Configuración de RAVPN habilitado para IPv6 con autenticación AAA en FTD administrado por FDM

Contenido

Introducción

Este documento describe los pasos para configurar VPN de acceso remoto habilitada para IPv6 con autenticación AAA en FTD administrado por FDM.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Firepower Device Manager (FDM) Virtual
- Cisco Secure Firewall Threat Defence (FTD) Virtual
- Flujo de autenticación VPN

Componentes Utilizados

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

- Cisco Secure FDM Virtual 7.6.0
- Cisco Secure FTD Virtual 7.6.0

- Cisco Secure Client 5.1.6.103

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.

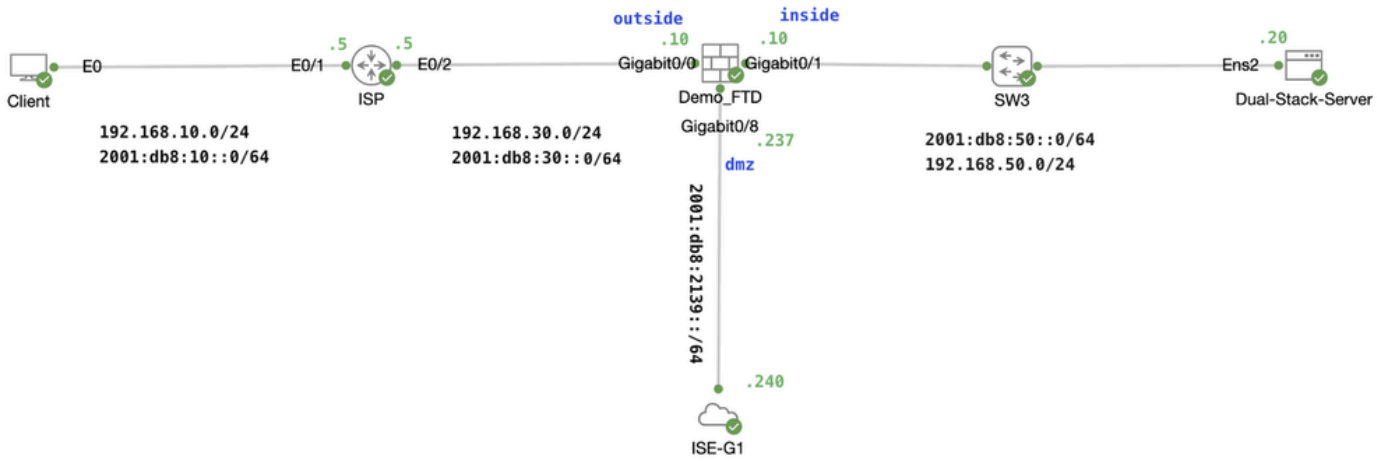
Antecedentes

La VPN de acceso remoto IPv6 (RAVPN) es cada vez más importante a medida que el mundo pasa de IPv4 a IPv6, ya que las direcciones IPv4 son limitadas y casi se han agotado, mientras que IPv6 ofrece un espacio de direcciones prácticamente ilimitado, que se adapta al creciente número de dispositivos conectados a Internet. A medida que más redes y servicios pasan a IPv6, disponer de capacidad IPv6 garantiza que su red siga siendo compatible y accesible. RAVPN IPv6 ayuda a las organizaciones a prepararse para el futuro de las redes, lo que garantiza una conectividad remota segura y escalable.

En este ejemplo, el cliente se comunica con el gateway VPN mediante una dirección IPv6 proporcionada por el proveedor de servicios, pero recibe las direcciones IPv4 e IPv6 de los grupos VPN, utilizando Cisco Identity Service Engine (ISE) como fuente de identidad de autenticación. ISE se configura solo con direcciones IPv6. El servidor interno se configura con direcciones IPv4 e IPv6, que representan hosts de pila doble. El cliente puede acceder a los recursos internos mediante la dirección VPN IPv4 o IPv6, según corresponda.

Configurar

Diagrama de la red

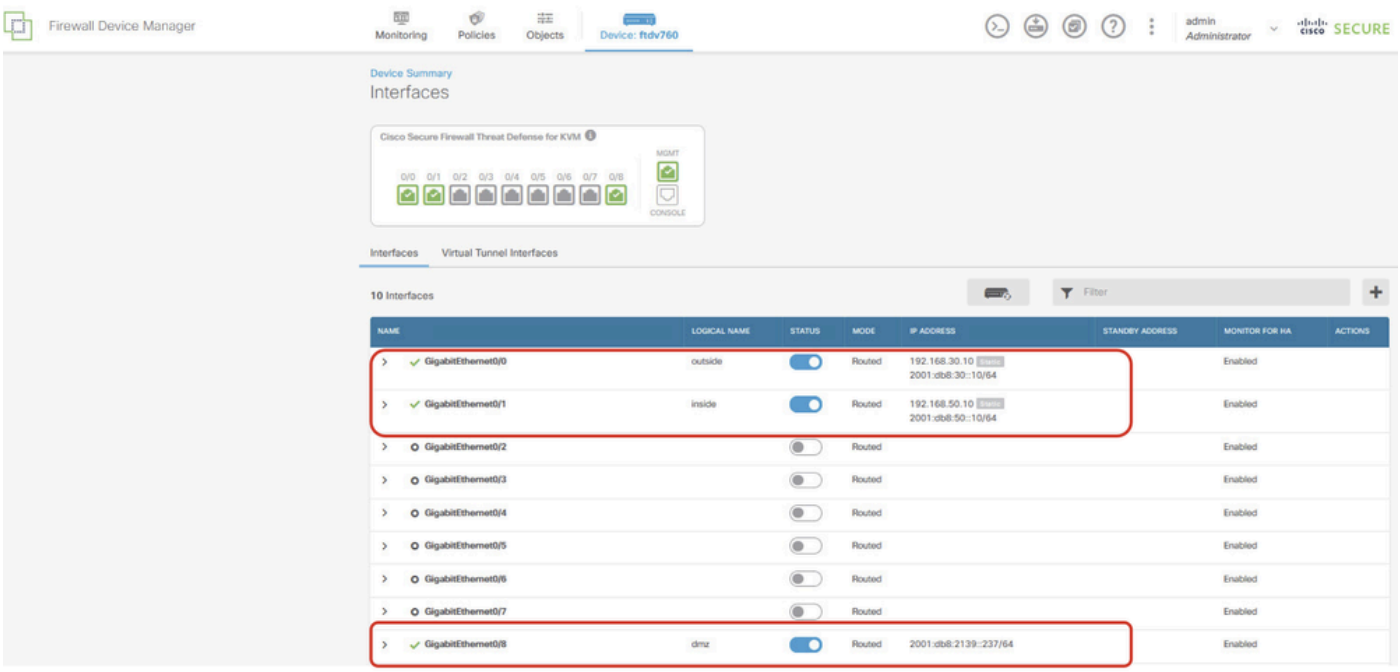


Topología

Configuraciones en FDM

Paso 1. Es esencial garantizar que la configuración preliminar de la interconexión IPv4 e IPv6

entre nodos se haya completado debidamente. La puerta de enlace del cliente y FTD es la dirección ISP relacionada. El gateway del servidor está dentro de la IP del FTD. ISE se encuentra en el área DMZ del FTD.

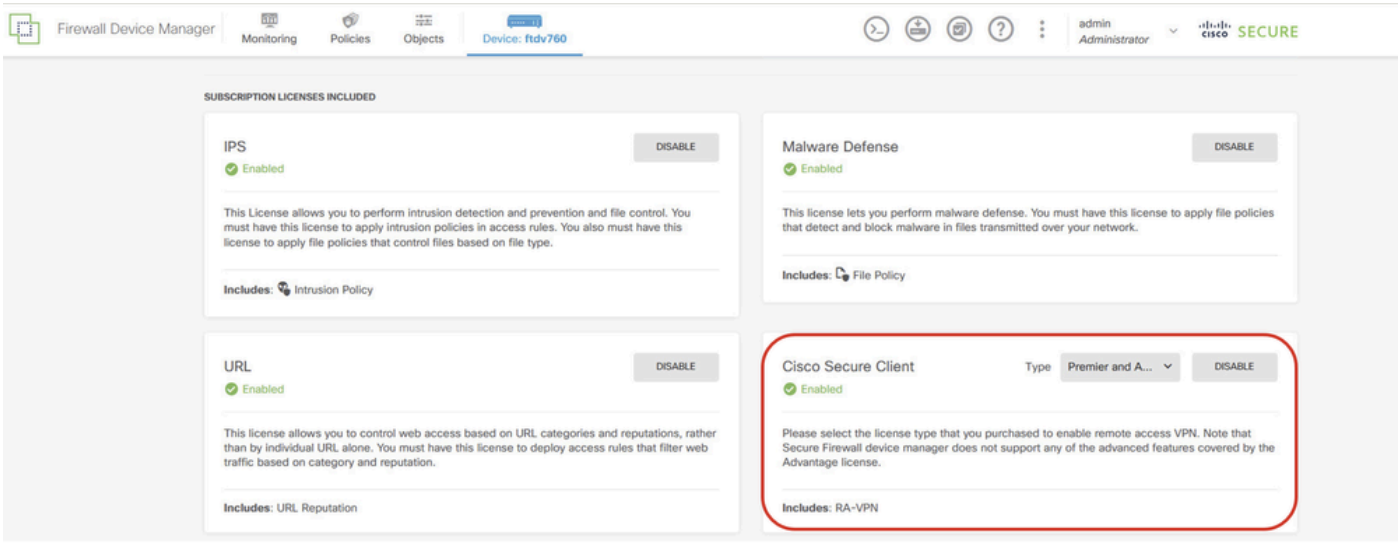


FTD_Interface_IP

FTD_Default_Route

Paso 2. Descargue el paquete de Cisco Secure Client llamado cisco-secure-client-win-5.1.6.103-webdeploy-k9.pkg de Cisco Software Download y asegúrese de que el archivo sea bueno después de la descarga confirmando que la suma de comprobación md5 del archivo descargado es la misma que la página de descarga de software de Cisco.

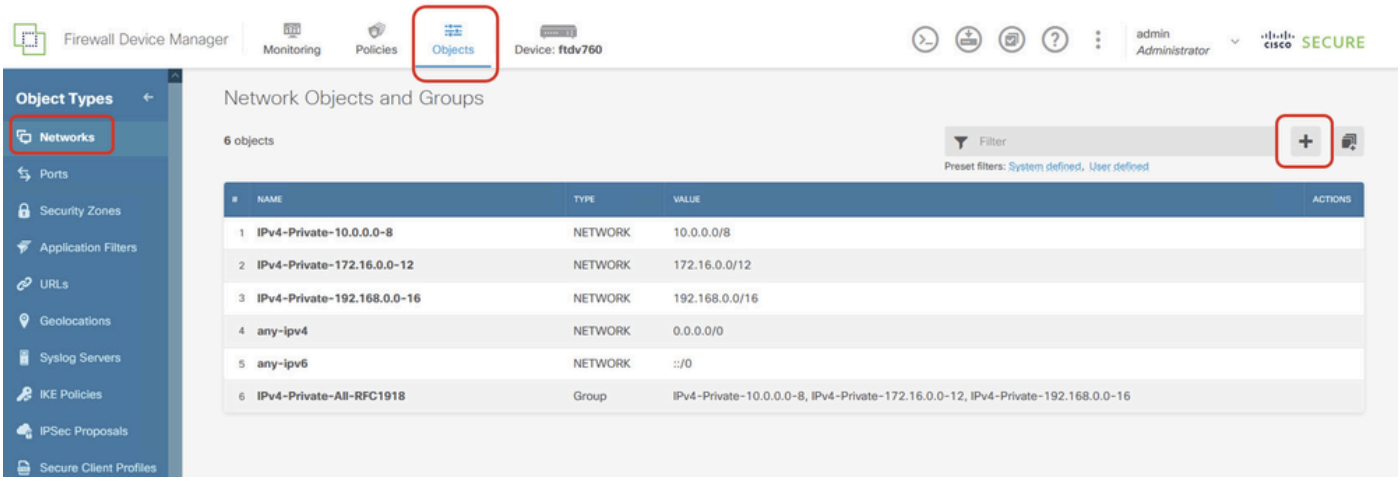
Paso 3. Verifique que las licencias relacionadas con RAVPN estén habilitadas en FTD.



Licencia_FDM

Paso 4. Crear conjunto de direcciones VPN.

Paso 4.1. Cree un pool de direcciones IPv6 e IPv4 creando objetos de red. Navegue hasta Objetos > Redes y haga clic en el botón +.

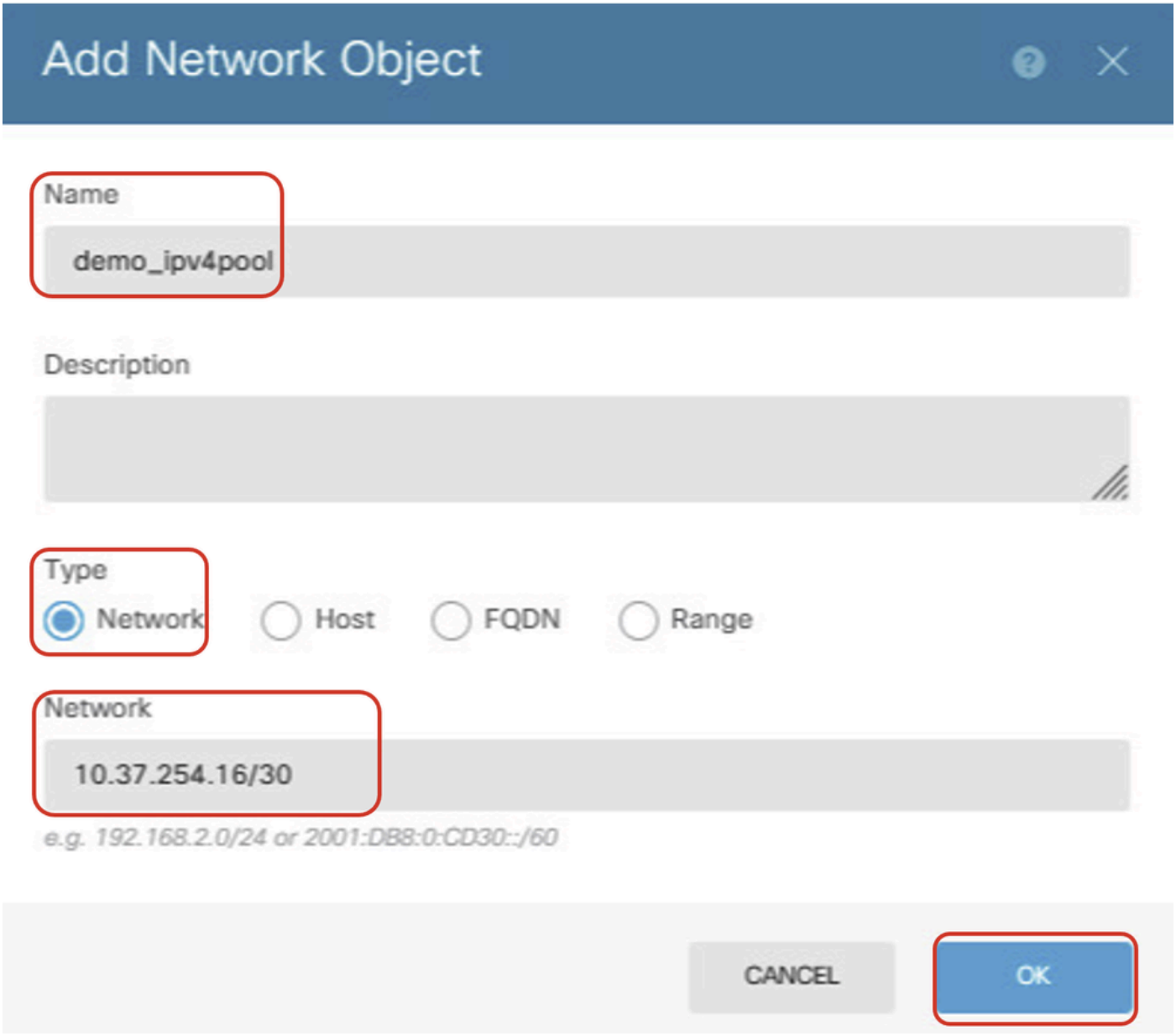


Create_VPN_Address_Pool_1

Paso 4.2. Proporcione la información necesaria de cada objeto de red. Haga clic en el botónAceptar.

