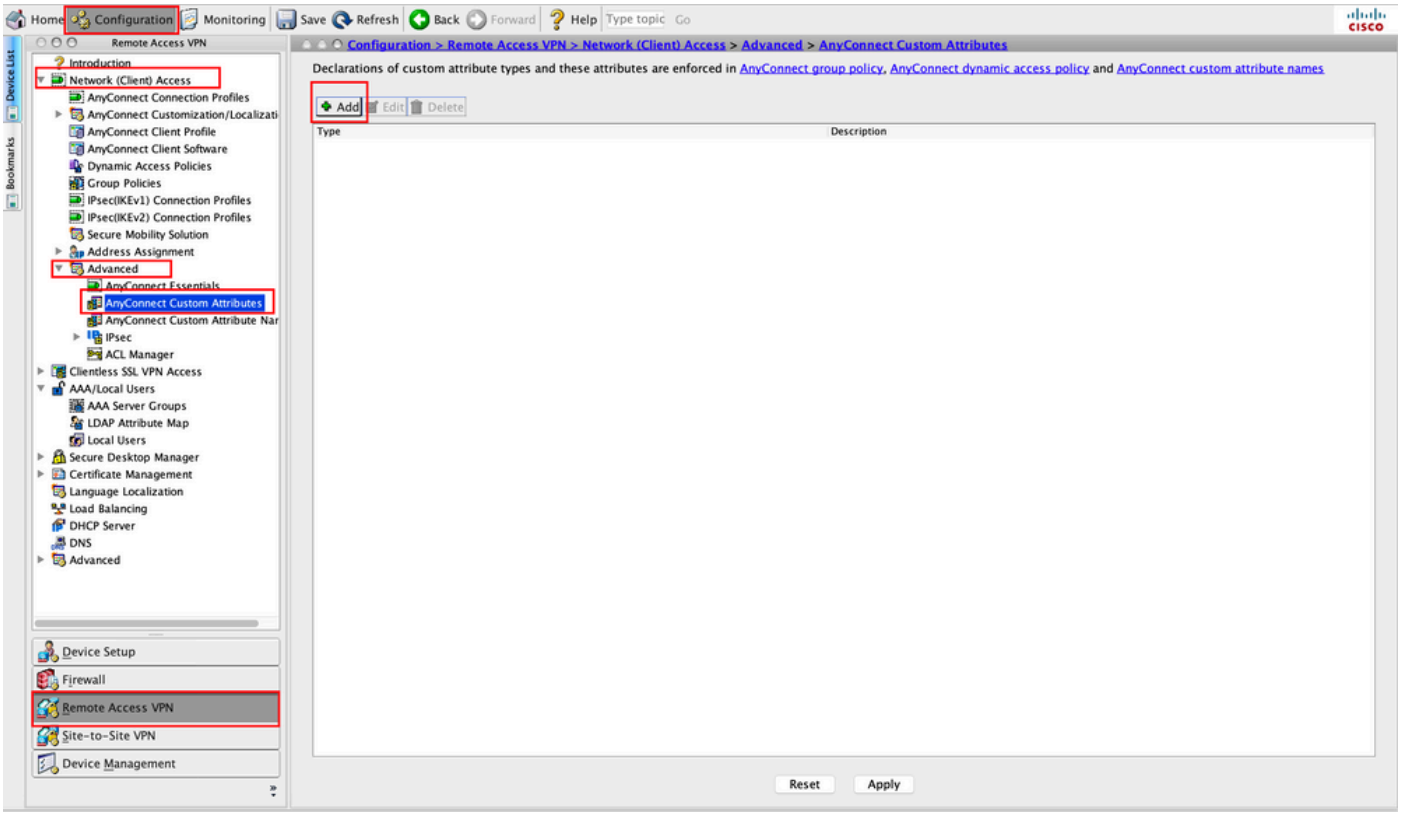
  Ubicación de la carpeta donde se debe agregar el perfil:
  Windows: **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**
  macOS: /opt/cisco/anyconnect/profile/mgmttun/

(Opcional) Configuración de un Atributo Personalizado para Soportar la Configuración de Túnel Todo

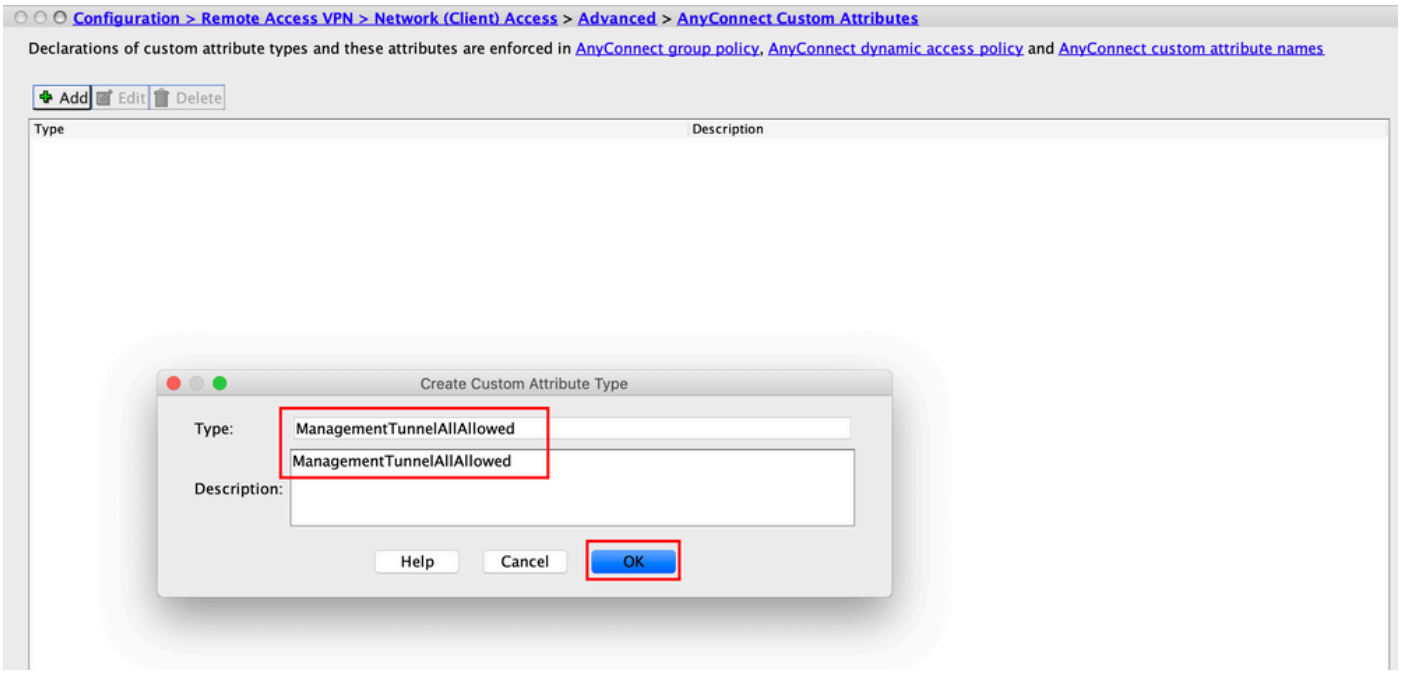
El túnel VPN de administración requiere una división que incluya la configuración de la tunelización, de forma predeterminada, para evitar un impacto en la comunicación de red iniciada por el usuario. Esto se puede anular al configurar el atributo personalizado en la directiva de

