Configuración de AAA y autenticación de certificado para Secure Client en FTD mediante FDM

Contenido

Introducción

Este documento describe los pasos para configurar Cisco Secure Client sobre SSL en FTD administrado por FDM con AAA y autenticación de certificados.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

- Cisco Firepower Device Manager Virtual 7.2.8
- Cisco Firewall Threat Defence Virtual 7.2.8

- Cisco Secure Client 5.1.4.74

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

Firepower Device Manager (FDM) es una interfaz de gestión simplificada basada en web que se utiliza para gestionar los dispositivos Cisco Firepower Threat Defence (FTD). El administrador de dispositivos Firepower permite a los administradores de red configurar y administrar sus appliances FTD sin utilizar el Firepower Management Center (FMC), que es más complejo. FDM proporciona una interfaz de usuario intuitiva para operaciones básicas como la configuración de interfaces de red, zonas de seguridad, políticas de control de acceso y VPN, así como para supervisar el rendimiento del dispositivo y los eventos de seguridad. Es adecuado para implementaciones pequeñas y medianas en las que se desea una gestión simplificada.
Este documento describe cómo integrar nombres de usuario precargados con Cisco Secure Client en FTD administrado por FDM.
Si está administrando FTD con FMC, consulte la guía Configure AAA and Cert Auth for Secure Client on FTD via FMC.

Esta es la cadena de certificados con el nombre común de cada certificado utilizado en el documento.

- CA: ftd-ra-ca-common-name
- Certificado de cliente: sslVPNClientCN
- Certificado de servidor: 192.168.1.200

Diagrama de la red

Esta imagen muestra la topología utilizada para el ejemplo de este documento.