Para el grupo IPv4, el tipo de objeto se puede seleccionar con Red o Rango. En este ejemplo, el tipo de objeto Red se elige para fines de demostración.

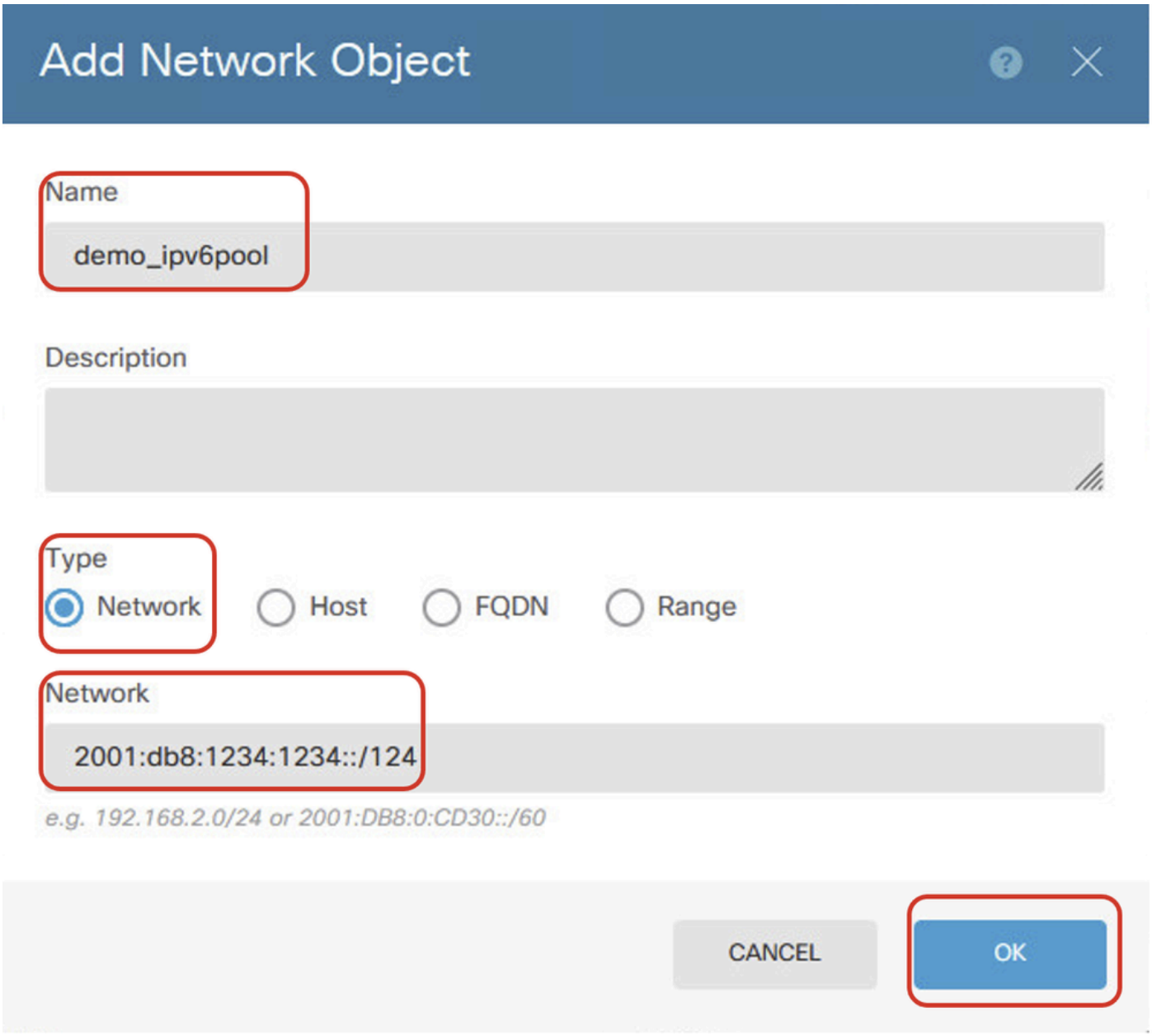
- Nombre: demo_ipv4pool
- Tipo: Red
- Red: 10.37.254.16/30



Create_VPN_Address_Pool_2_IPv4

Para el grupo IPv6, el tipo de objeto solo se puede seleccionar con Red en este momento.

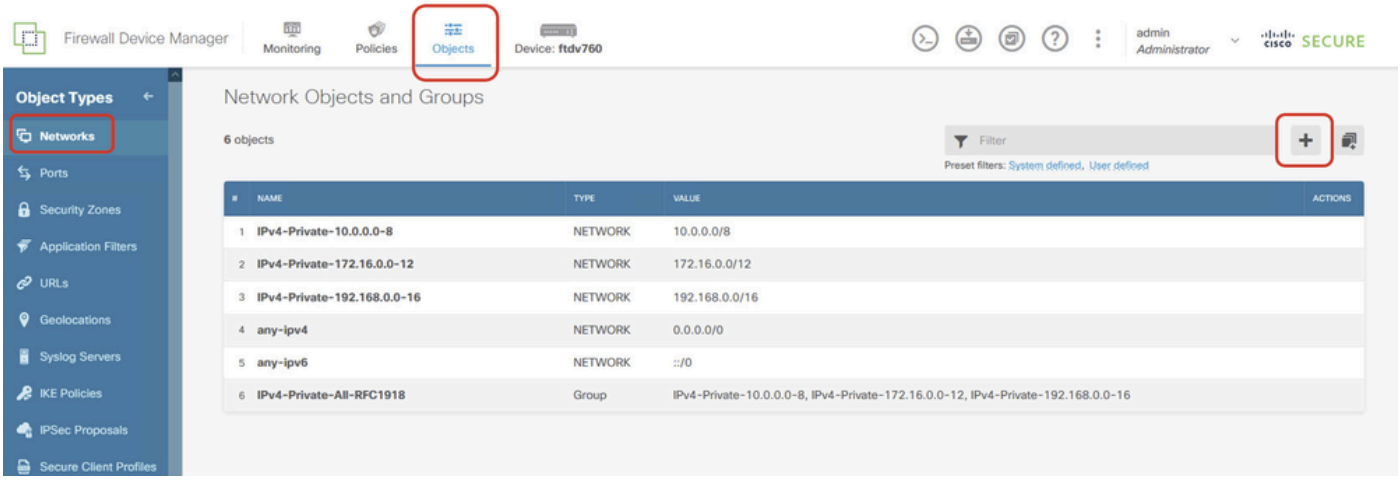
- Nombre: demo_ipv6pool
- Tipo: Red
- Red: 2001:db8:1234:1234::/124



Create_VPN_Address_Pool_2_IPv6

Paso 5. Crear la red interna para NAT exenta.

Paso 5.1. Navegue hasta Objetos > Redes y haga clic en el botón +.

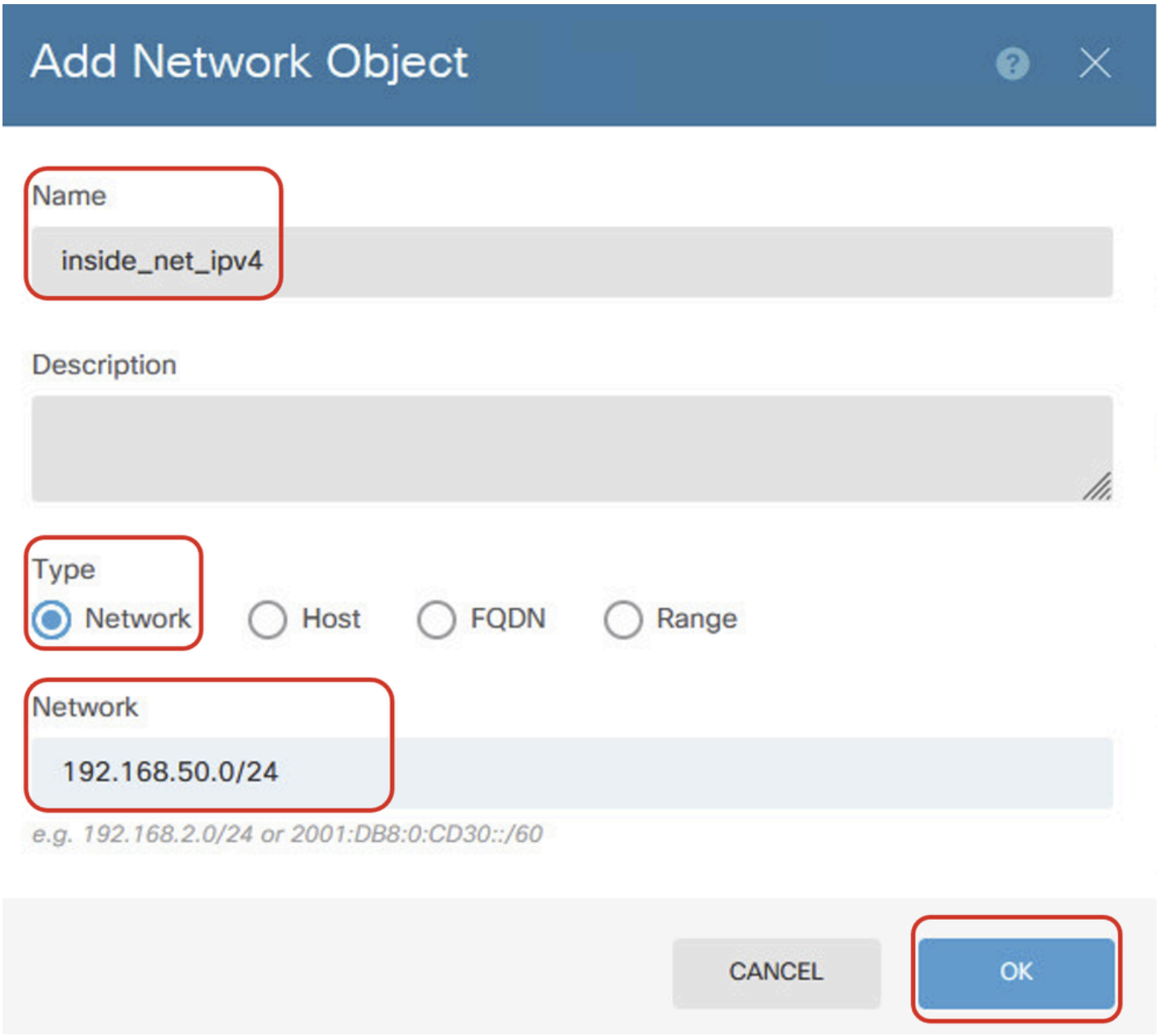


Create_NAT_Exempt_Network_1

Paso 5.2. Proporcione la información necesaria de cada objeto de red. Haga clic en el botón OK (Aceptar)

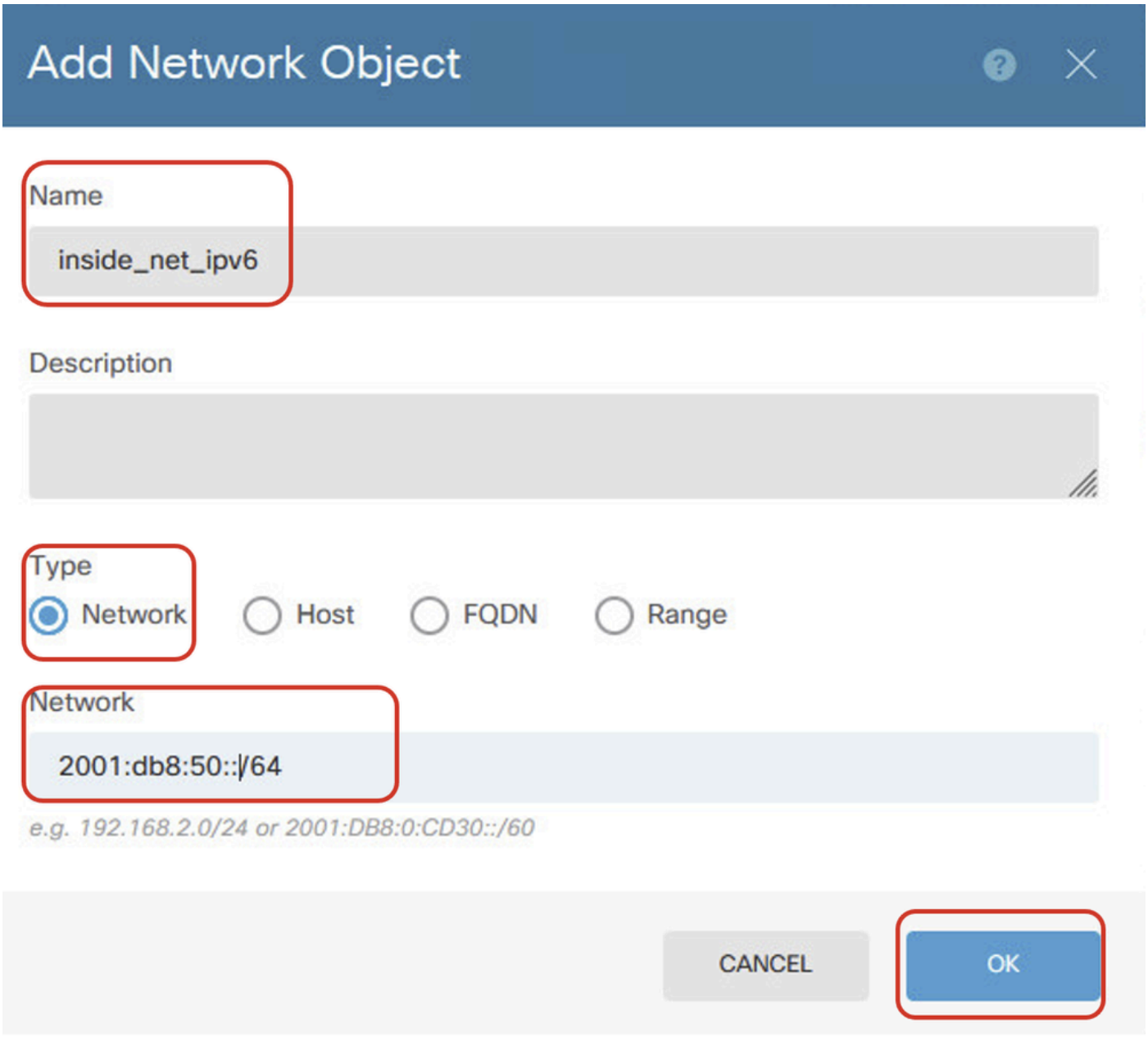
En este ejemplo, se configuran las redes IPv4 e IPv6.

- Nombre: inside_net_ipv4
- Tipo: Red
- Red: 192.168.50.0/24



Create_NAT_Exempt_Network_2_IPv4

- Nombre: inside_net_ipv6
- Tipo: Red
- Red: 2001:db8:50::/64

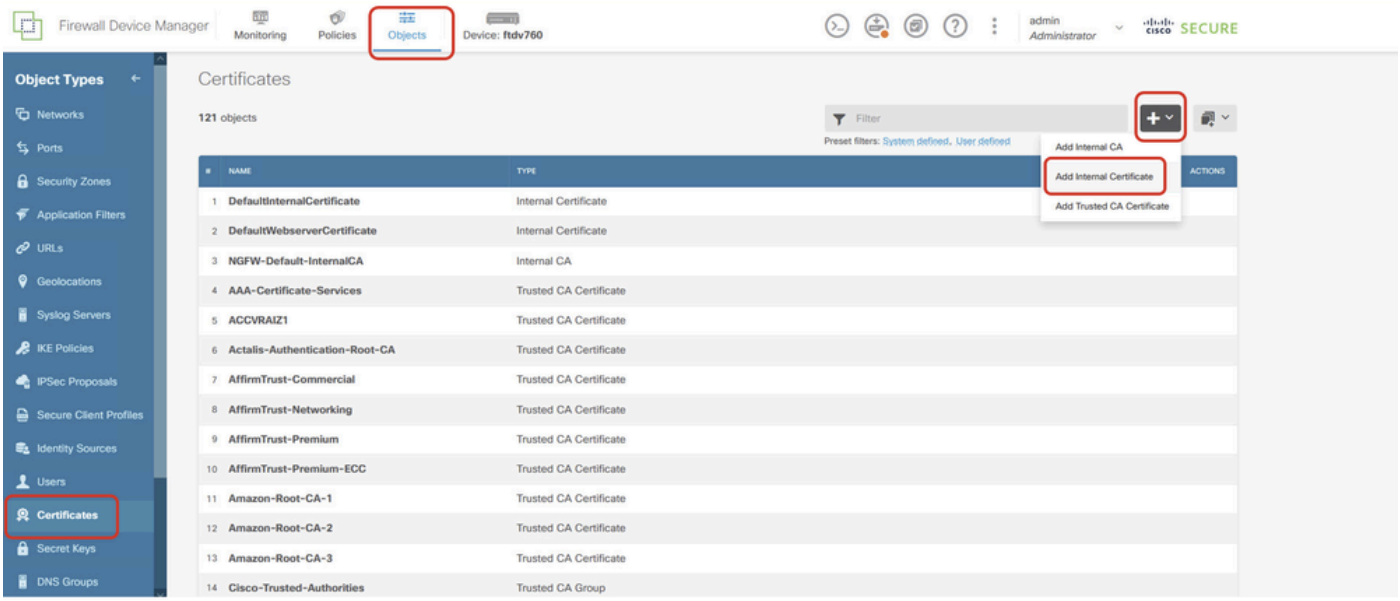


Create_NAT_Exempt_Network_2_IPv6

Paso 6. Cree el certificado utilizado para RAVPN. Tiene dos opciones: puede cargar un certificado firmado por una entidad emisora de certificados (CA) de terceros o generar un nuevo certificado autofirmado.