grupo utilizada por la conexión del túnel de administración.

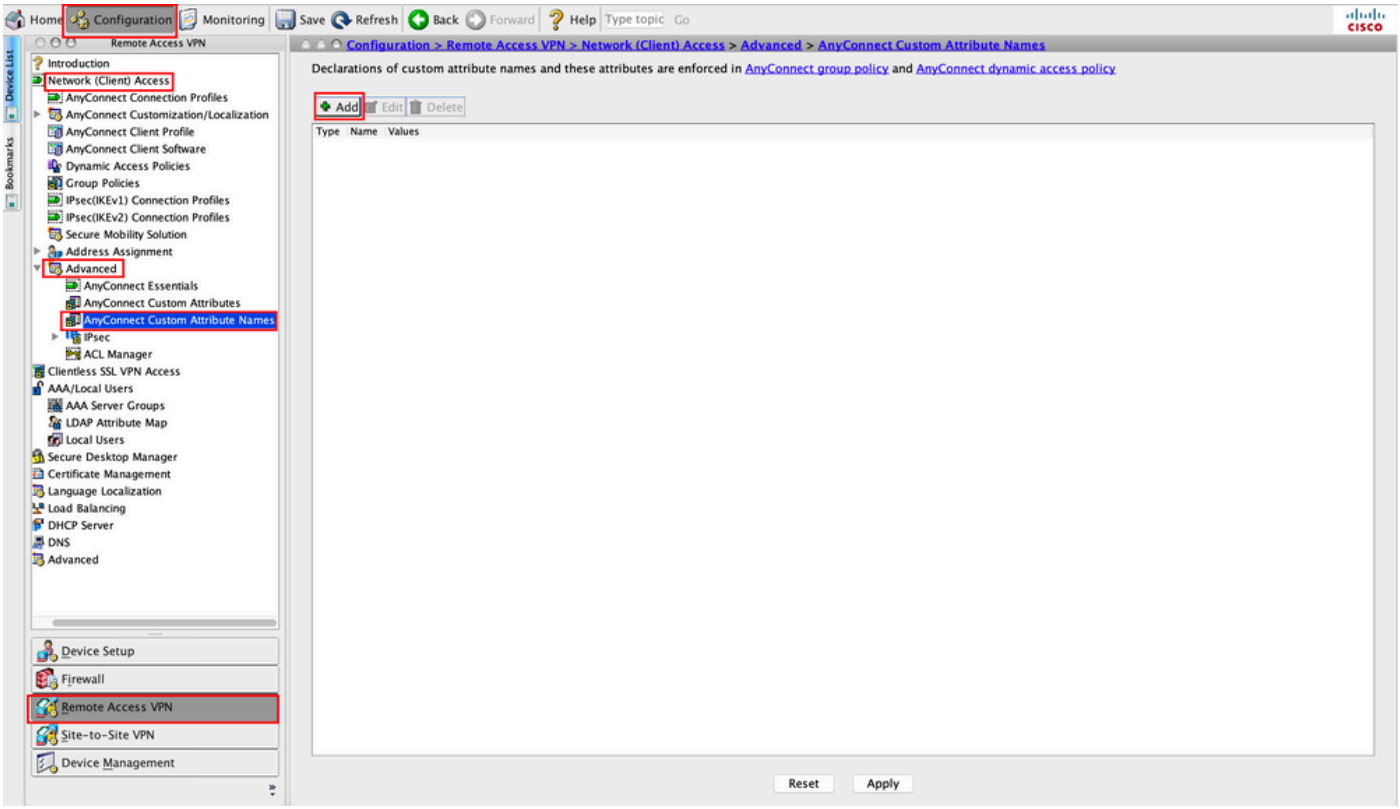
Paso 1. Desplácese hasta Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. Haga clic en Add, como se muestra en la imagen.