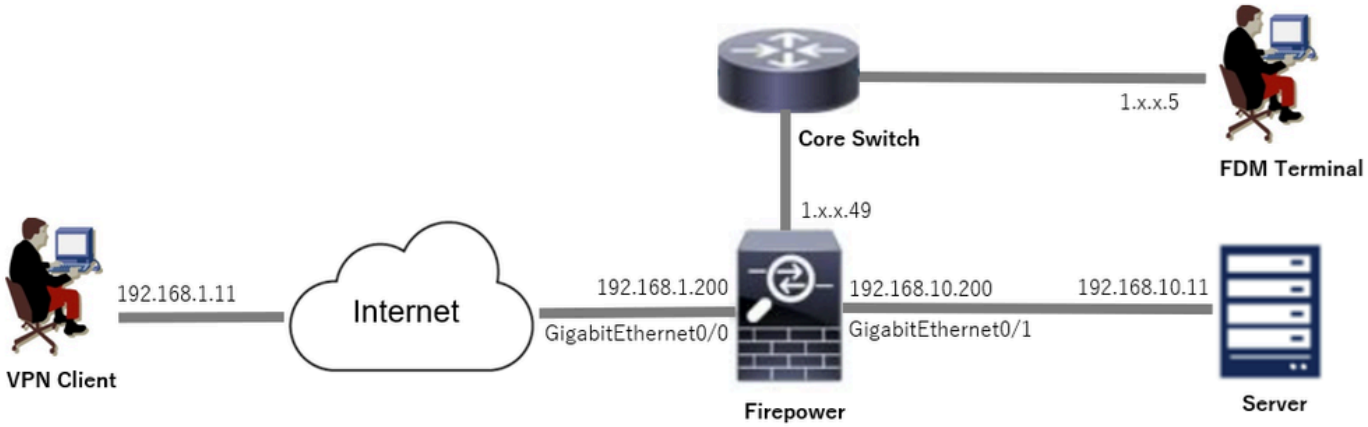


Diagrama de la red

Configuraciones

Configuración en FDM

Paso 1. Configuración de la interfaz FTD

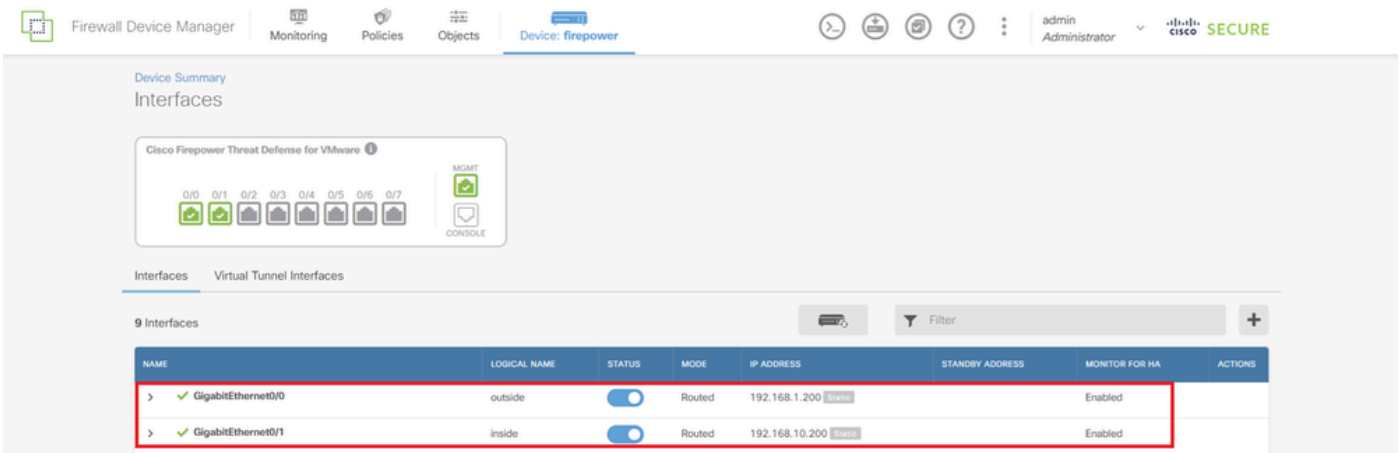
Vaya a Device > Interfaces > View All Interfaces, configure inside and outside interface for FTD inInterfaces.

Para GigabitEthernet0/0,

- Nombre: fuera
- Dirección IP: 192.168.1.200/24

Para GigabitEthernet0/1,

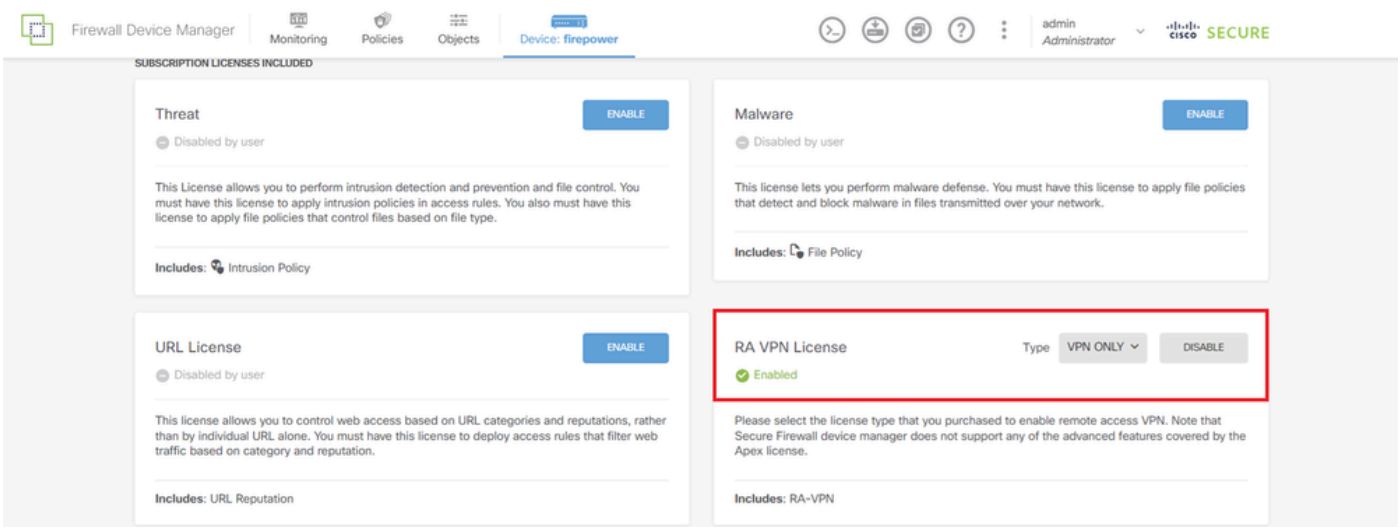
- Nombre: interior
- Dirección IP: 192.168.10.200/24