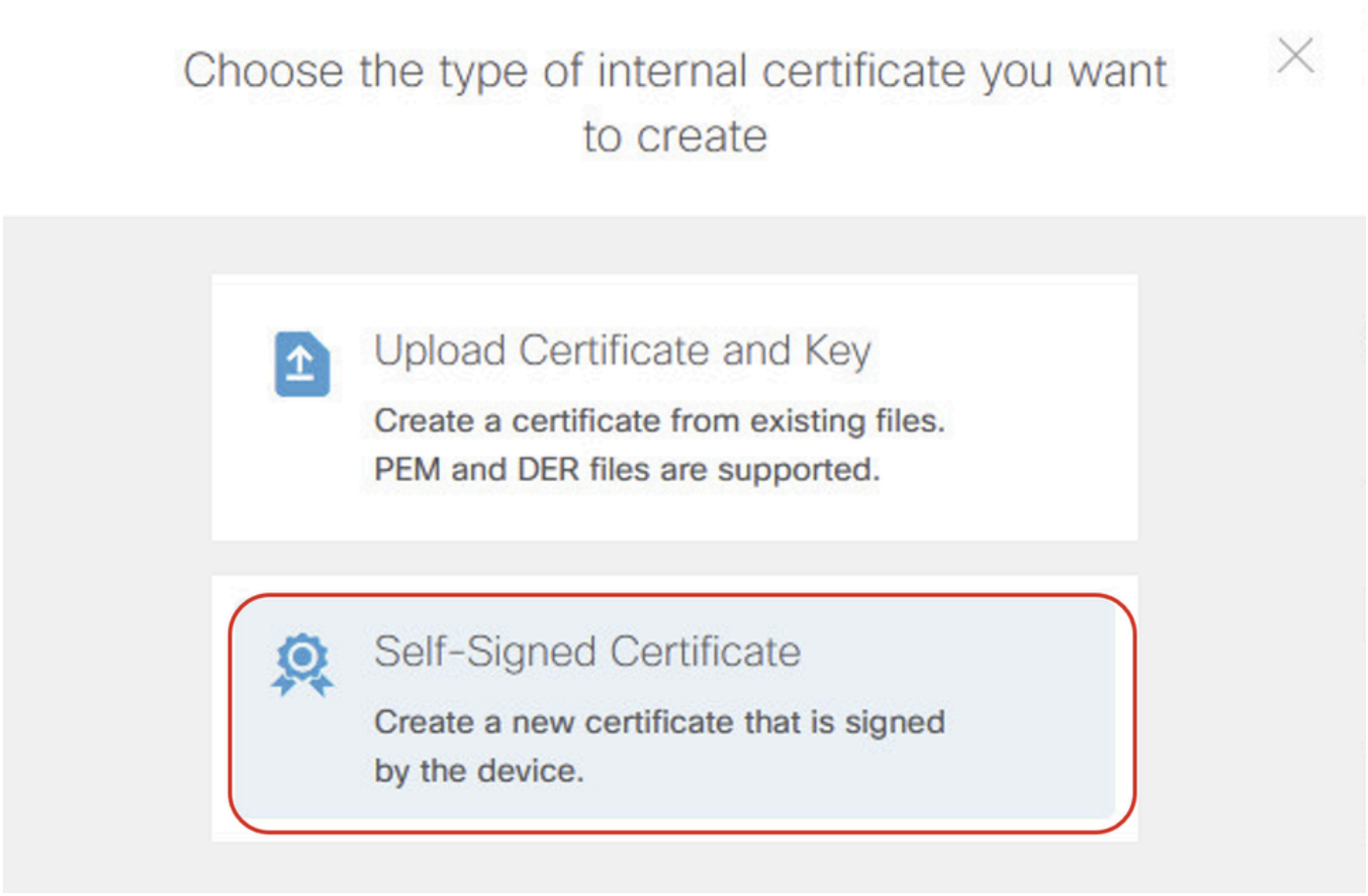
En este ejemplo, se utiliza un nuevo certificado autofirmado con contenido personalizado del certificado para fines de demostración.

Paso 6.1. Navegue hasta Objetos > Certificados. Haga clic en el botón + y seleccione Agregar certificado interno.



Create_Certificate_1

Paso 6.2. Haga clic en Certificado autofirmado.



Paso 6.3. Haga clic en la pestaña General y proporcione la información necesaria.

Nombre: demovpn

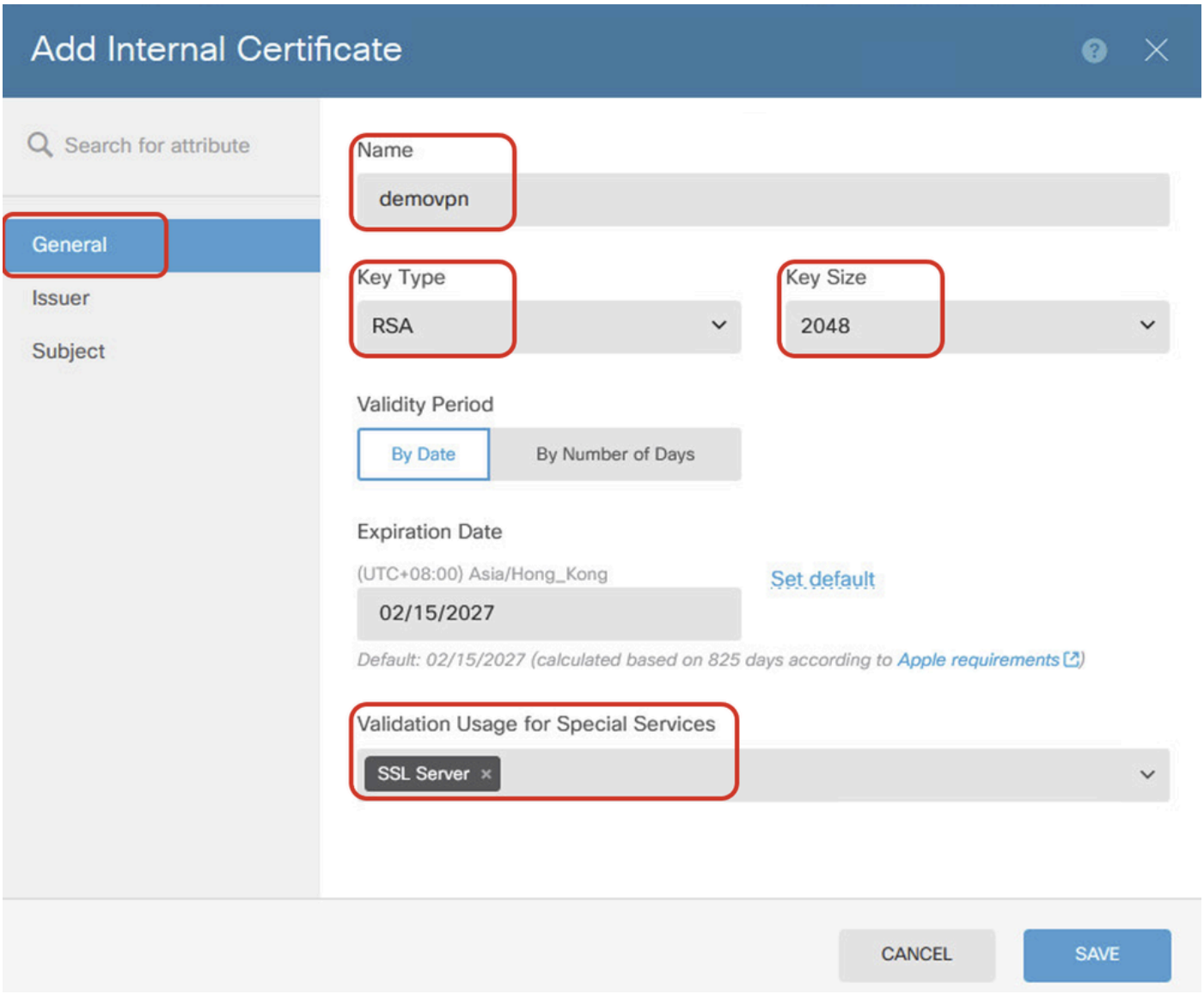
Tipo de clave: RSA

Tamaño de clave: 2048

Período de validez: Predeterminado

Fecha de vencimiento: Predeterminado

Uso de validación para servicios especiales: Servidor SSL

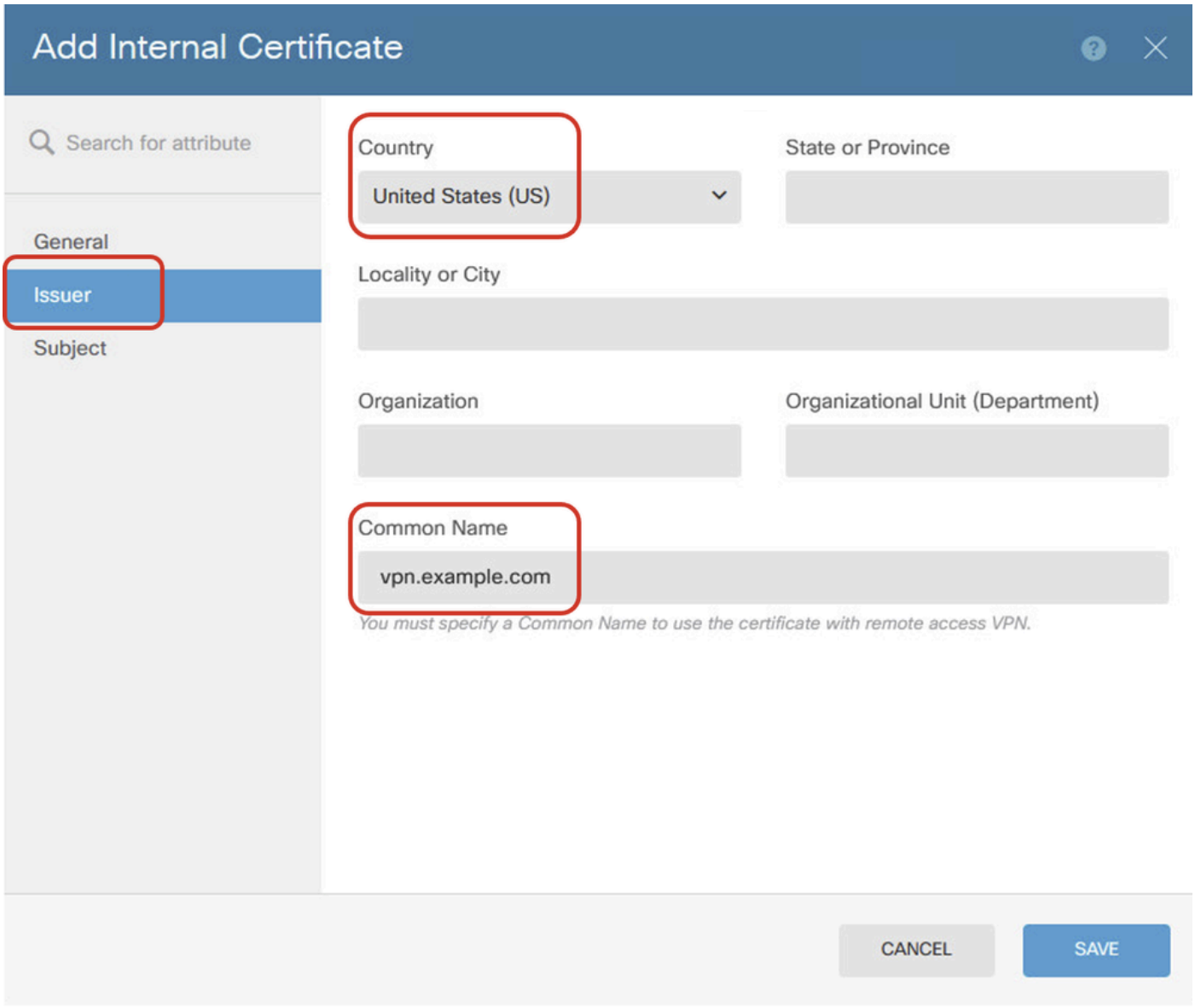


Create_Certificate_3

Paso 6.4. Haga clic en la pestaña Emisor y proporcione la información necesaria.

País: Estados Unidos (US)

Nombre común: vpn.example.com

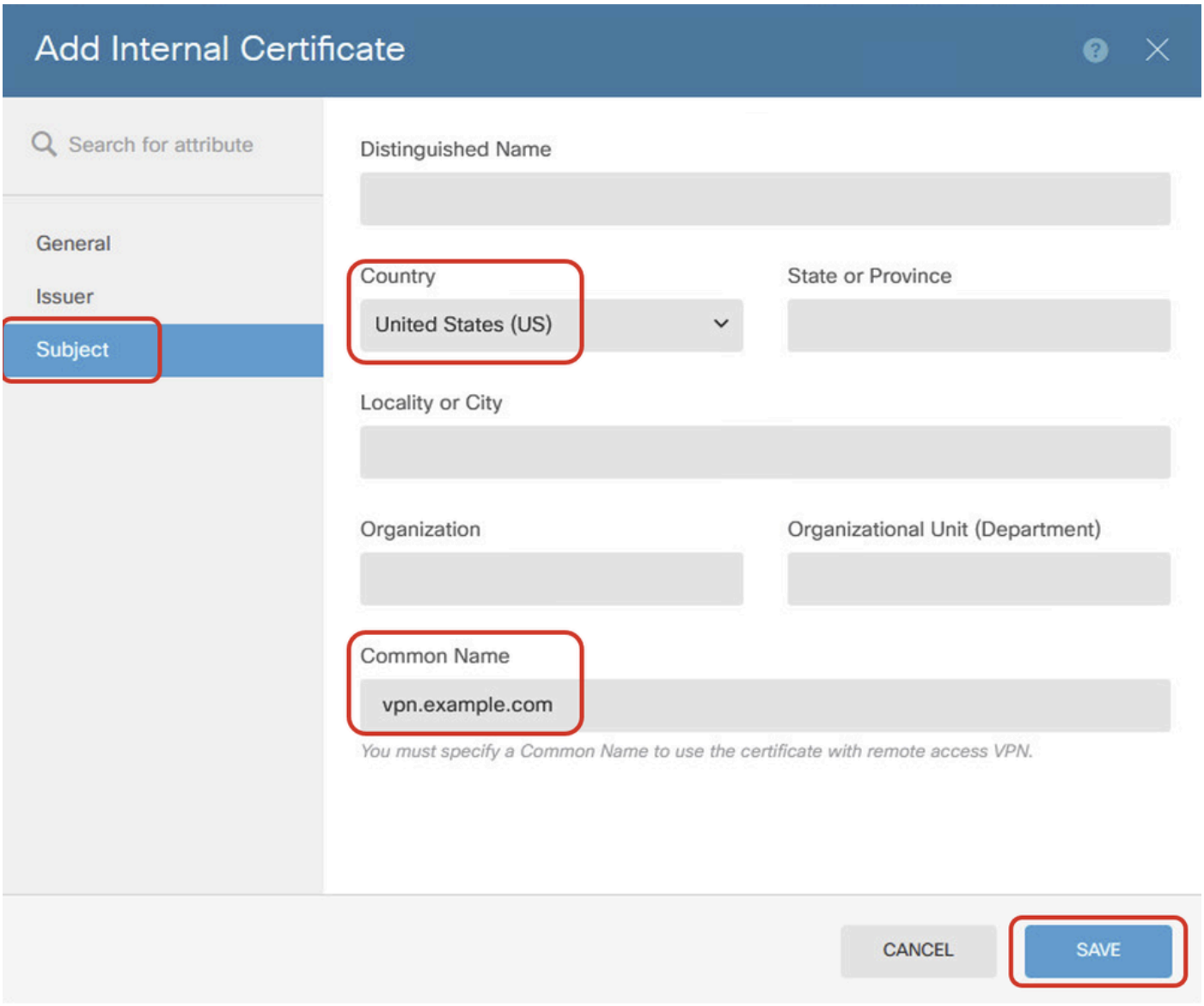


Create_Certificate_4

Paso 6.5. Haga clic en la pestaña Asunto, proporcione la información necesaria y luego haga clic en GUARDAR.