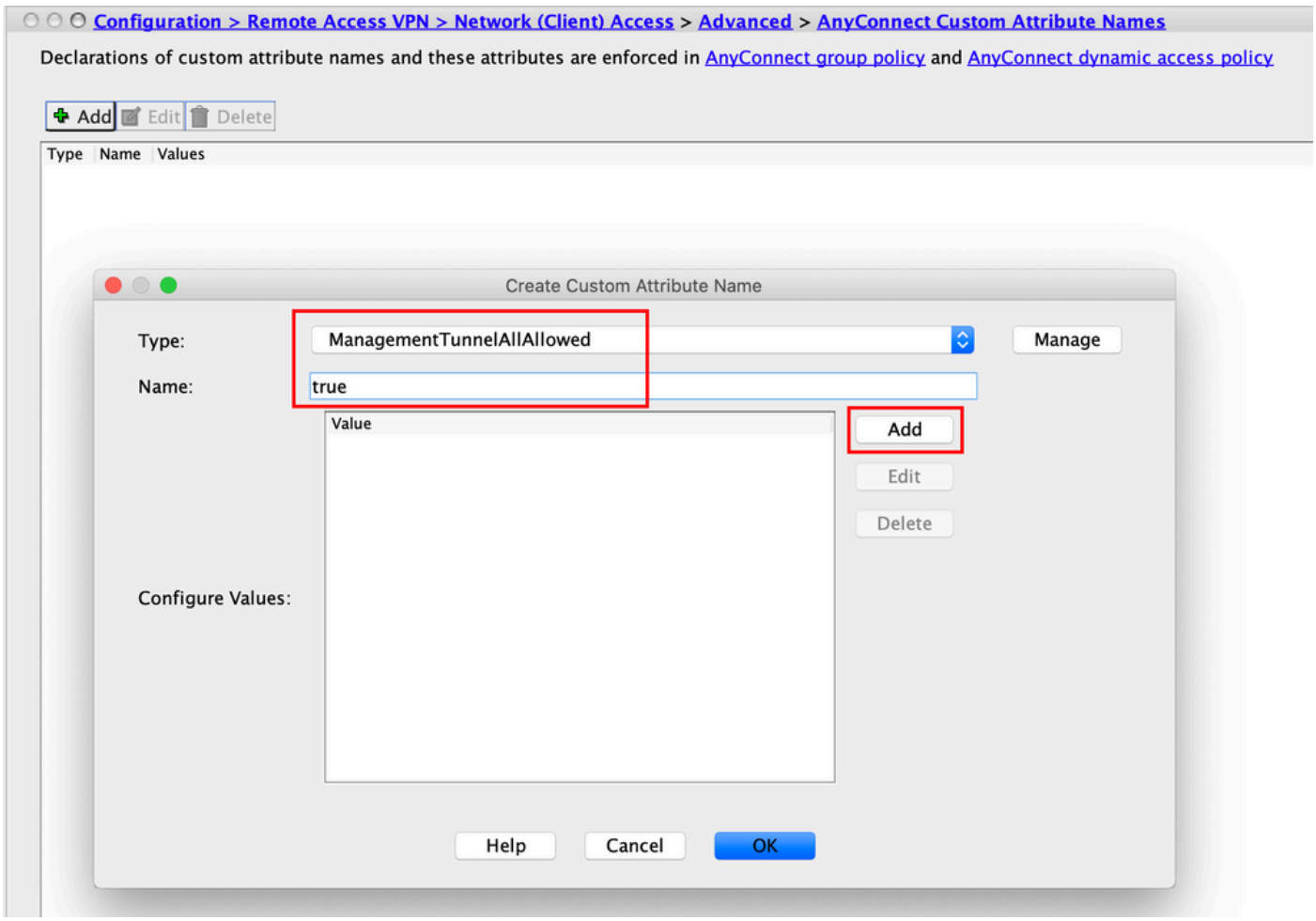
Paso 2. Establezca el tipo de atributo personalizado en ManagementTunnelAllAllowed y proporcionar una Description. Haga clic en OK, como se muestra en la imagen.



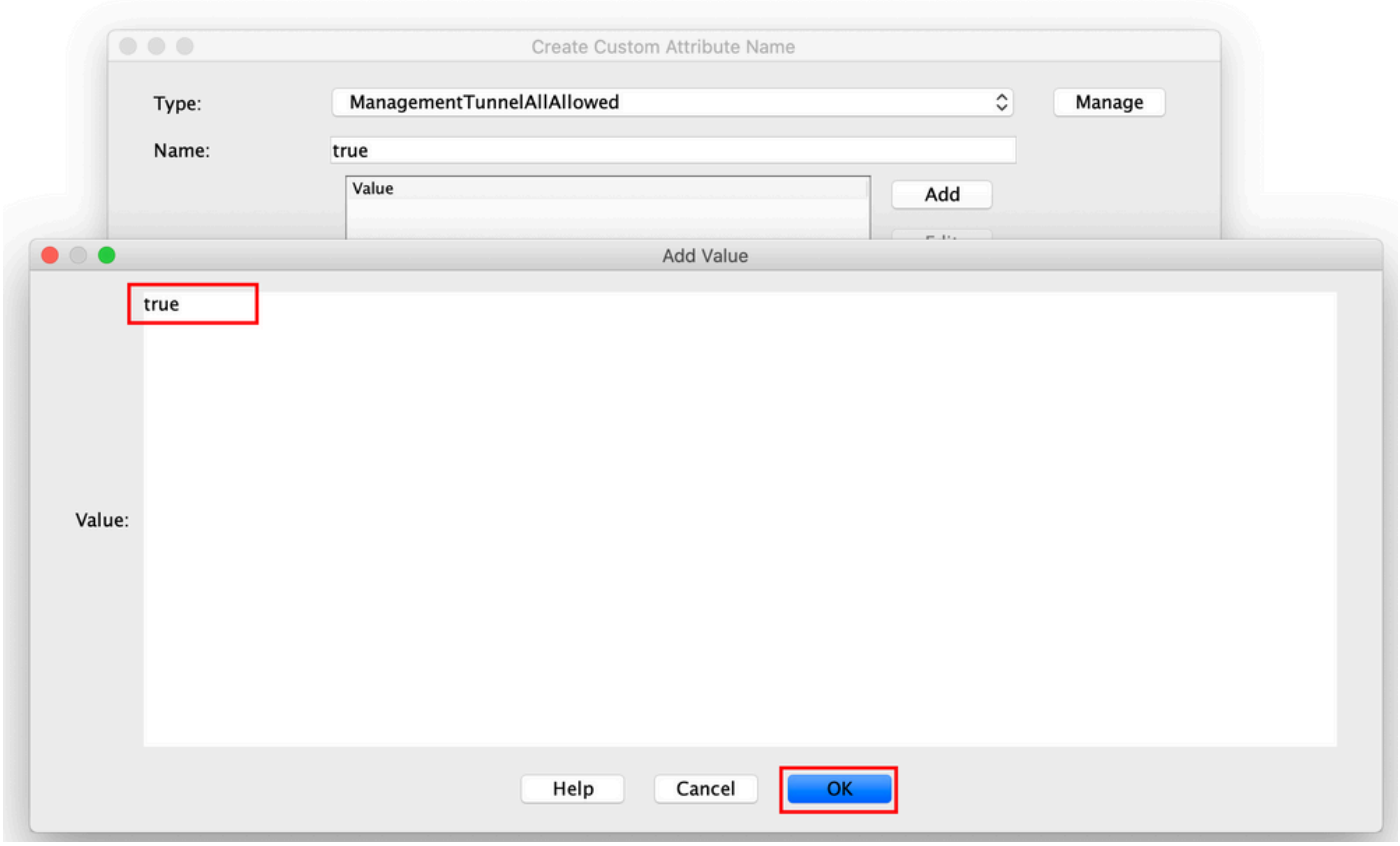
Paso 3. Desplácese hasta **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names.** Haga clic en Add, como se muestra en la imagen.