Interfaz FTD

Paso 2. Confirmar licencia de cliente seguro de Cisco

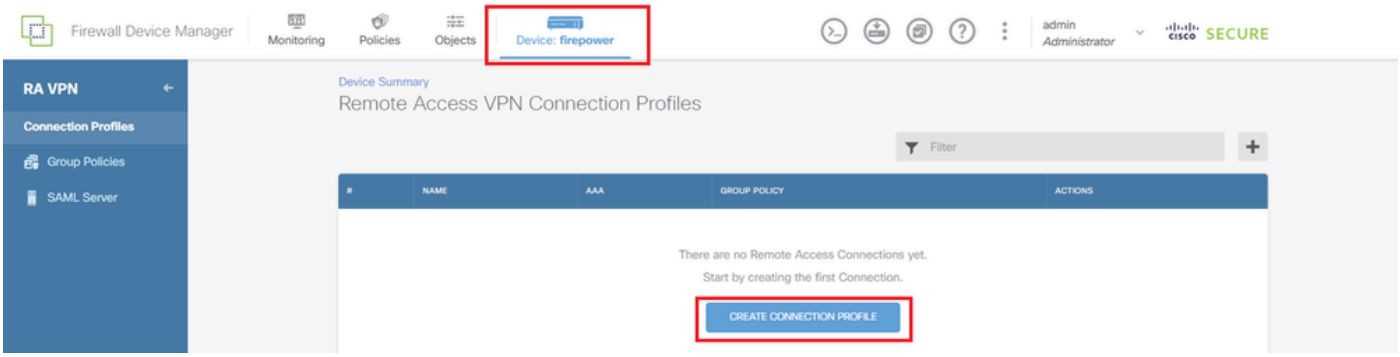
Vaya a Device > Smart License > View Configuration, confirme la licencia de Cisco Secure Client en el elemento RA VPN License.