País: Estados Unidos (US)

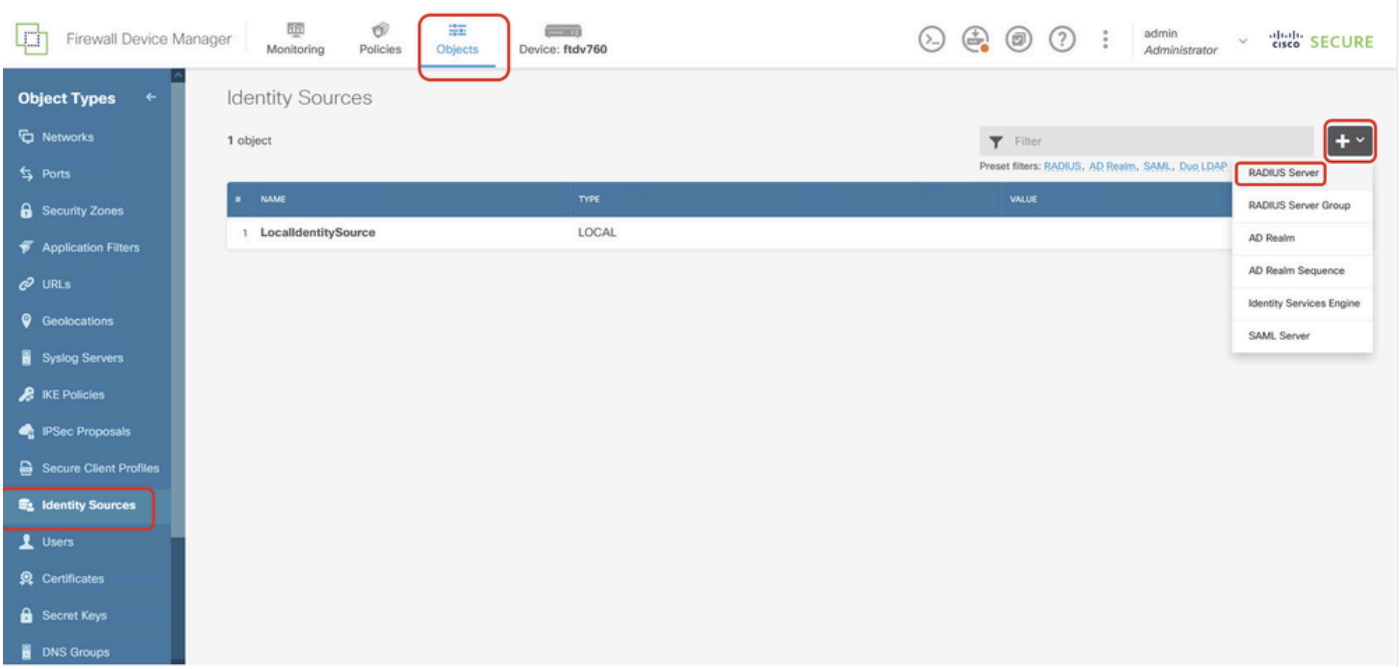
Nombre común: vpn.example.com



Create_Certificate_5

Paso 7. Crear origen de identidad del servidor RADIUS.

Paso 7.1. Navegue hastaObjetos > Orígenes de identidad, haga clic en el botón + y elijaServidor RADIUS.



Create_Radius_Source_1

Paso 7.2. Proporcione la información necesaria del servidor RADIUS. Haga clic en el botón Aceptar.

Nombre: demo_ise

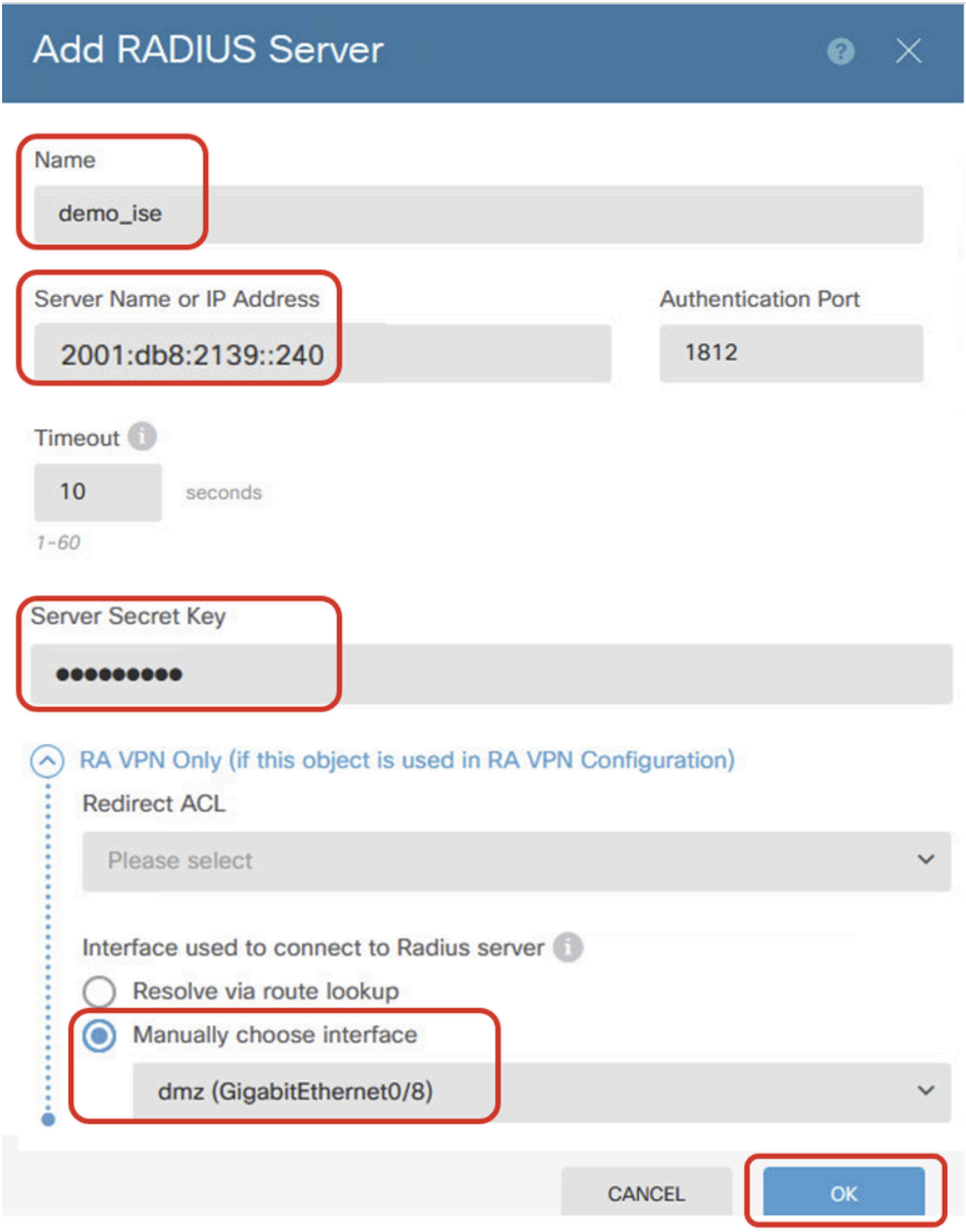
Nombre de servidor o dirección IP: 2001:db8:2139::240

Puerto de autenticación: 1812 (default)

timeout (tiempo de espera): 10 (default)

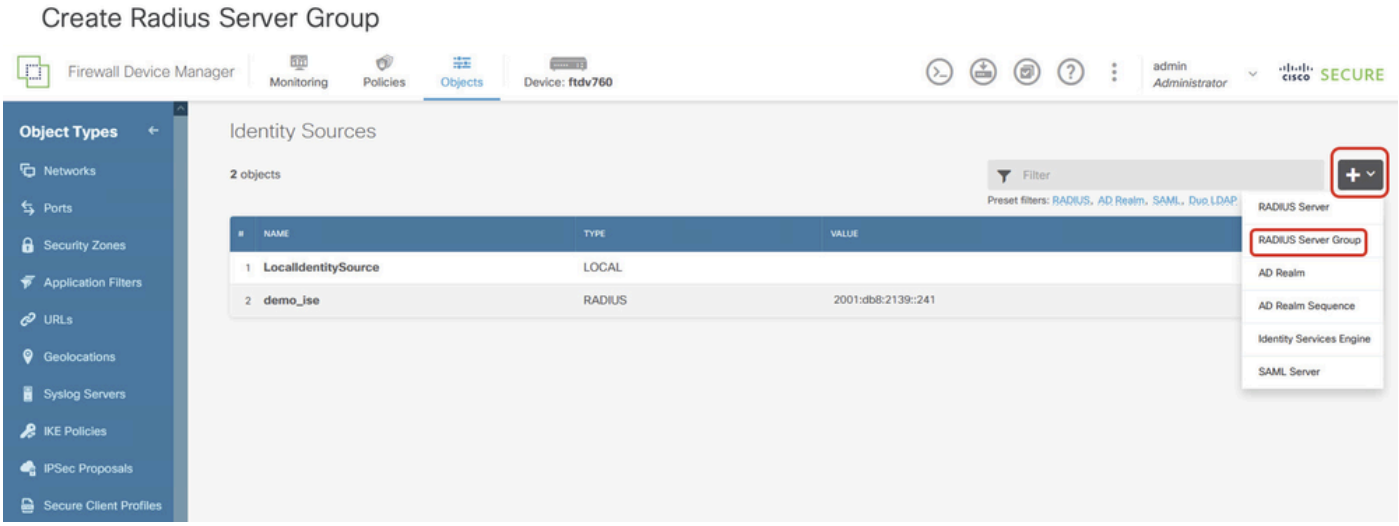
Clave secreta del servidor: Cisco

Interfaz utilizada para conectar con el servidor Radius: Seleccione manualmente la interfaz. En este ejemplo, elija dmz (GigabitEthernet0/8).



Create_Radius_Source_2

Paso 7.3. Navegue hasta Objetos > Orígenes de identidad. Haga clic en el botón + y elija Grupo de servidores RADIUS.



Create_Radius_Source_3

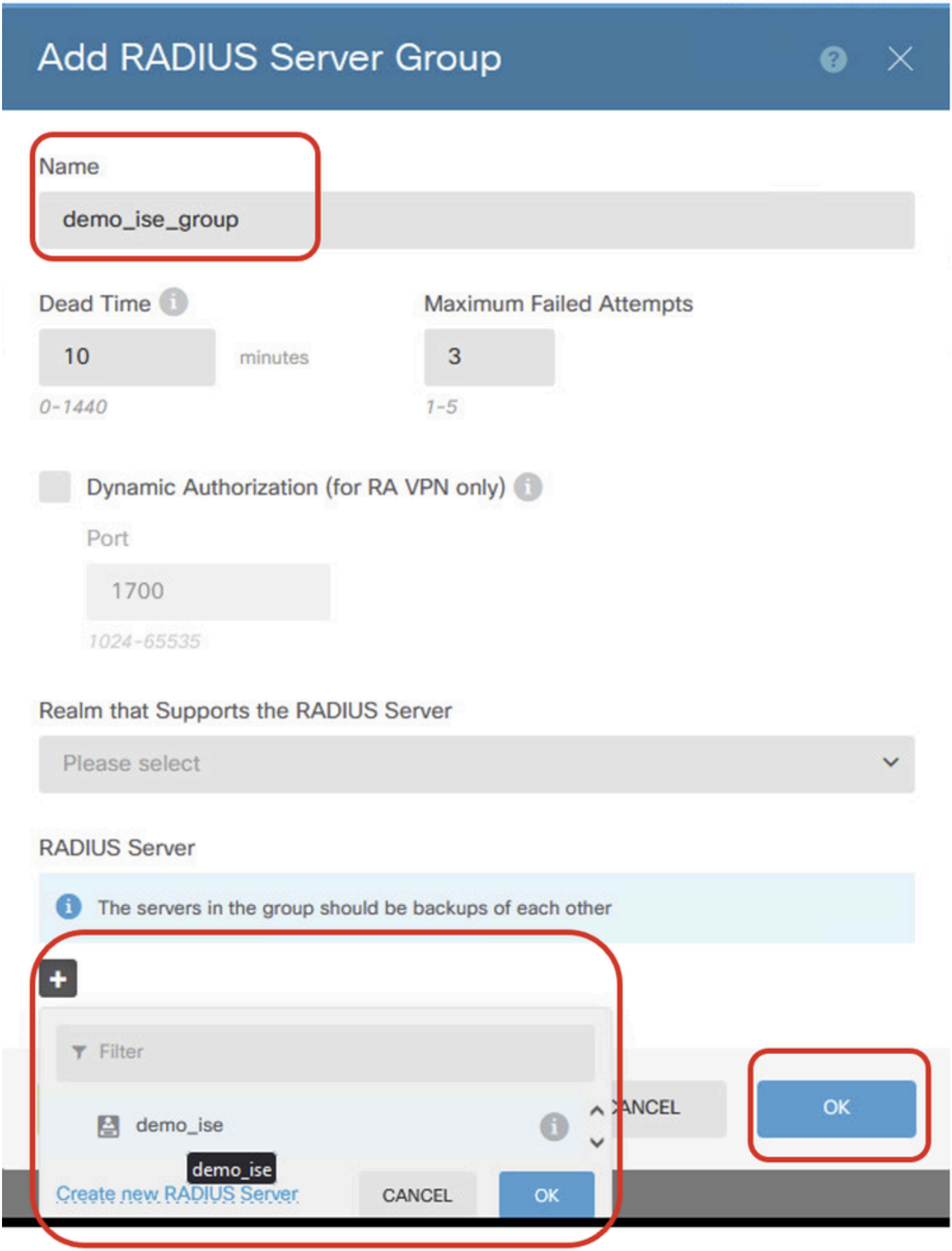
Paso 7.4. Proporcione la información necesaria del grupo de servidores RADIUS. Haga clic en el botón OK (Aceptar)

Nombre: demo_ise_group

Tiempo muerto: 10 (default)

Máximo de intentos fallidos: 3 (default)

Servidor RADIUS: Haga clic en el botón + y seleccione el nombre creado en el paso 6.2. En este ejemplo es demo_ise.



Create_Radius_Source_4

Paso 8. Cree la política de grupo utilizada para RAVPN. En este ejemplo, se configuran parámetros personalizados de banner y tiempo de espera para fines de demostración. Puede realizar modificaciones en función de sus necesidades reales.