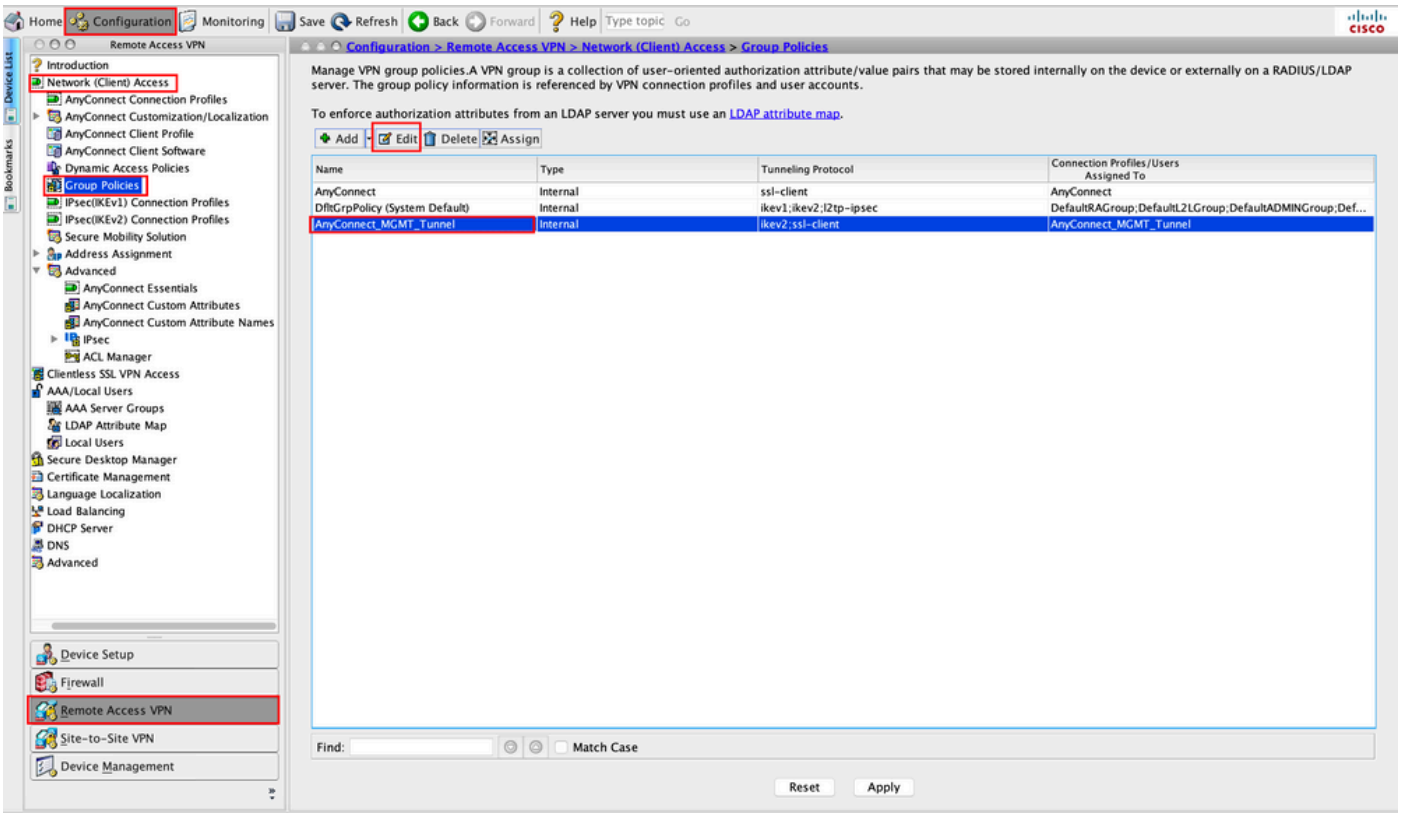
Paso 4. Elija el tipo como **ManagementTunnelAllAllowed** . Establezca el Nombre como true. Haga clic en Addpara proporcionar un valor de atributo personalizado, como se muestra en la imagen.