Licencia de cliente seguro

Paso 3. Agregar perfil de conexión VPN de acceso remoto

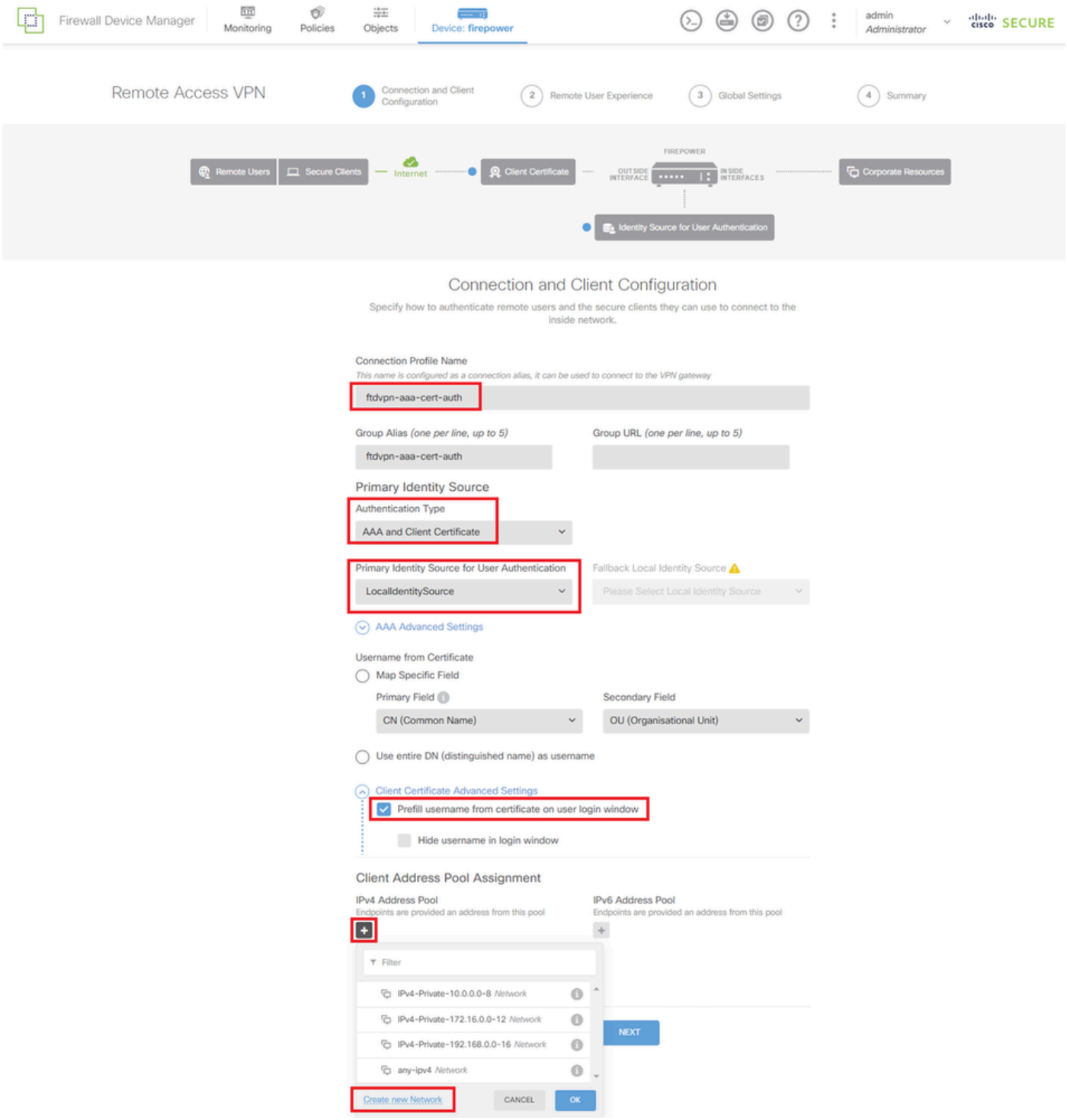
Vaya a Device > Remote Access VPN > View Configuration, haga clic en el botón CREATE CONNECTION PROFILE.



Agregar perfil de conexión VPN de acceso remoto

Introduzca la información necesaria para el perfil de conexión y haga clic en el botón Create new Network en el elemento IPv4 Address Pool.

- Nombre del perfil de conexión: ftdvpn-aaa-cert-auth
- Tipo de autenticación: AAA y certificado de cliente
- Origen de identidad principal para autenticación de usuario: LocalIdentitySource
- Configuración avanzada de certificado de cliente: rellenar el nombre de usuario del certificado en la ventana de inicio de sesión del usuario