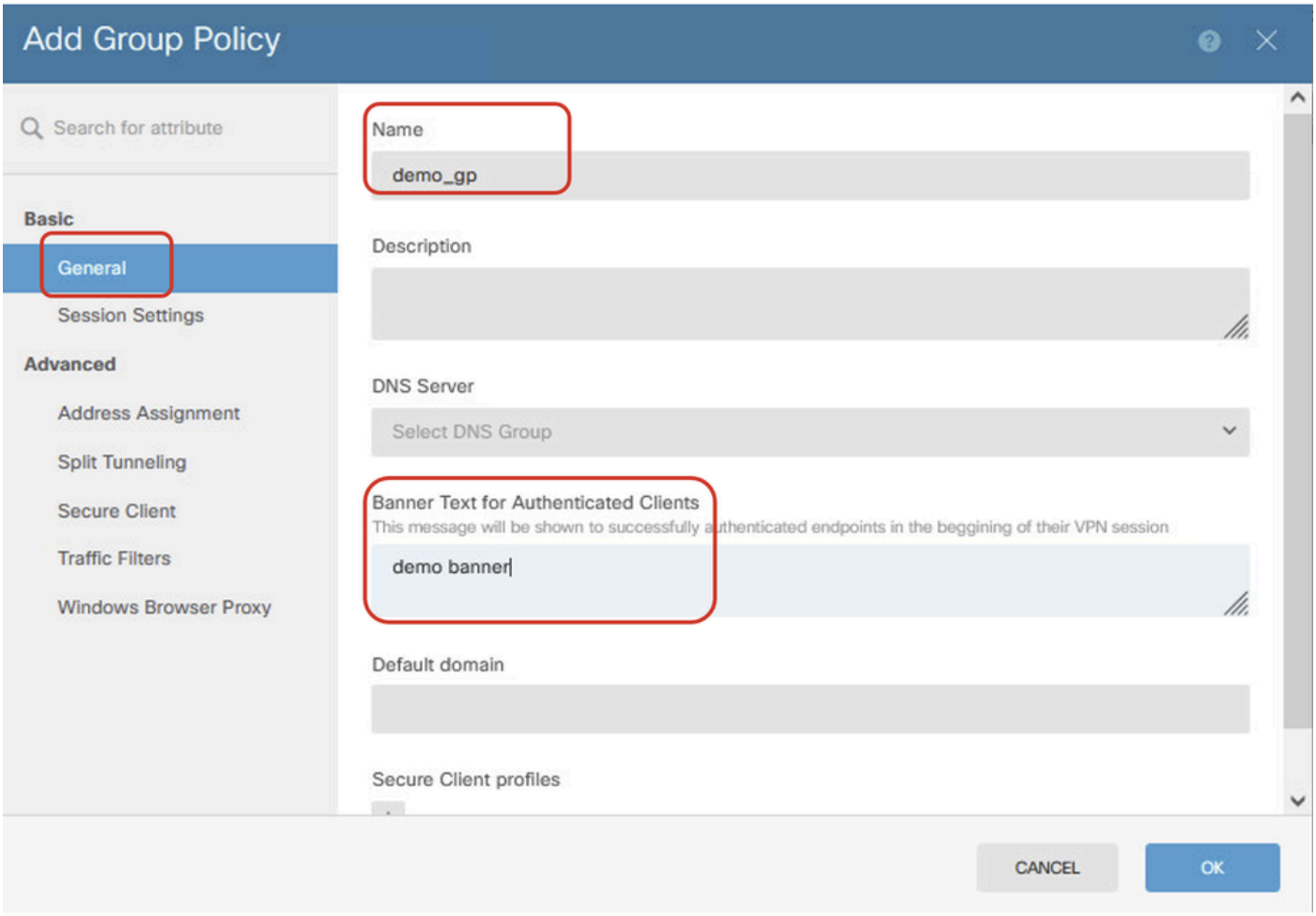
Paso 8.1. Vaya a Remote Access VPN > View Configuration. Haga clic en Políticas de grupo en la barra lateral izquierda y luego haga clic en el botón +.

Create_Group_Policy_1

Paso 8.2. Haga clic en General y proporcione la información necesaria.

Nombre: demo_gp

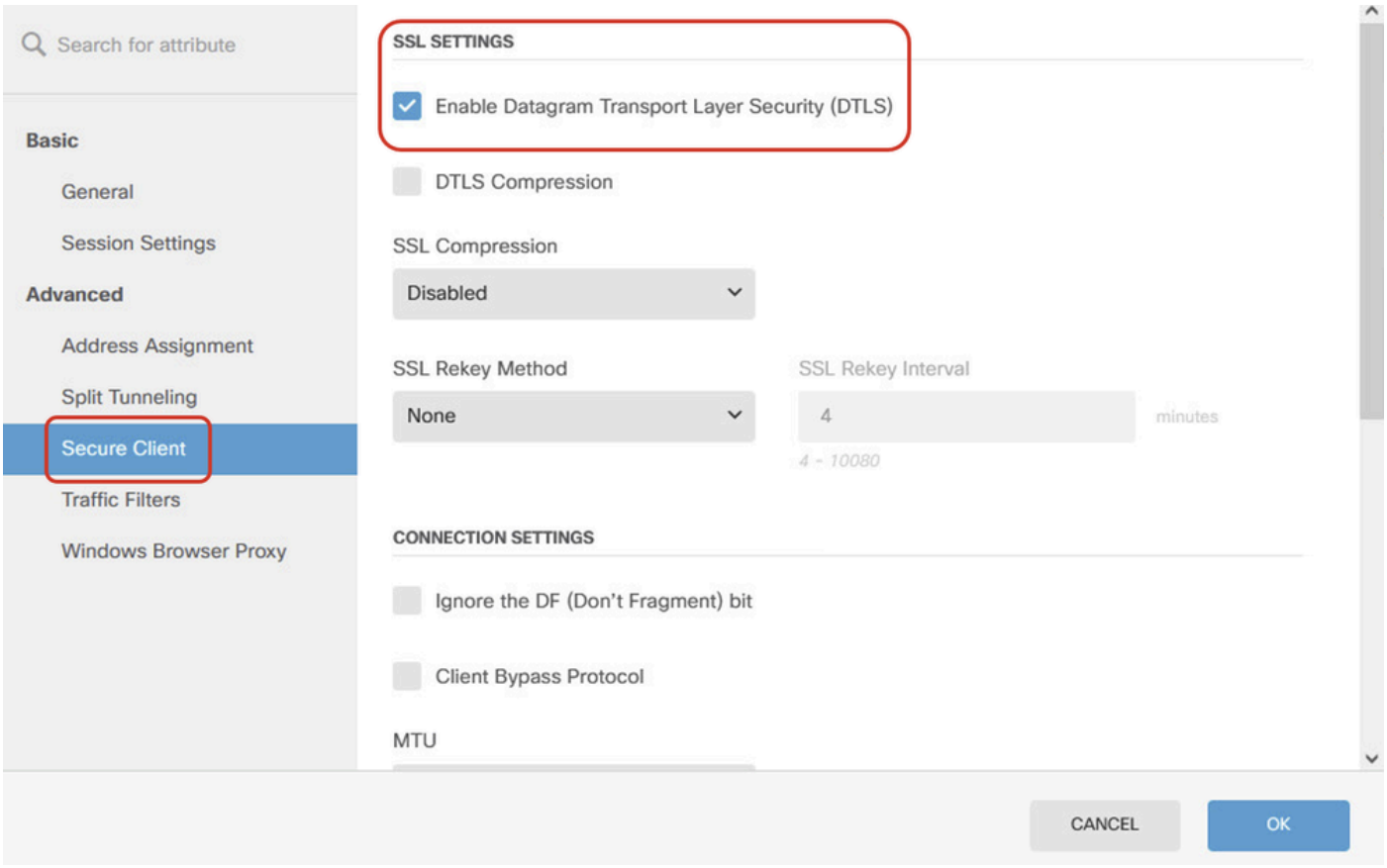
Texto de banner para clientes autenticados: banner de demostración



Create_Group_Policy_2

Paso 8.3. Haga clic en Secure Client y proporcione la información necesaria.

Marque Enable Datagram Transport Layer Security (DTLS).

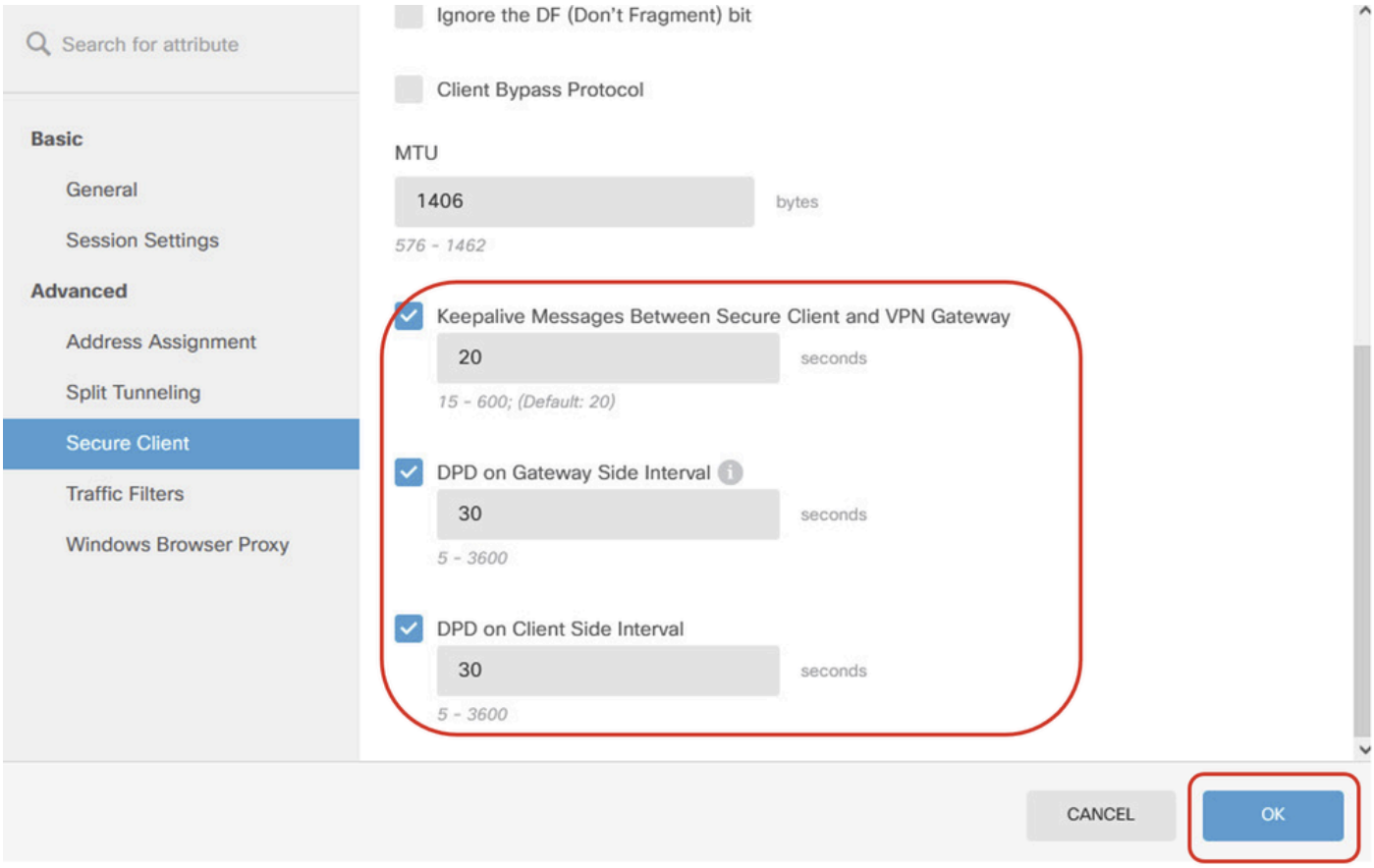


Create_Group_Policy_3

Marque Mensajes Keepalive entre Secure Client y VPN Gateway (valor predeterminado).

Marque DPD en Intervalo del lado de la puerta de enlace (valor predeterminado).

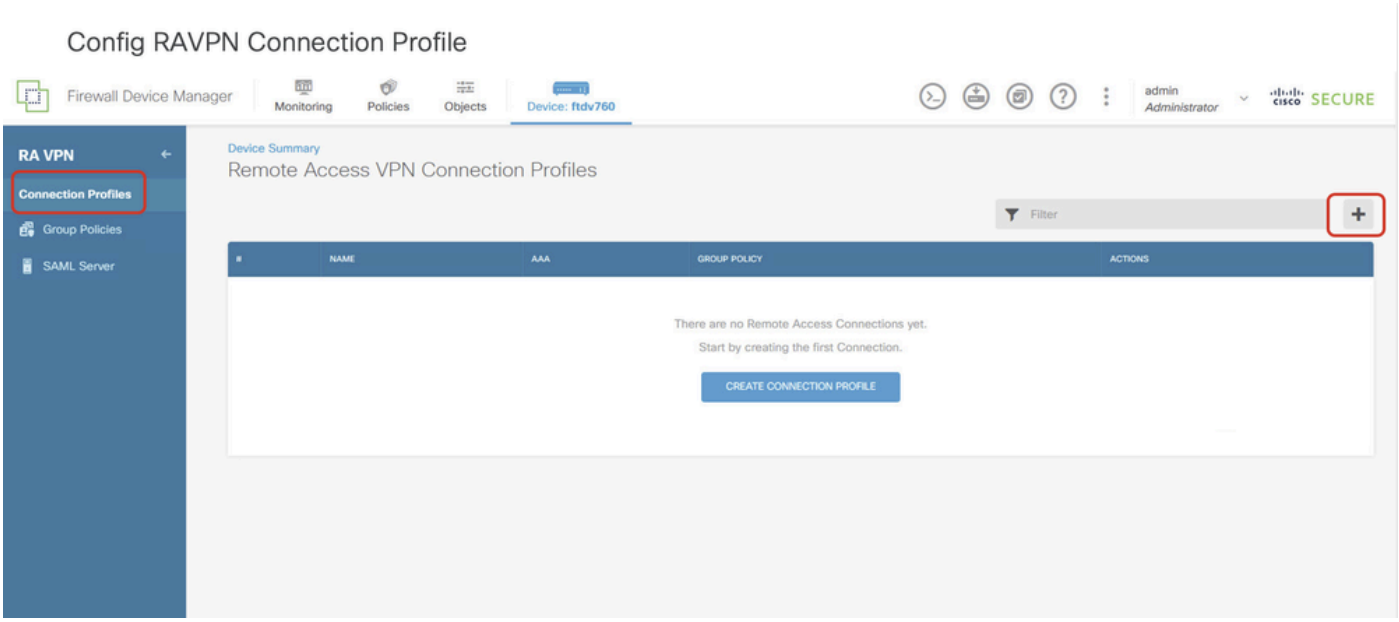
Verifique DPD en el Intervalo del Lado del Cliente (valor predeterminado).



Create_Group_Policy_3_Cont

Paso 9. Crear un perfil de conexión RAVPN.

Paso 9.1. Vaya aVPN de acceso remoto > Ver configuración. Haga clic en Perfil de conexión en la barra lateral izquierda y luego haga clic en el botón + para iniciar el asistente.

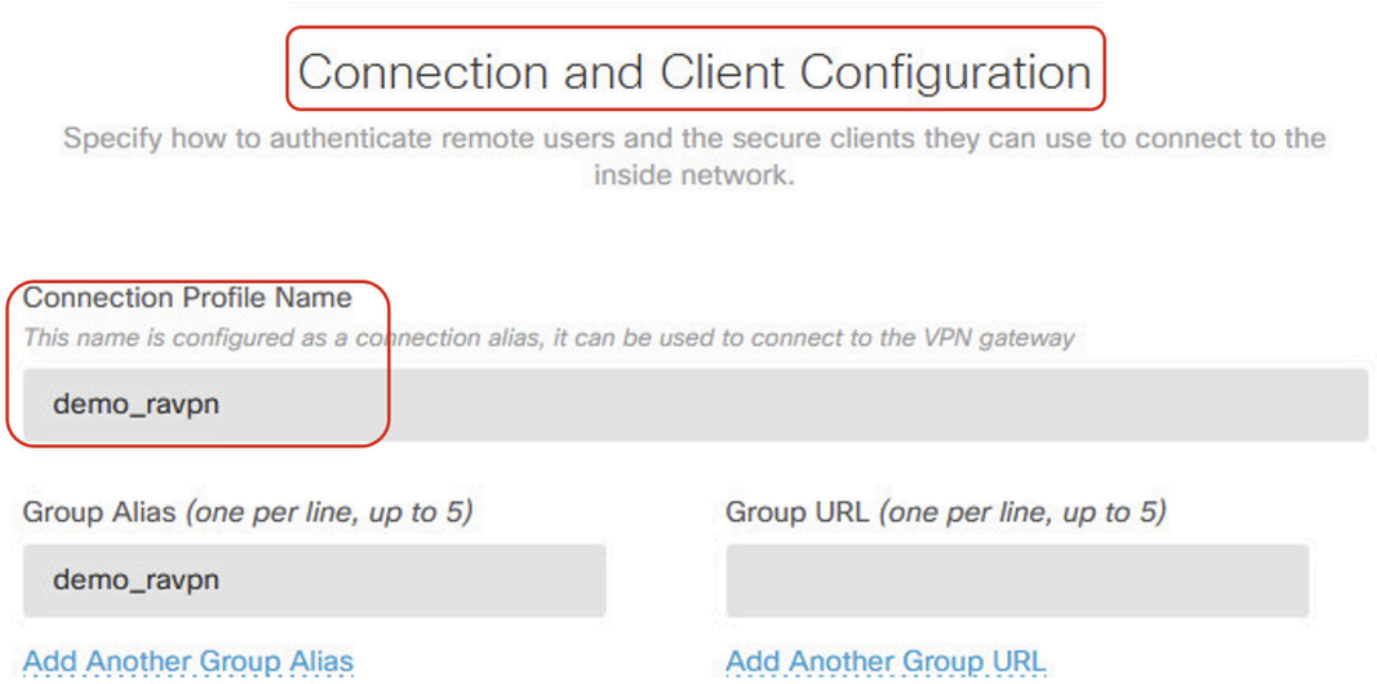


Create_RAVPN_Wizard_1

Paso 9.2. Proporcione la información necesaria en la sección Conexión y configuración del cliente y haga clic en el botón NEXT (Siguiente).