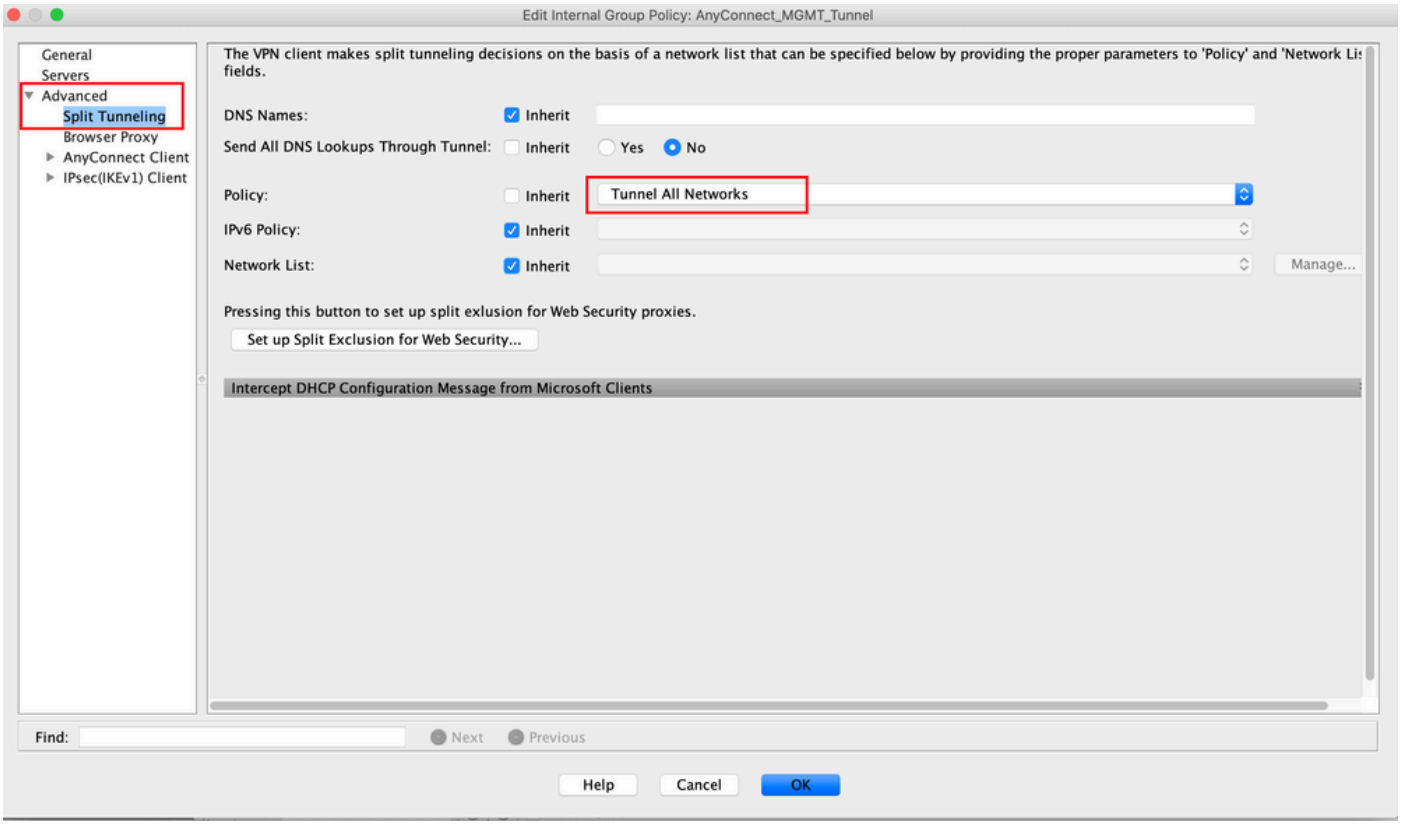
Paso 5. Establezca el valor como true. Haga clic en **OK**, como se muestra en la imagen.



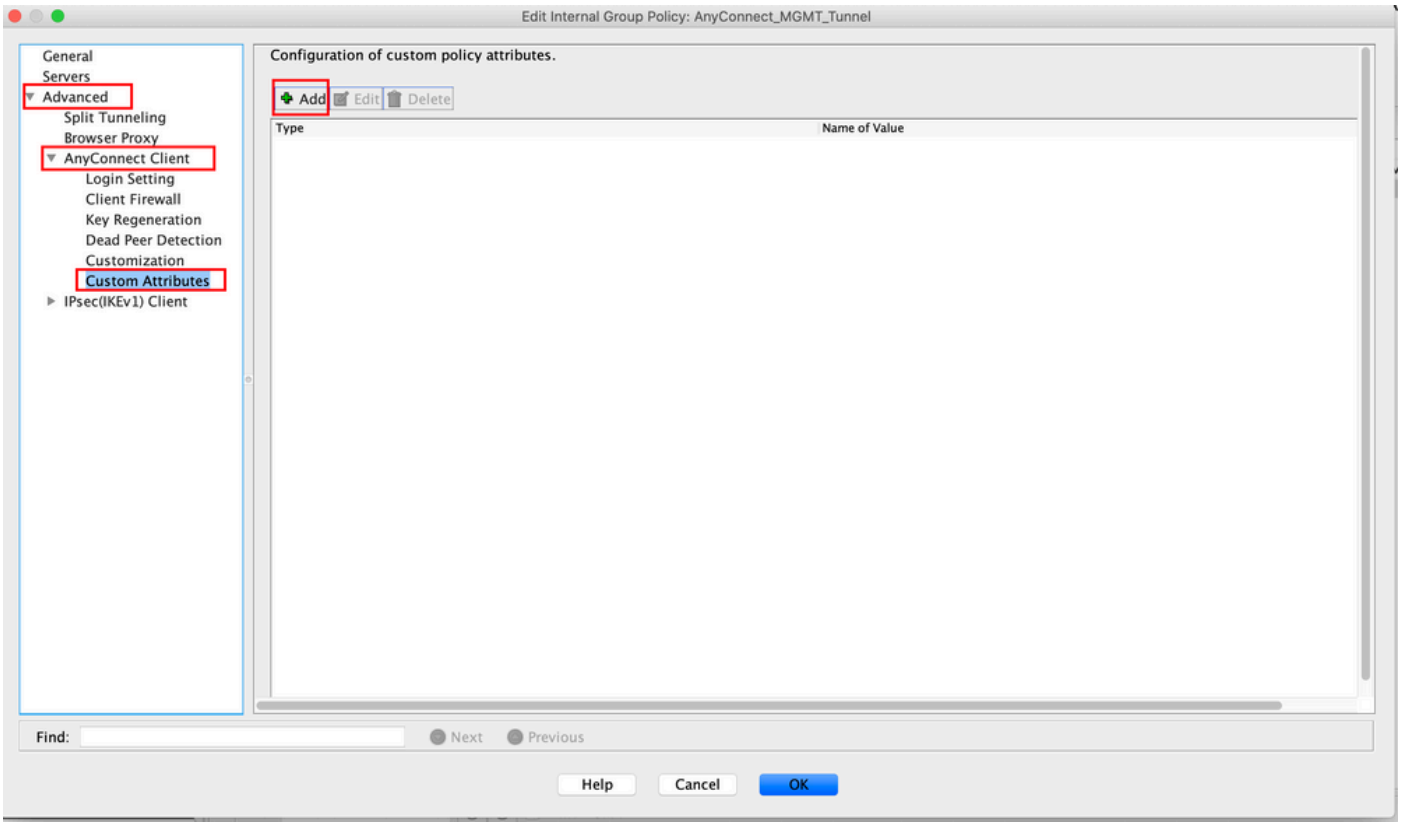
Paso 6. Desplácese hasta Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Elija la directiva de grupo. Haga clic en Edit , como se muestra en la imagen.