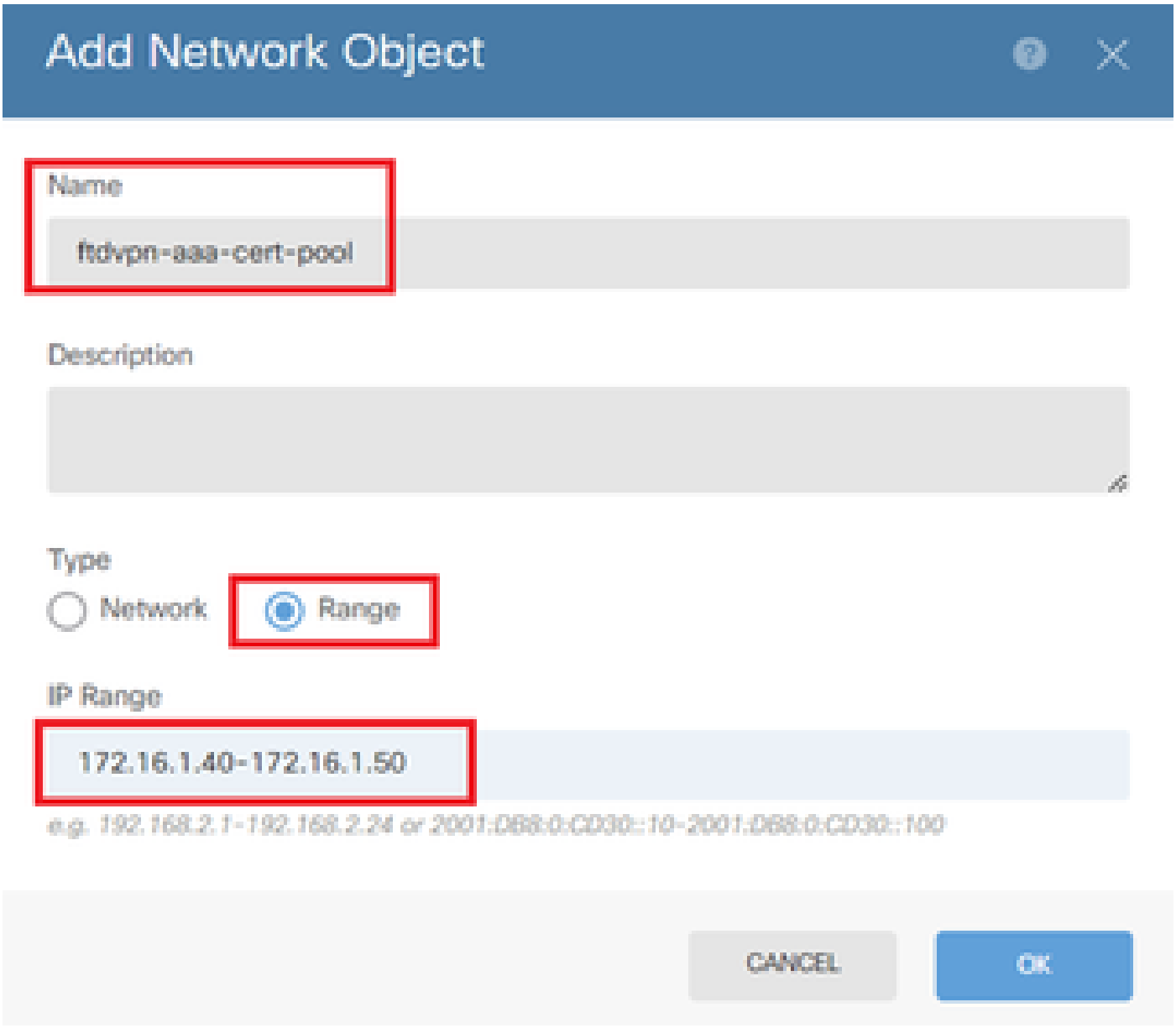


Detalles del perfil de conexión VPN

Paso 4. Agregar conjunto de direcciones para el perfil de conexión

Introduzca la información necesaria para agregar un nuevo conjunto de direcciones IPv4. Seleccione el nuevo conjunto de direcciones IPv4 agregado para el perfil de conexión y haga clic en el botón Next.