Nombre del perfil de conexión: demo_ravpn

Alias de grupo: demo_ravpn



Create_RAVPN_Wizard_2_Conn_Name

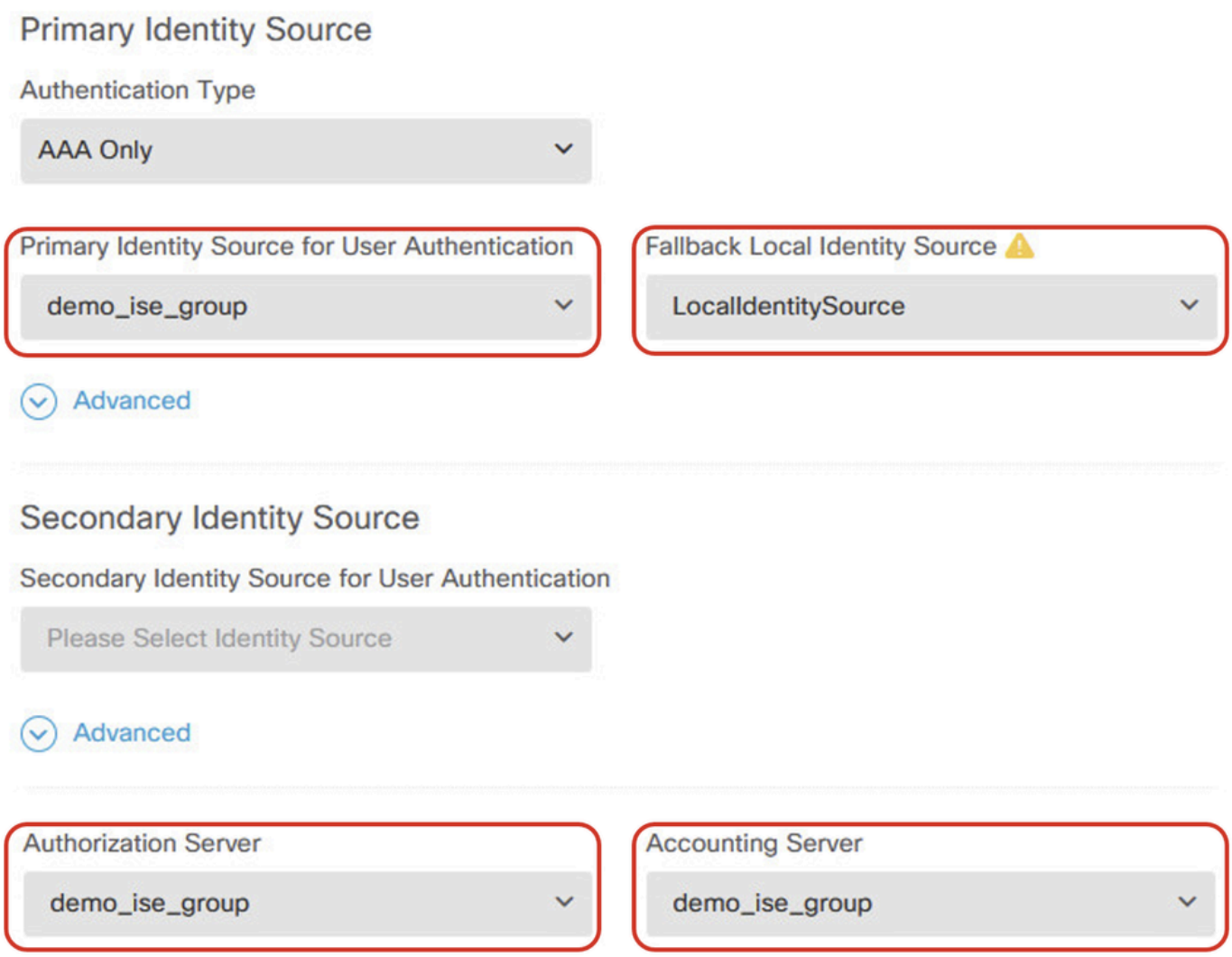
Origen de identidad principal > Tipo de autenticación: Sólo AAA

Origen de identidad principal > Origen de identidad principal: demo_ise_group (nombre configurado en el paso 7.4.)

Origen de identidad local de reserva: LocalIdentitySource

Servidor de autorización: demo_ise_group (el nombre configurado en el paso 7.4.)

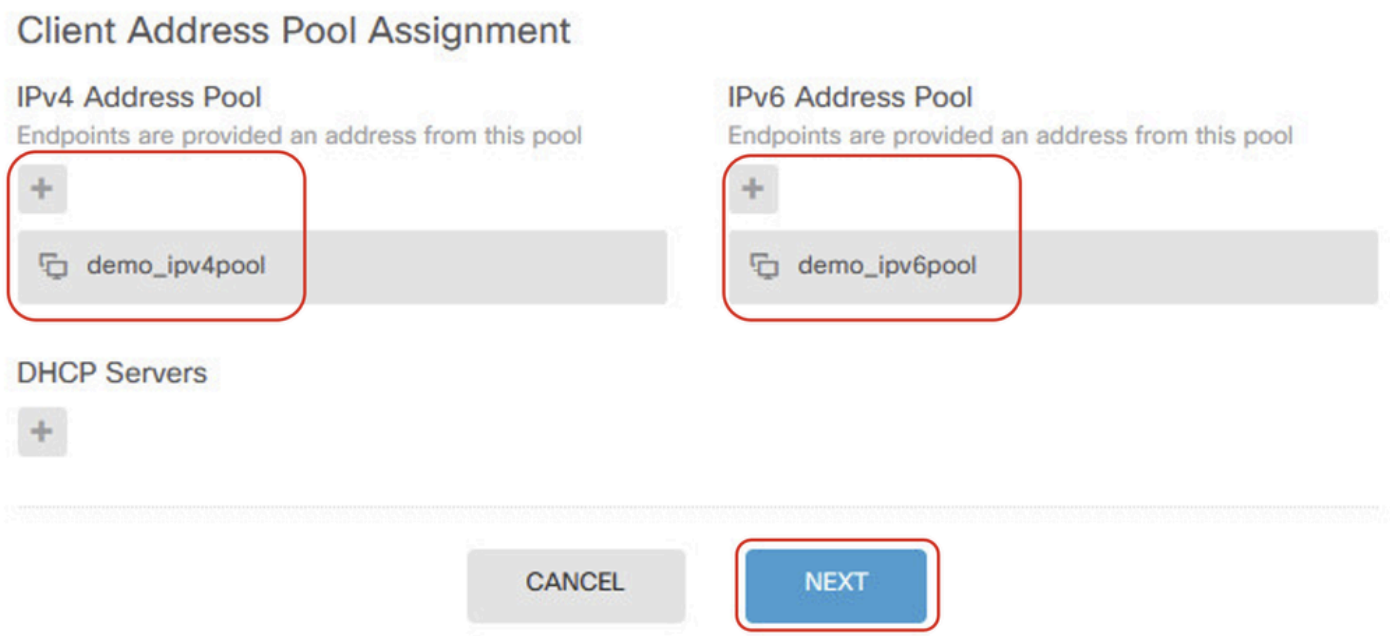
Servidor de cuentas: demo_ise_group (el nombre configurado en el paso 7.4.)



Create_RAVPN_Wizard_2_Identity_Source

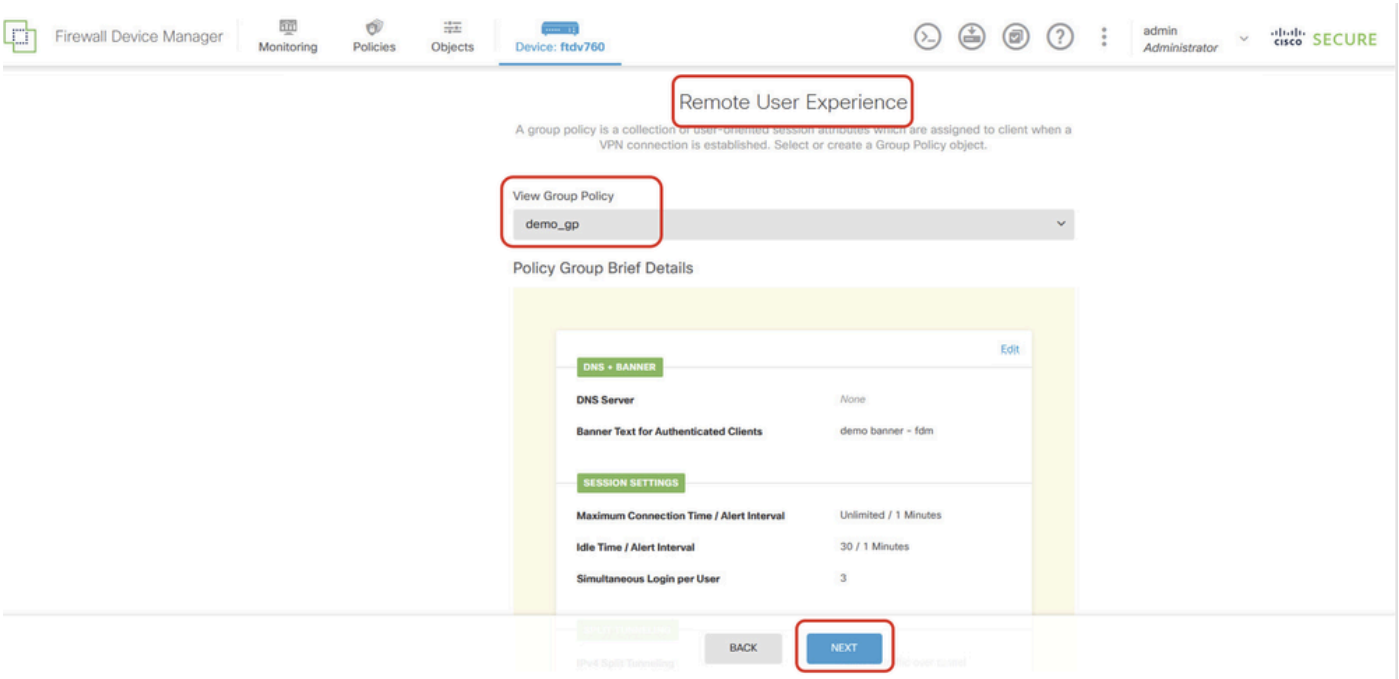
Conjunto de direcciones IPv4: demo_ipv4pool (nombre configurado en el paso 4.2.)

Pool de Direcciones IPv6: demo_ipv6pool (el nombre configurado en el paso 4.2.)



Create_RAVPN_Wizard_2_Address_Pool

Paso 9.3. Elija la política de grupo configurada en el Paso 8.2. en la sección Experiencia de usuario remoto y haga clic en el botón NEXT.

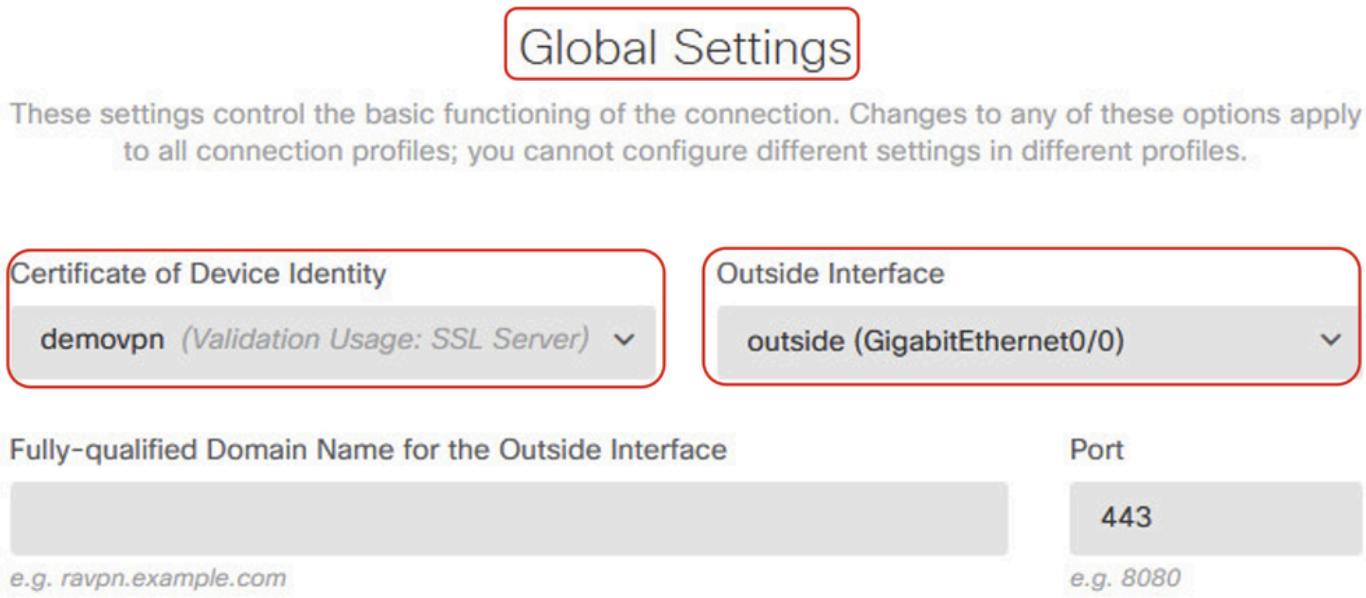


Create_RAVPN_Wizard_3

Paso 9.4. Proporcione la información necesaria en la sección Configuración global y haga clic en el botón NEXT (Siguiente).

Certificado de identidad del dispositivo: demovpn (el nombre configurado en el paso 6.3.)

Interfaz externa: fuera



Create_RAVPN_Wizard_4

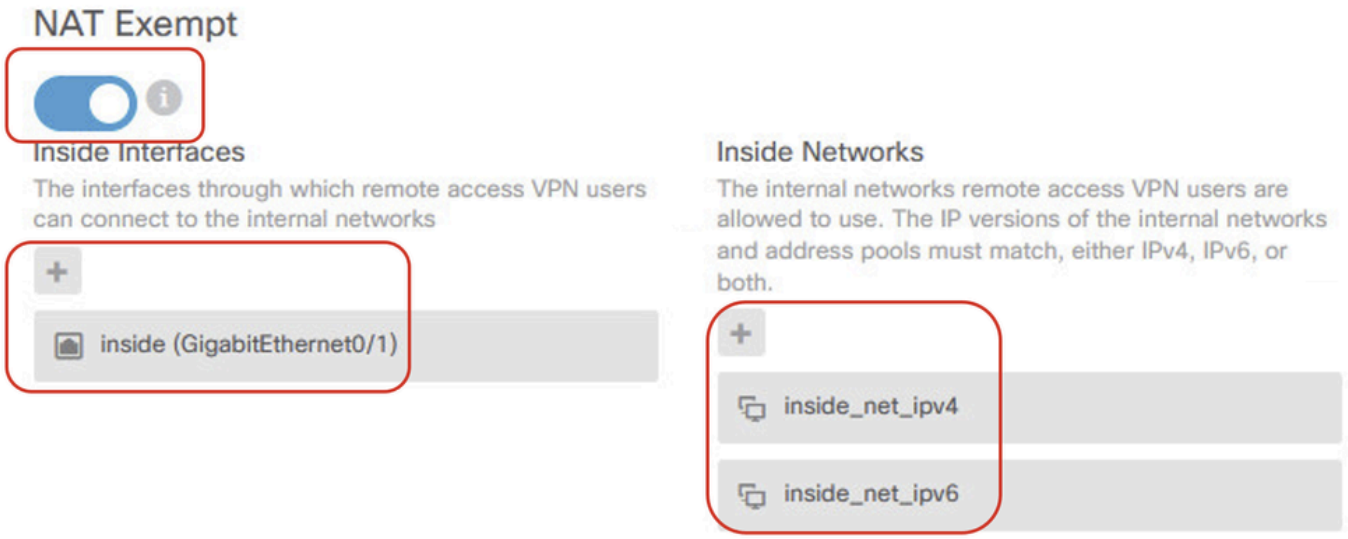
Control de acceso para tráfico VPN: Verifique Bypass Access Control policy for decrypted traffic (sysopt permit-vpn).