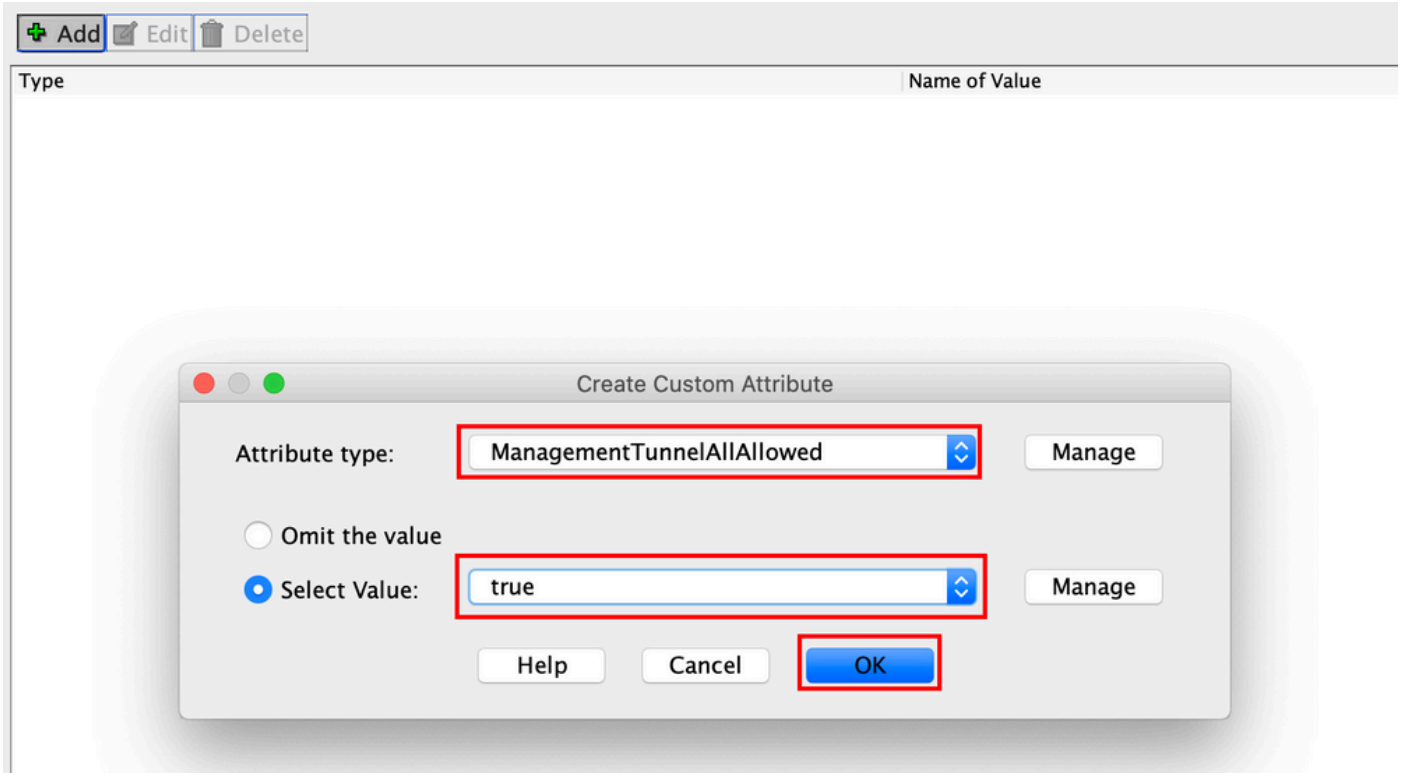
Paso 7. Como se muestra en esta imagen, navegue hasta Advanced > Split Tunneling. Configure la política como Tunnel All Networks.



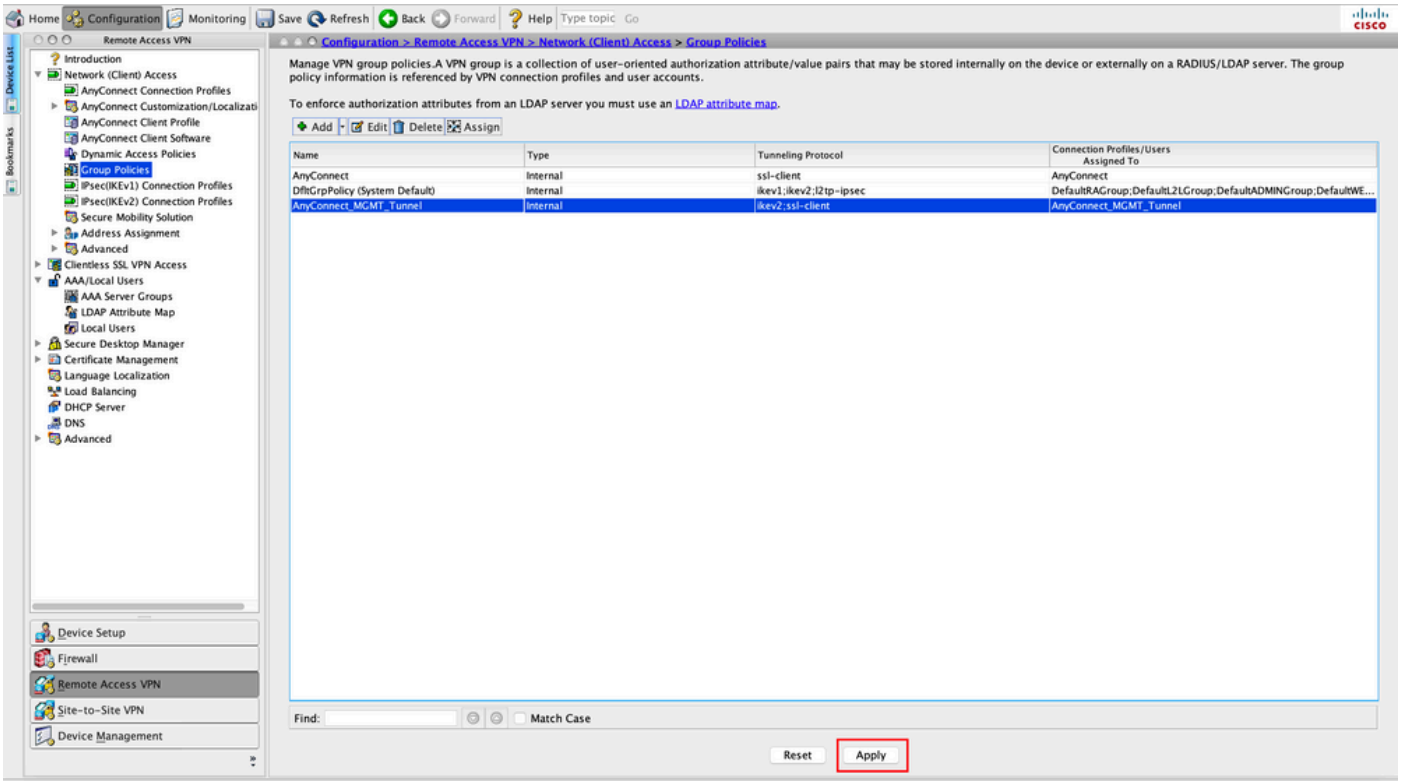
Paso 8. Desplácese hasta Advanced > Anyconnect Client > Custom Attributes. Haga clic en Add, como se muestra en la imagen.