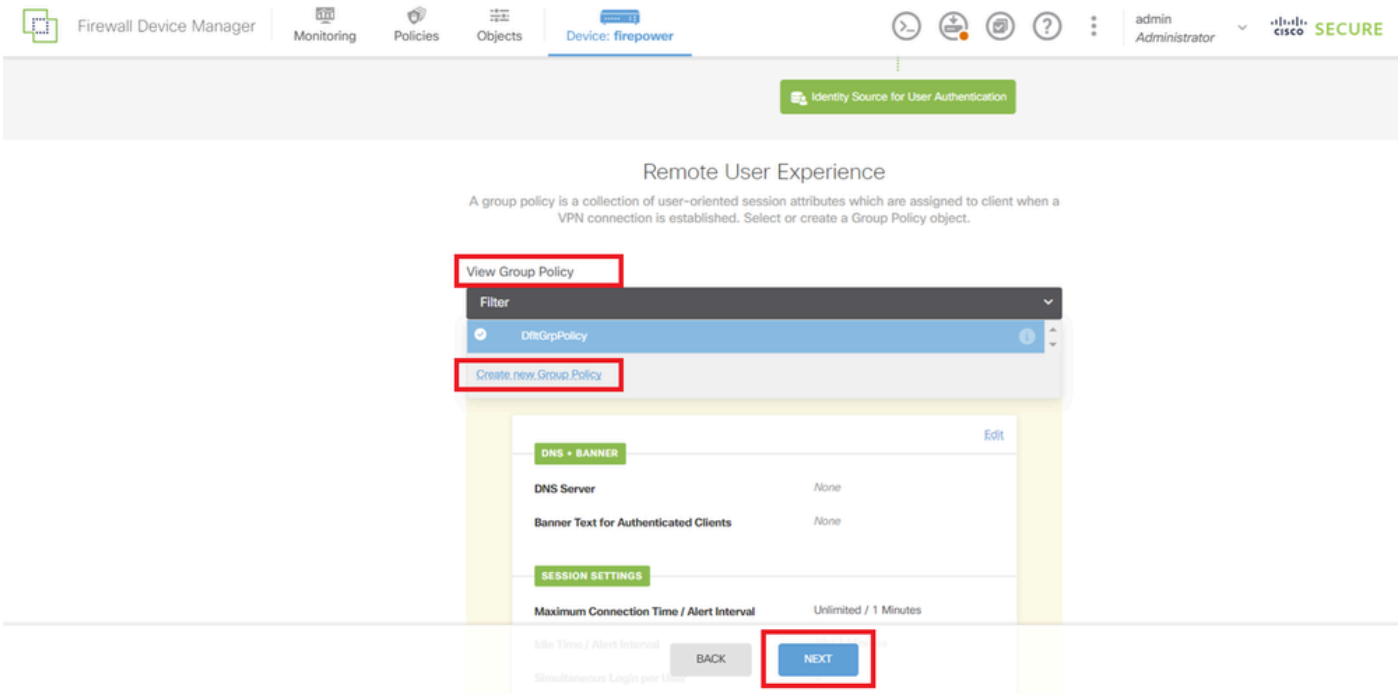
- Nombre: ftdvpn-aaa-cert-pool
- Tipo: Rango
- Intervalo IP: 172.16.1.40-172.16.1.50



Detalles del conjunto de direcciones IPv4