Create_RAVPN_Wizard_4_VPN_ACP

Exención de NAT: Haga clic en el control deslizante hasta la posición Activado

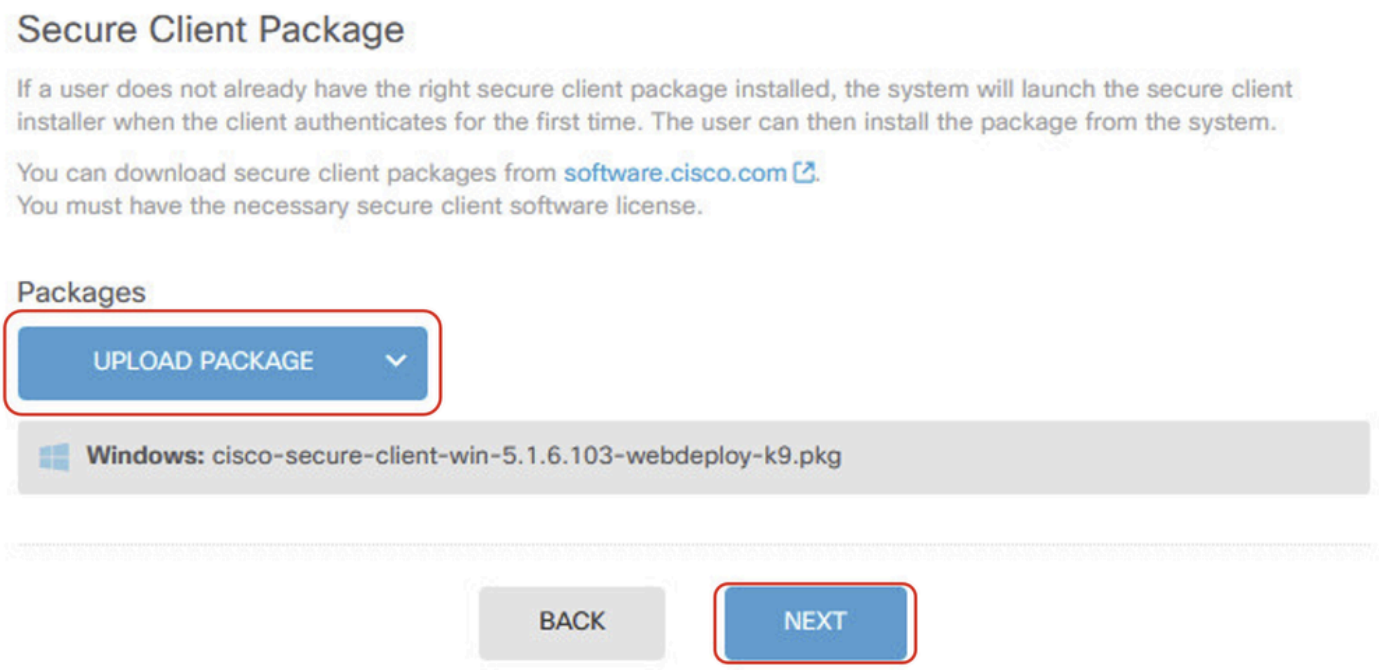
Interfaces internas: dentro

Redes internas: inside_net_ipv4, inside_net_ipv6 (el nombre configurado en el paso 5.2.)



Create_RAVPN_Wizard_4_VPN_NATExempt

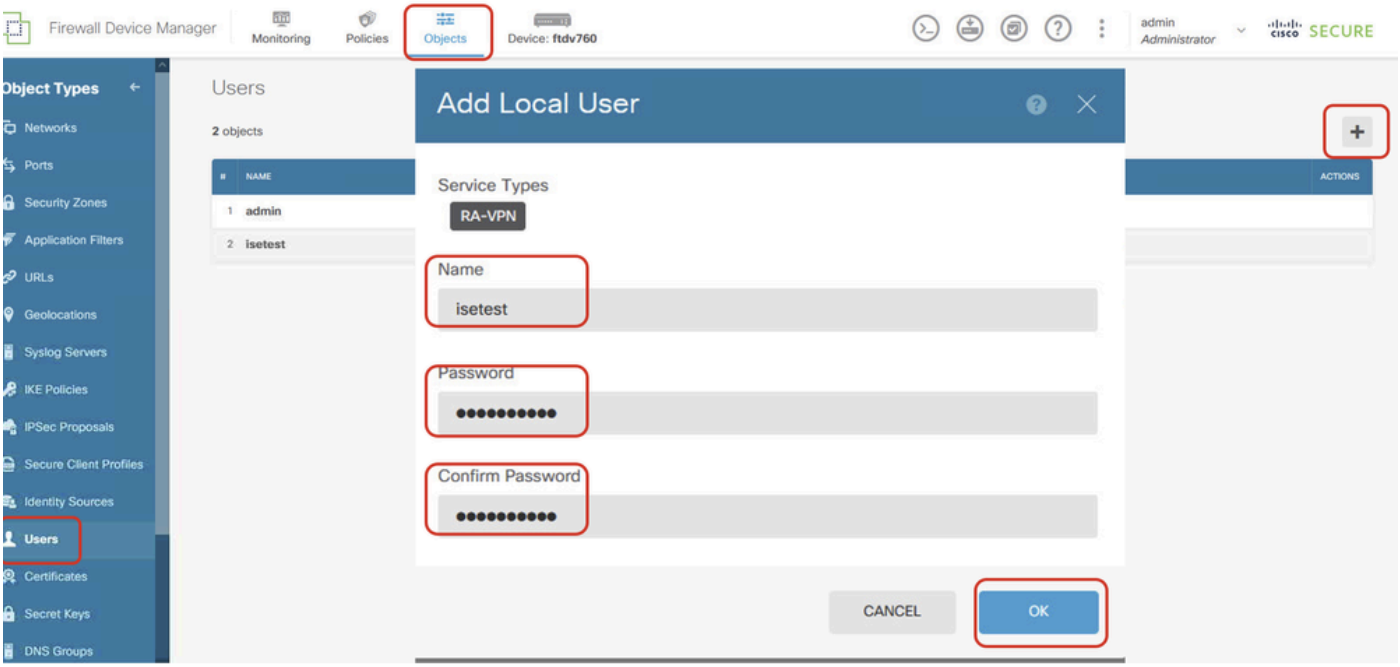
Paquete de Secure Client: Haga clic en CARGAR PAQUETE y cargue el paquete como corresponda. En este ejemplo, se carga el paquete de Windows.



Create_RAVPN_Wizard_4_Image

Paso 9.5. Revise el resumen. Si necesita modificar algo, haga clic en el botón BACK. Si todo está bien, haga clic en el botón FINISH.

Paso 10. Cree un usuario local si elige Origen de identidad local de reserva con LocalIdentitySource en el paso 9.2. La contraseña del usuario local debe ser la misma que la configurada en ISE.



Create_Local_User

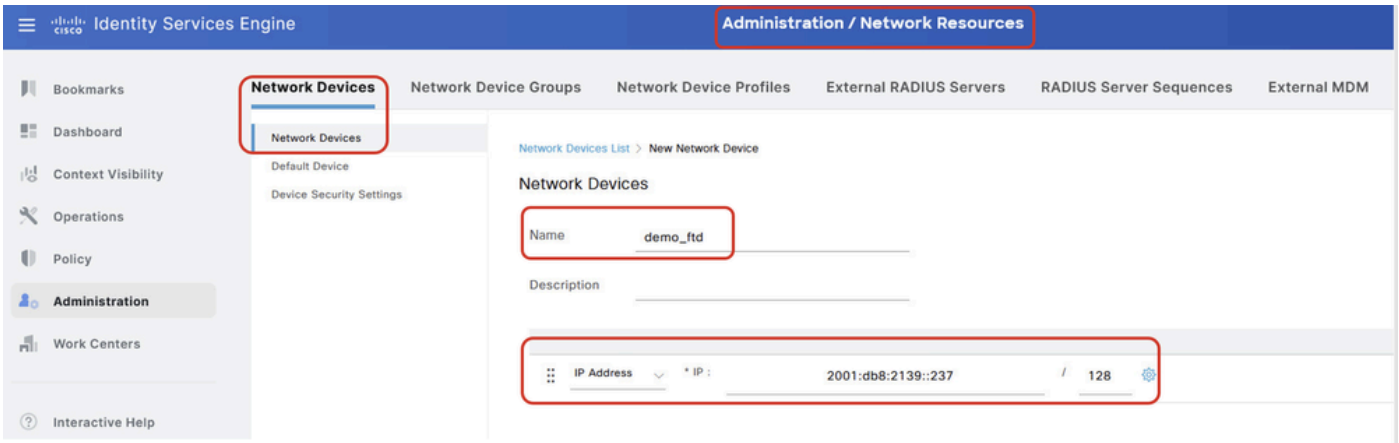
Paso 11. Implementar los cambios de configuración.

Implementar_cambios

Configuraciones en ISE

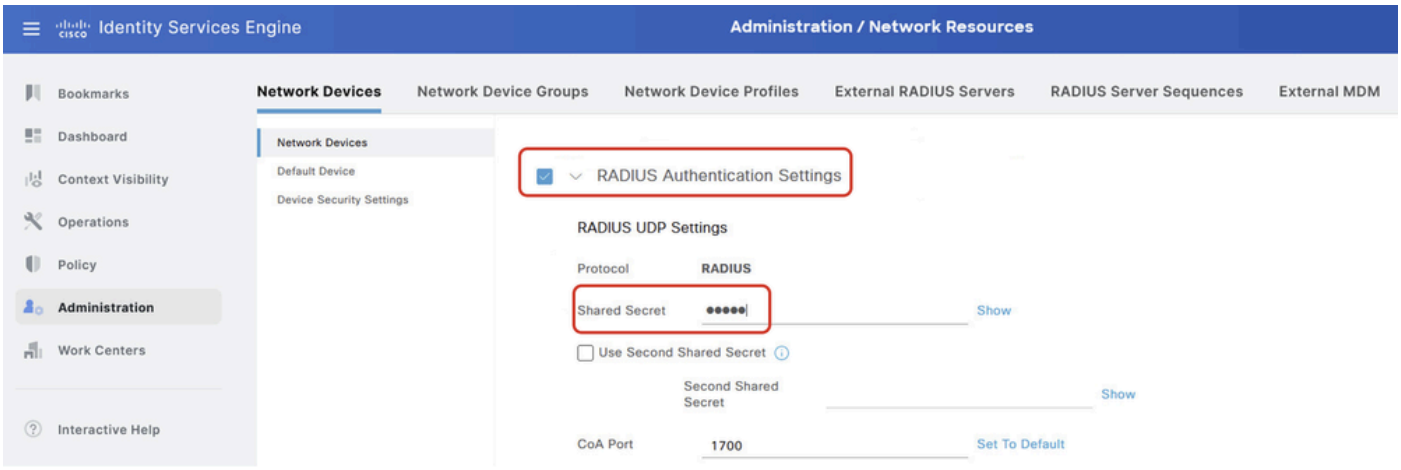
Paso 12. Crear dispositivos de red.

Paso 12.1. Navegue hasta Administration > Network Resources > Network Devices, haga clic en Add, proporcione el nombre, la dirección IP y desplácese hacia abajo en la página.



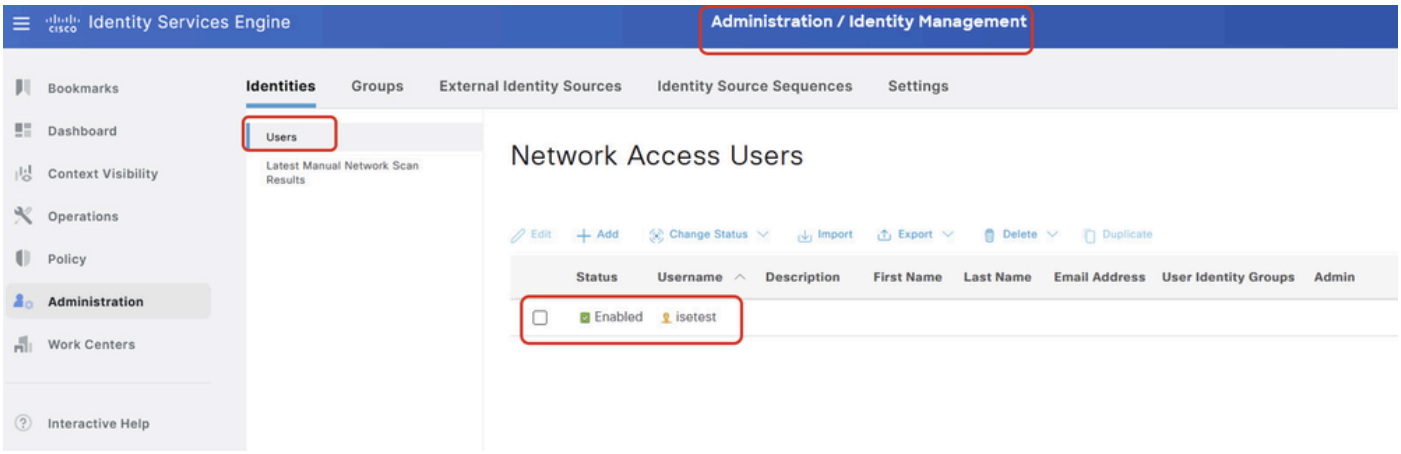
Create_Network_Devices

Paso 12.2. Marque la casilla de verificación de RADIUS Authentication Settings. Proporcione el secreto compartido y haga clic en Enviar.



Create_Network_Devices_Cont

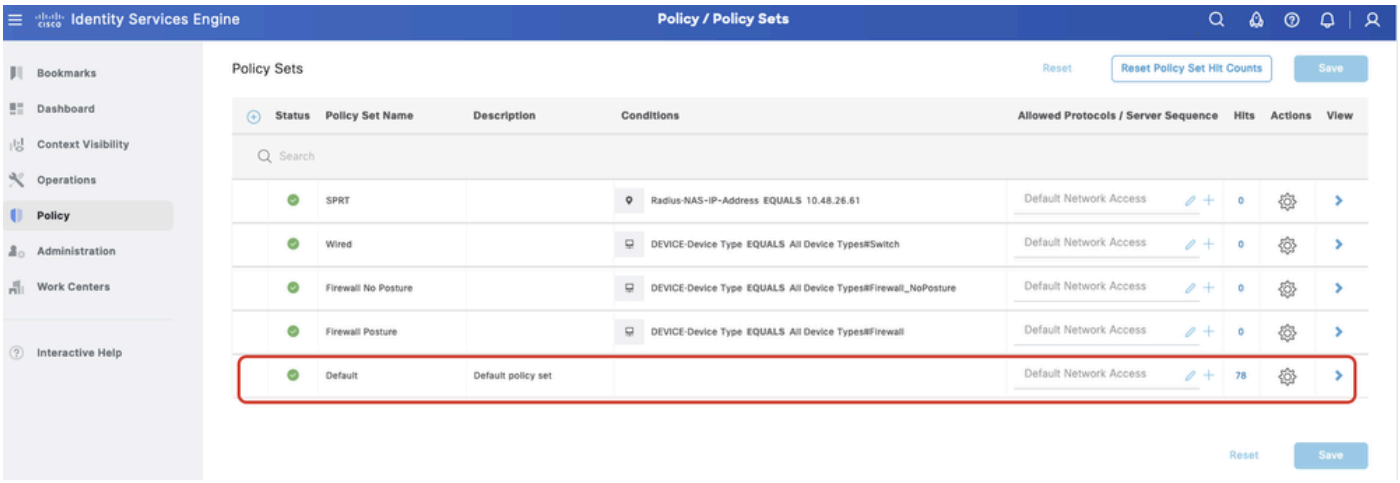
Paso 13. Crear usuarios de acceso a la red. Vaya a Administration > Identity Management > Identities. Haga clic en Agregar para crear un nuevo usuario. La contraseña es la misma con el usuario local de FDM creado en el paso 10. para asegurarse de que la reserva funciona.