Paso 9. Elija el tipo de atributo como ManagementTunnelAllAllowed y seleccione el valor como true. Haga clic en OK, como se muestra en la imagen.



Paso 10. Haga clic en Apply para enviar la configuración al ASA, como se muestra en la imagen.



Configuración de CLI después de la ManagementTunnelAllAllowed Se agrega el atributo personalizado:

```
webvpn
 enable outside
 anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
 hsts
  enable
  max-age 31536000
```

```
  include-sub-domains
  no preload
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
 anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
!
anyconnect-custom-data ManagementTunnelAllAllowed true true
!
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelall
 client-bypass-protocol enable
 address-pools value VPN_Pool
 anyconnect-custom ManagementTunnelAllAllowed value true
 webvpn
  anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

Verificación

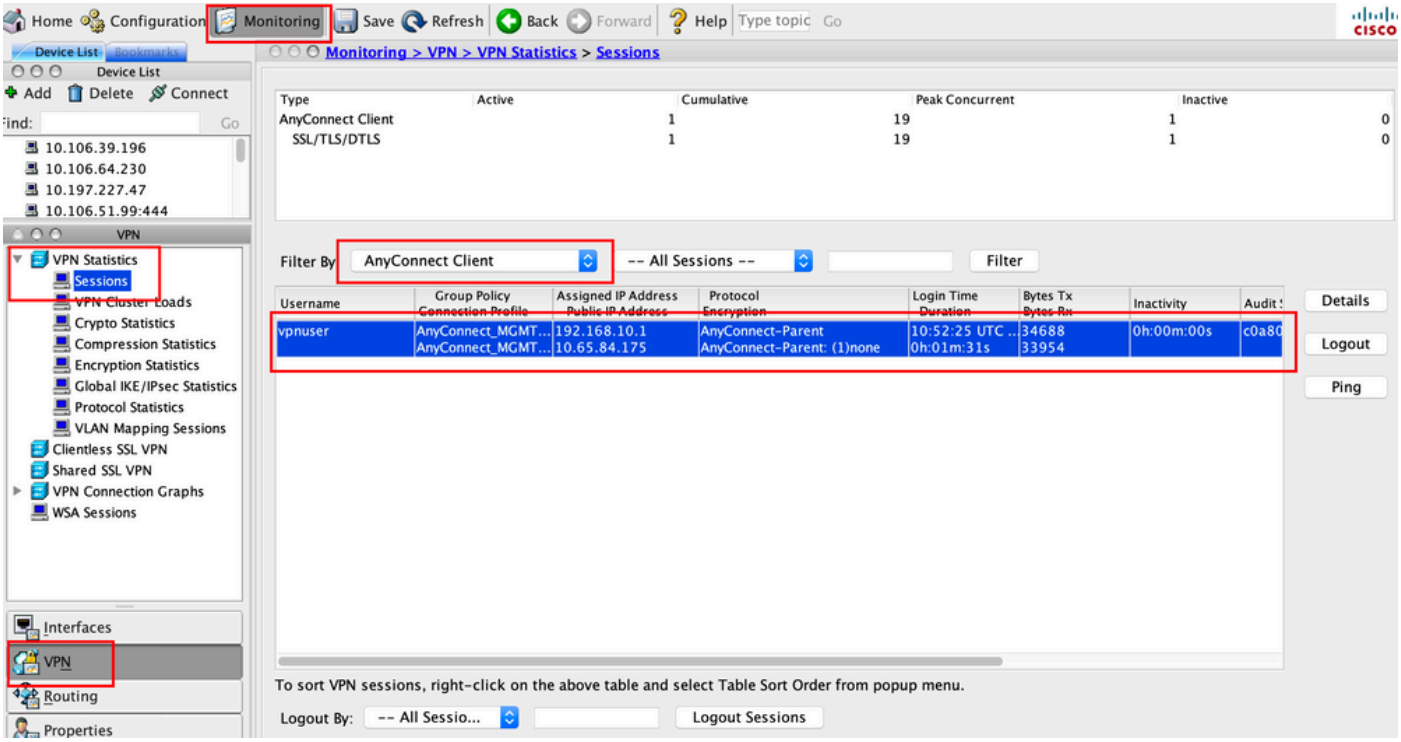
Verifique la conexión del túnel de administración VPN en la CLI de ASA con el show vpn-sessiondb detail anyconnect comando.

```
ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : vpnuser                Index        : 10
Assigned IP  : 192.168.10.1           Public IP    : 10.65.84.175
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-
256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 17238                  Bytes Rx     : 1988
Pkts Tx      : 12                     Pkts Rx      : 13
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : AnyConnect_MGMT_Tunnel Tunnel Group : AnyConnect_MGMT_Tunnel
Login Time   : 01:23:55 UTC Tue Apr 14 2020
Duration     : 0h:11m:36s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a801010000a0005e9510ab
Security Grp : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