Paso 5. Agregar directiva de grupo para el perfil de conexión

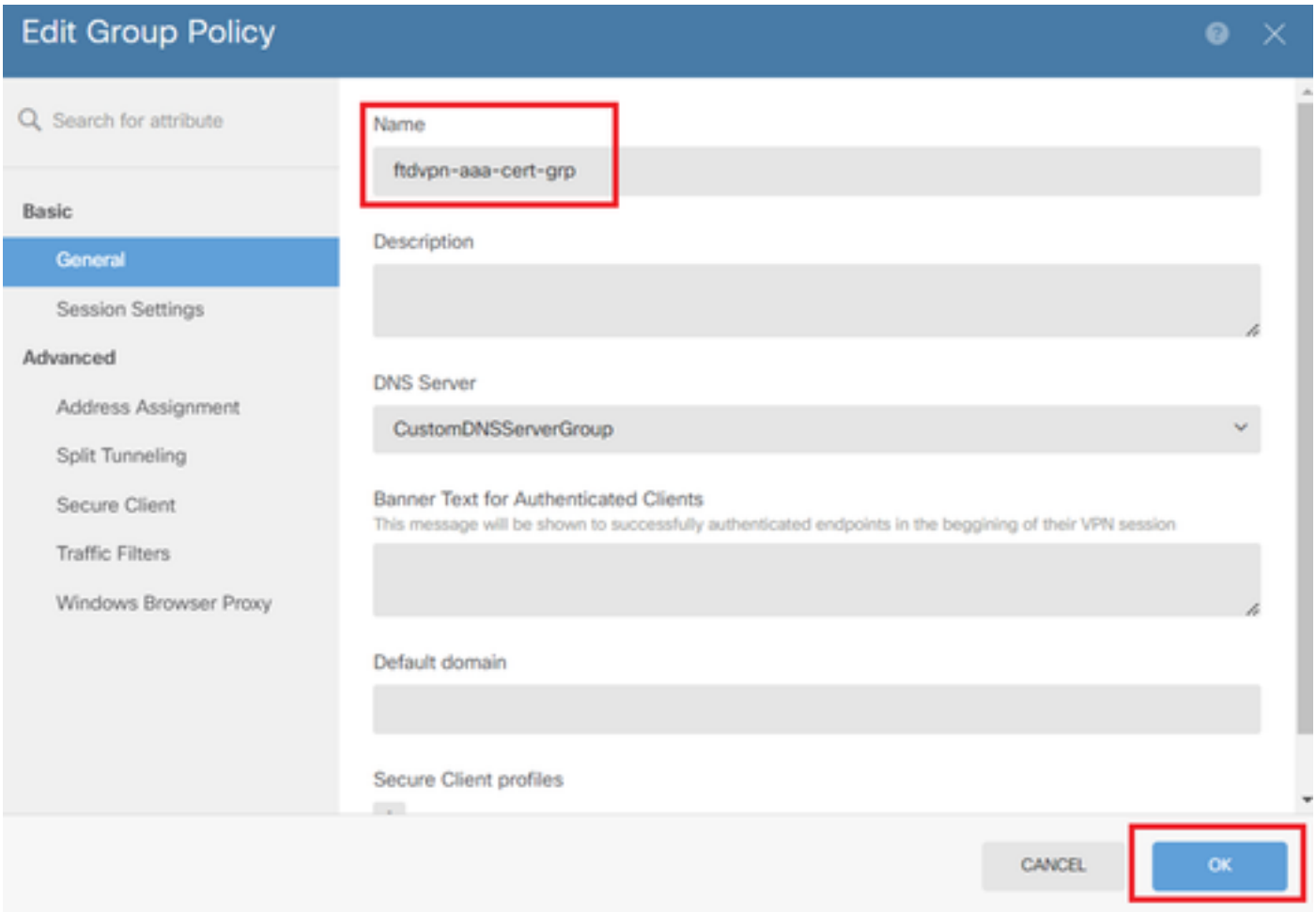
Haga clic en Crear nueva directiva de grupo en el elemento Ver directiva de grupo.