Create_ISE_User

Paso 14. (Opcional) Cree un nuevo juego de políticas con una regla de autenticación y una regla

de autorización personalizadas. En este ejemplo, el conjunto de políticas predeterminado se utiliza para fines de demostración.

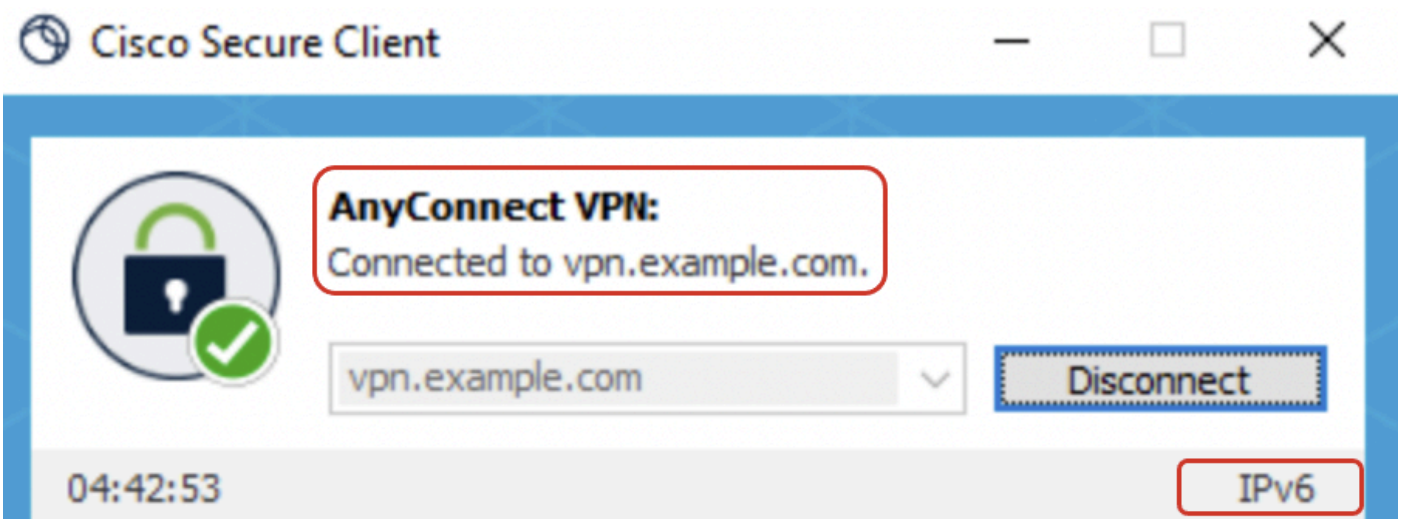


ISE_Default_Policy_Set

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Paso 15. Conecte el gateway VPN a través de la dirección IPv6 en el cliente. La conexión VPN se ha realizado correctamente.



Verify_Connection_Successful

Paso 16. Navegue hasta la CLI de FTD a través de SSH o la consola. Ejecute el comando show vpn-sessiondb detail anyconnect en la CLI de FTD (Line) para verificar los detalles de la sesión VPN.

```
<#root>

ftdv760# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed
```

Username : isetest

Index : 2

Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 15402 Bytes Rx : 14883
Pkts Tx : 10 Pkts Rx : 78
Pkts Tx Drop : 0 Pkts Rx Drop : 10
Group Policy : demo_gp Tunnel Group : demo_ravpn
Login Time : 05:22:30 UTC Mon Dec 23 2024
Duration : 0h:05m:05s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : c0a81e0a000020006768f396
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 2.1

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Encryption : none Hashing : none
TCP Src Port : 58339 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 24 Minutes
Client OS : win
Client OS Ver: 10.0.19042
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 7421 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 2.2

Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

```
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 58352
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 25 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 7421 Bytes Rx : 152
Pkts Tx : 1 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 2.3
```

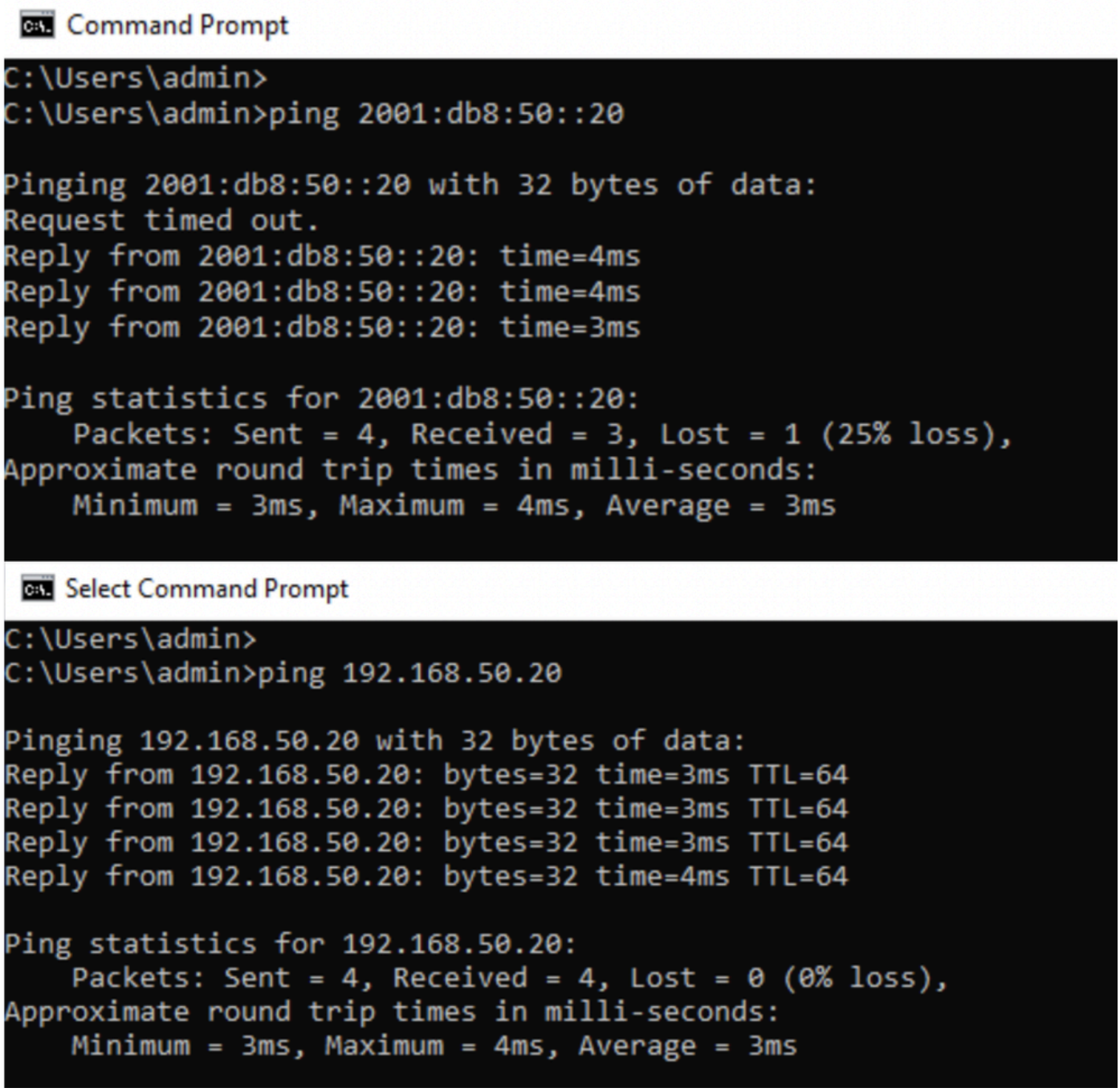
Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

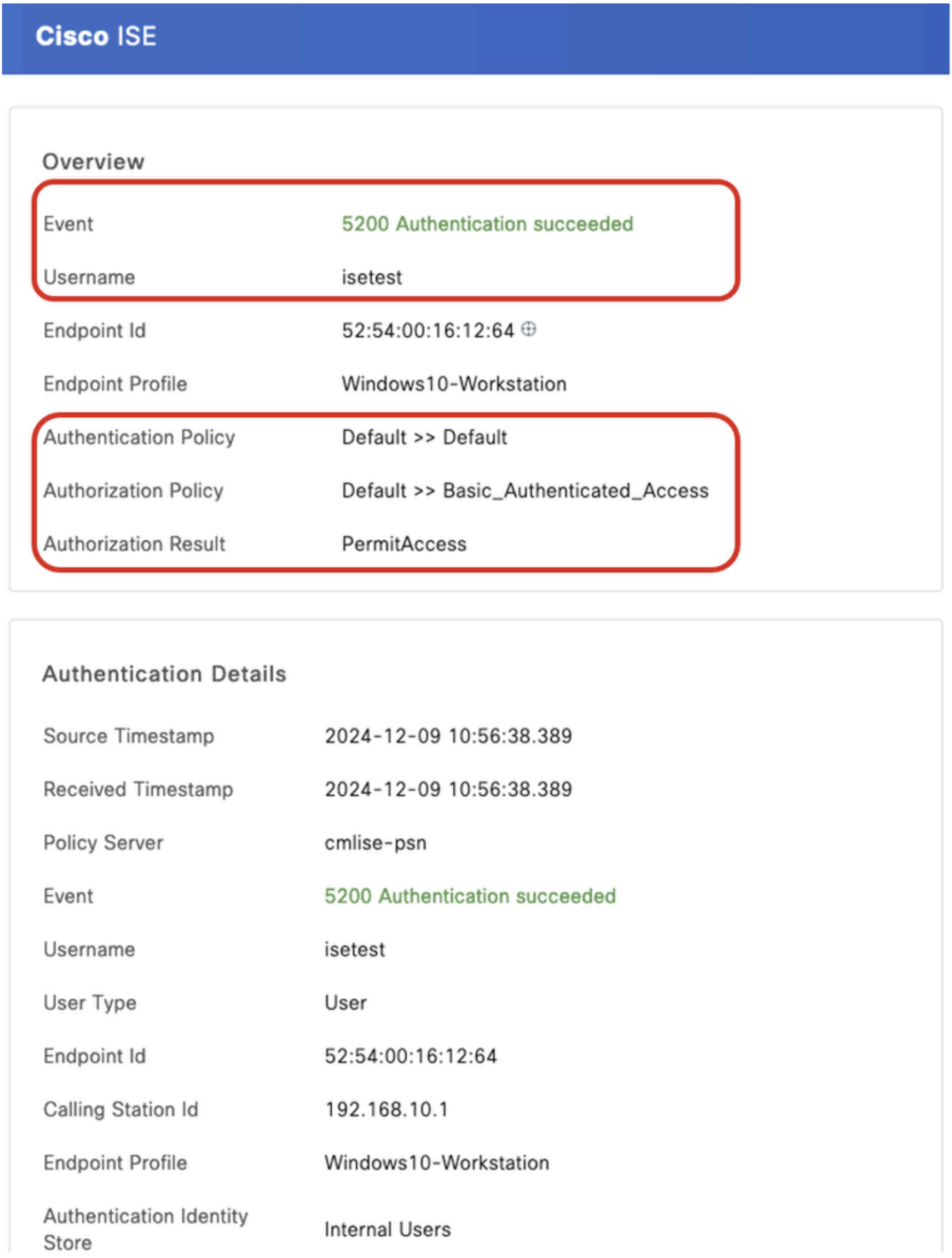
```
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 58191
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 560 Bytes Rx : 14731
Pkts Tx : 8 Pkts Rx : 76
Pkts Tx Drop : 0 Pkts Rx Drop : 10
```

Paso 17. Prueba de ping en el cliente. En este ejemplo, el cliente hace ping correctamente a las direcciones IPv4 e IPv6 del servidor.



Verify_Cisco_Secure_Client_Ping

Paso 18. El registro activo de RADIUS de ISE muestra una autenticación correcta.



ISE_Authentication_Success_Log

Paso 19. La autenticación de prueba de FTD pasa a LOCAL cuando FTD no puede alcanzar ISE.

Paso 19.1. Cuando la autenticación de FTD vaya a ISE, ejecute el comando show aaa-server en FTD (Line) CLI para verificar las estadísticas.

En este ejemplo, no hay contadores para LOCAL y la autenticación se dirige al servidor RADIUS.

<#root>

```
ftdv760# show aaa-server

Server Group:    LOCAL
Server Protocol: Local database
Server Address:  None
Server port:     None
Server status:   ACTIVE, Last transaction at 08:18:11 UTC Fri Dec 6 2024
Number of pending requests              0
Average round trip time                 0ms
Number of authentication requests       0
Number of authorization requests        0
Number of accounting requests           0
Number of retransmissions               0
Number of accepts                       0
Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0
Server Group:    demo_ise_group
Server Protocol: radius


Server Address:  2001:db8:2139::240


Server port:     1812(authentication), 1646(accounting)
Server status:   ACTIVE, Last transaction at 02:56:41 UTC Mon Dec 9 2024
Number of pending requests              0
Average round trip time                 100ms

Number of authentication requests       1  <== Increased



Number of authorization requests        1  <== Increased



Number of accounting requests           1  <== Increased


Number of retransmissions               0

Number of accepts                       2  <== Increased


Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0
```

Paso 19.2. Cierre la interfaz de ISE para simular que FTD no puede recibir ninguna respuesta de ISE.

<#root>

```
ftdv760# ping 2001:db8:2139::240


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:2139::240, timeout is 2 seconds:
???
Success rate is 0 percent (0/3)
```

Paso 19.3. El cliente inicia la conexión VPN e introduce el mismo nombre de usuario y contraseña creados en el paso 10. La conexión VPN sigue siendo correcta.

Ejecute el comando show aaa-server en FTD (Line) CLI nuevamente para verificar la estadística, los contadores de autenticación, autorización y aceptación para LOCAL han aumentado. El contador de aceptaciones para el servidor RADIUS no ha aumentado.

<#root>

```
ftdv760# show aaa-server
Server Group:    LOCAL
Server Protocol: Local database
Server Address:  None
Server port:     None
Server status:   ACTIVE, Last transaction at 03:36:26 UTC Mon Dec 9 2024
Number of pending requests              0
Average round trip time                 0ms

Number of authentication requests       1  <== Increased


Number of authorization requests        1  <== Increased


Number of accounting requests           0
Number of retransmissions               0

Number of accepts                       2  <== Increased


Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0
Server Group:    demo_ise_group
Server Protocol: radius

Server Address:  2001:db8:2139::240
Server port:     1812(authentication), 1646(accounting)
Server status:   ACTIVE, Last transaction at 03:36:41 UTC Mon Dec 9 2024
Number of pending requests              0
Average round trip time                 100ms
```

```
Number of authentication requests       2
Number of authorization requests        1
Number of accounting requests           6
Number of retransmissions               0

Number of accepts                       2  <== Not increased


Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      6
Number of unrecognized responses        0
```

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Puede ejecutar estos comandos en FTD Line para resolver problemas de la sección VPN.

debug webvpn 255
debug webvpn anyconnect 255

Puede recopilar un archivo DART del cliente para la resolución de problemas de VPN para determinar si el problema es con Secure Client. Para obtener orientación, consulte el documento de CCO correspondiente Collect DART Bundle for Secure Client.

Puede ejecutar estos comandos en FTD Line para resolver problemas en la sección Radius.

```
ftdv760# debug radius ?

all      All debug options
decode   Decode debug option
dynamic-authorization CoA listener debug option
session  Session debug option
user     User debug option
<cr>
```

```
ftdv760# debug aaa ?

accounting
authentication
authorization
common
condition
```

```
internal
shim
url-redirect
<cr>
```

Puede revisarlos para resolver el problema relacionado con el tráfico después de la conexión VPN exitosamente.

1. Capture el tráfico en FTD Line para ver si Lina descarta el tráfico, refiriéndose a este documento de CCO; Use las capturas de Firepower Threat Defence y Packet Tracer - Cisco.
2. Revise la política de control de acceso para asegurarse de que el tráfico VPN relacionado pueda pasar si se inhabilita la política de control de acceso de omisión para tráfico descifrado.
3. Revise la exención de NAT para asegurarse de que el tráfico VPN se excluya de NAT.

Información Relacionada

- Guía de configuración de FDM de RAVPN - Cisco
- Recopile el paquete DART para Secure Client - Cisco
- Utilice capturas de Firepower Threat Defence y Packet Tracer - Cisco
- Solución de problemas de Cisco Secure Client - Cisco
- Soporte técnico y descargas de Cisco

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).