--- Output Omitted ---
DTLS-Tunnel:
  Tunnel ID    : 10.3
  Assigned IP  : 192.168.10.1           Public IP    : 10.65.84.175
  Encryption   : AES-GCM-256            Hashing      : SHA384
  Ciphersuite  : ECDHE-ECDSA-AES256-GCM-SHA384
```

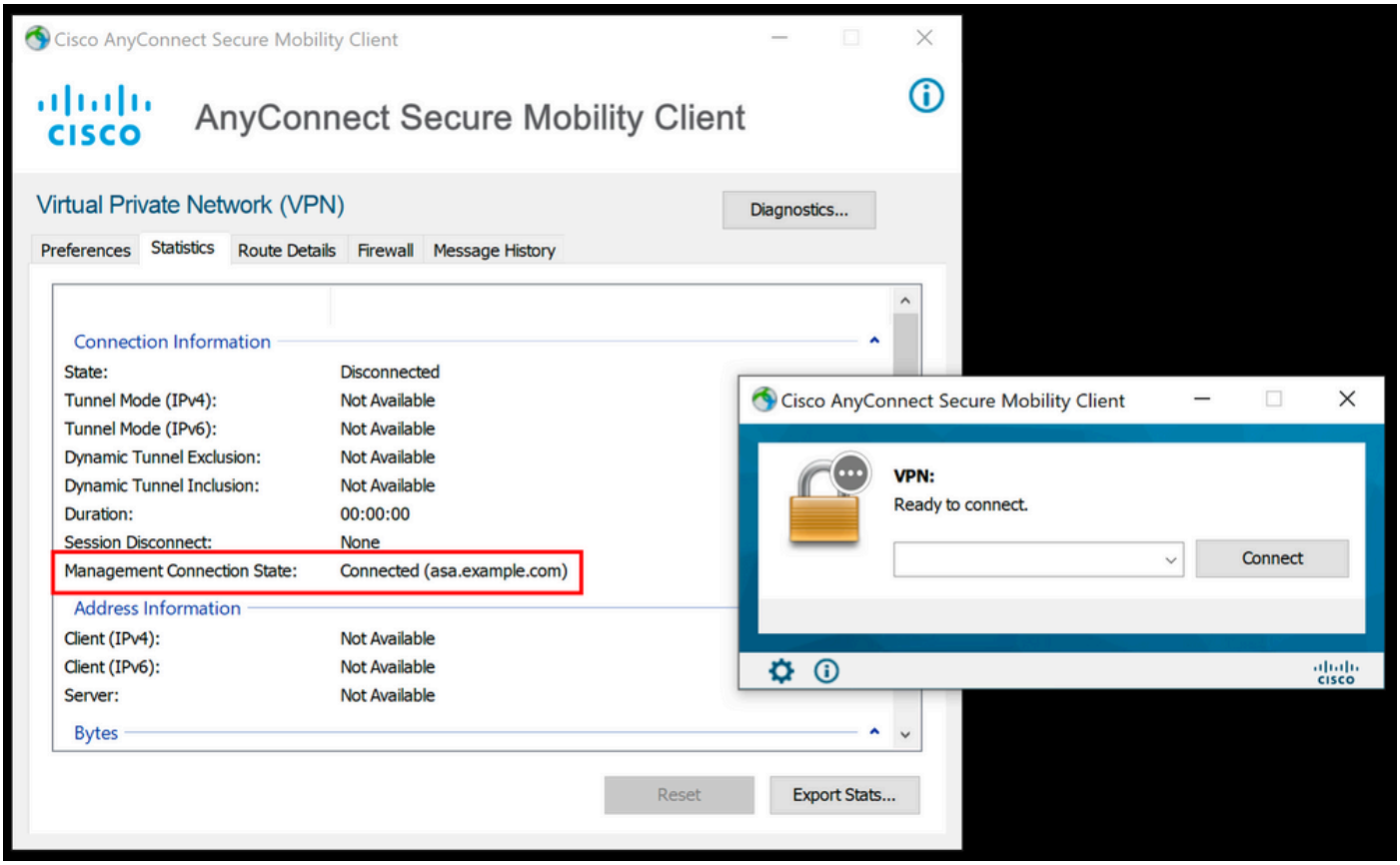
```
Encapsulation: DTLSv1.2              UDP Src Port : 57053
UDP Dst Port : 443                   Auth Mode    : Certificate
Idle Time Out: 30 Minutes            Idle TO Left : 18 Minutes
Client OS    : Windows
Client Type  : DTLS VPN Client
Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.8.03036
Bytes Tx     : 17238                 Bytes Rx     : 1988
Pkts Tx      : 12                    Pkts Rx      : 13
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
```

Verifique la conexión del túnel VPN de administración en ASDM.

Navegue hasta **Monitoring > VPN > VPN Statistics > Sessions** . Filtre por **cliente AnyConnect** para ver la sesión del cliente.



Verificación de la conexión del túnel de administración VPN en el equipo cliente:



Troubleshoot

La nueva línea de estadísticas de la interfaz de usuario (estado de conexión de administración) se puede utilizar para solucionar problemas de conectividad del túnel de administración. Estos son los estados de error más comunes:

Desconectado (deshabilitado):

- La función está desactivada.
- Asegúrese de que el perfil VPN de administración se haya implementado en el cliente, a través de la conexión de túnel de usuario (requiere que agregue el perfil VPN de administración a la política de grupo de túnel de usuario) o fuera de banda mediante la carga manual del perfil.
- Asegúrese de que el perfil VPN de administración esté configurado con una sola entrada de host que incluya un grupo de túnel.

Desconectado (red de confianza):

- TND ha detectado una red de confianza, por lo que no se ha establecido el túnel de gestión.

Desconectado (túnel de usuario activo):

- Hay un túnel VPN de usuario activo actualmente.

Desconectado (fallo al iniciar el proceso):

- Se ha producido un error en el inicio del proceso al intentar establecer la conexión del túnel

de administración.

Desconectado (fallo de conexión):

- Error de conexión al establecer el túnel de administración.
- Asegúrese de que la autenticación del certificado esté configurada en el grupo de túnel, que no haya ningún banner en la directiva de grupo y que el certificado del servidor sea de confianza.

Desconectado (configuración de VPN no válida):

- Se recibió una configuración de tunelización dividida no válida del servidor VPN.
- Verifique la configuración de tunelización dividida en la política de grupo de túnel de administración.

Desconectado (actualización de software pendiente):

- Hay una actualización de software de AnyConnect pendiente.

Desconectado:

- El túnel de gestión está a punto de establecerse o no puede establecerse por algún otro motivo.

Recopile DART para obtener más información sobre la solución de problemas.

Información Relacionada

- Configuración del Túnel VPN de Administración
- Troubleshooting del Túnel VPN de Administración
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).