Agregar directiva de grupo

Introduzca la información necesaria para agregar una nueva directiva de grupo y haga clic en el botón Aceptar. Seleccione la nueva directiva de grupo agregada para el perfil de conexión.

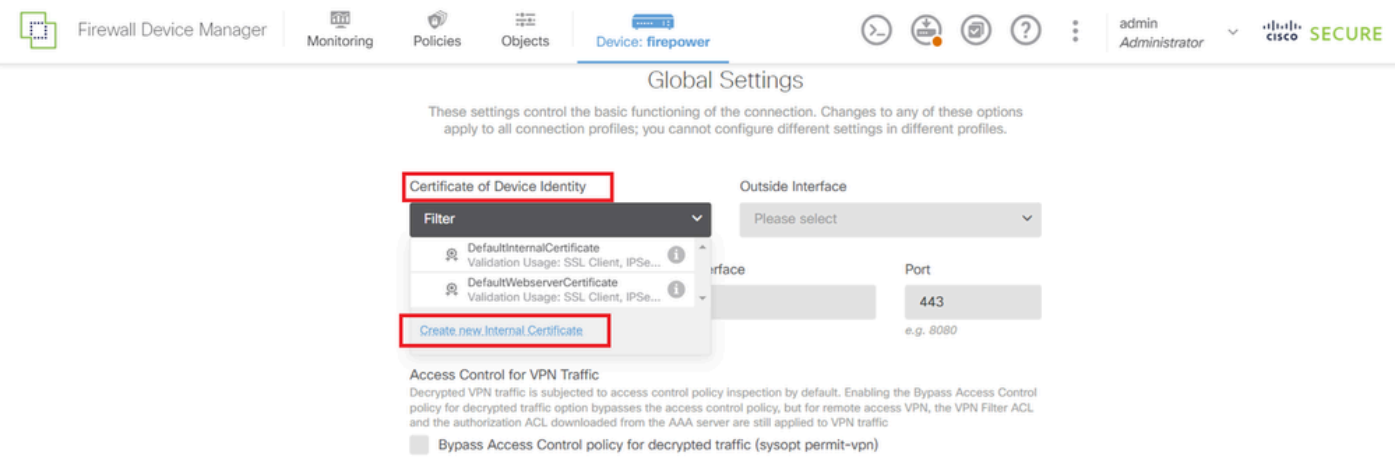
- Nombre: ftdvpn-aaa-cert-grp



Detalles de la directiva de grupo

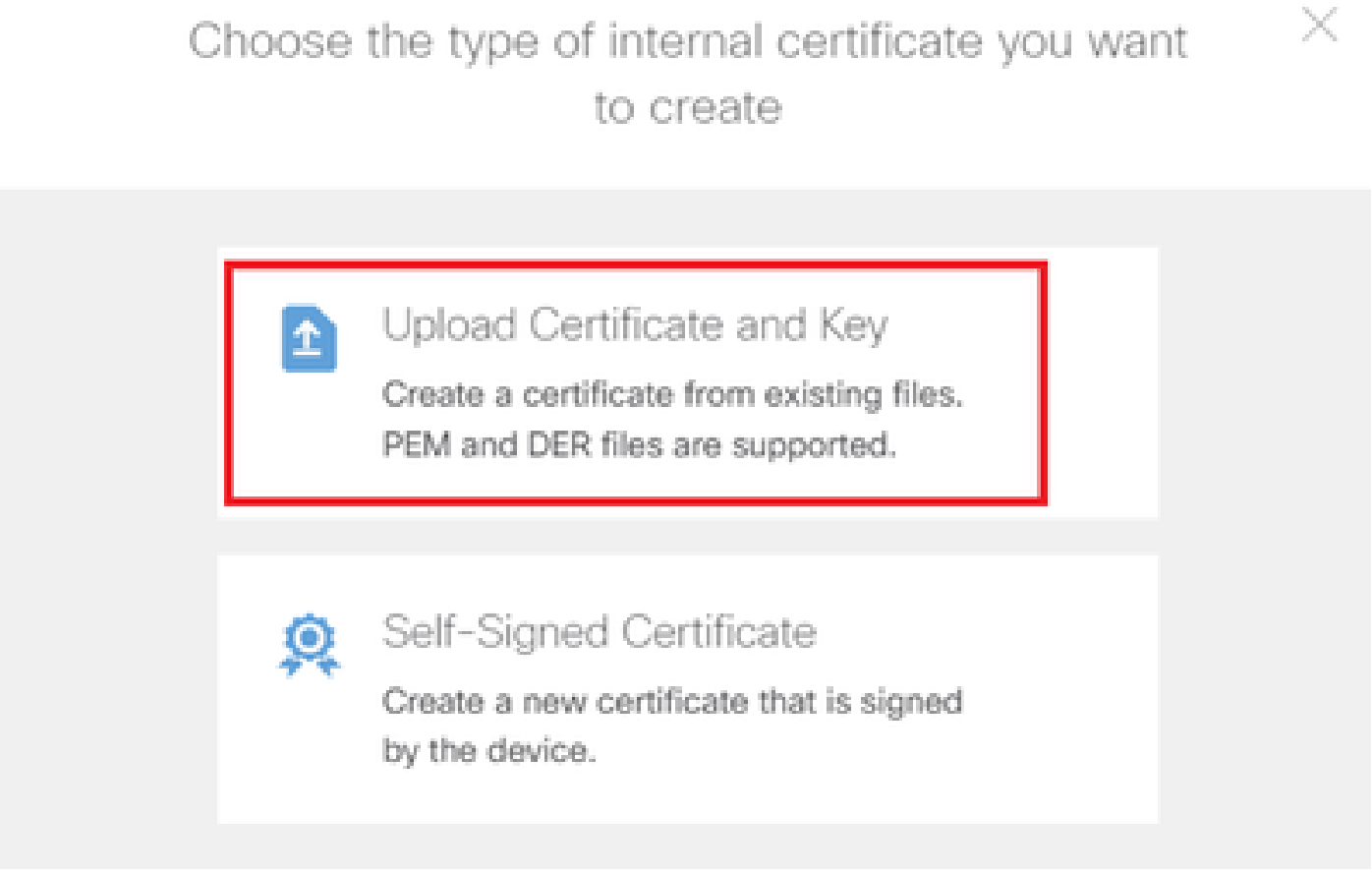
Paso 6. Configuración del certificado de identidad del dispositivo y la interfaz externa para el perfil de conexión

Haga clic en Create new Internal certificate en el elemento Certificate of Device Identity.



Agregar certificado interno

Haga clic en Cargar certificado y clave.

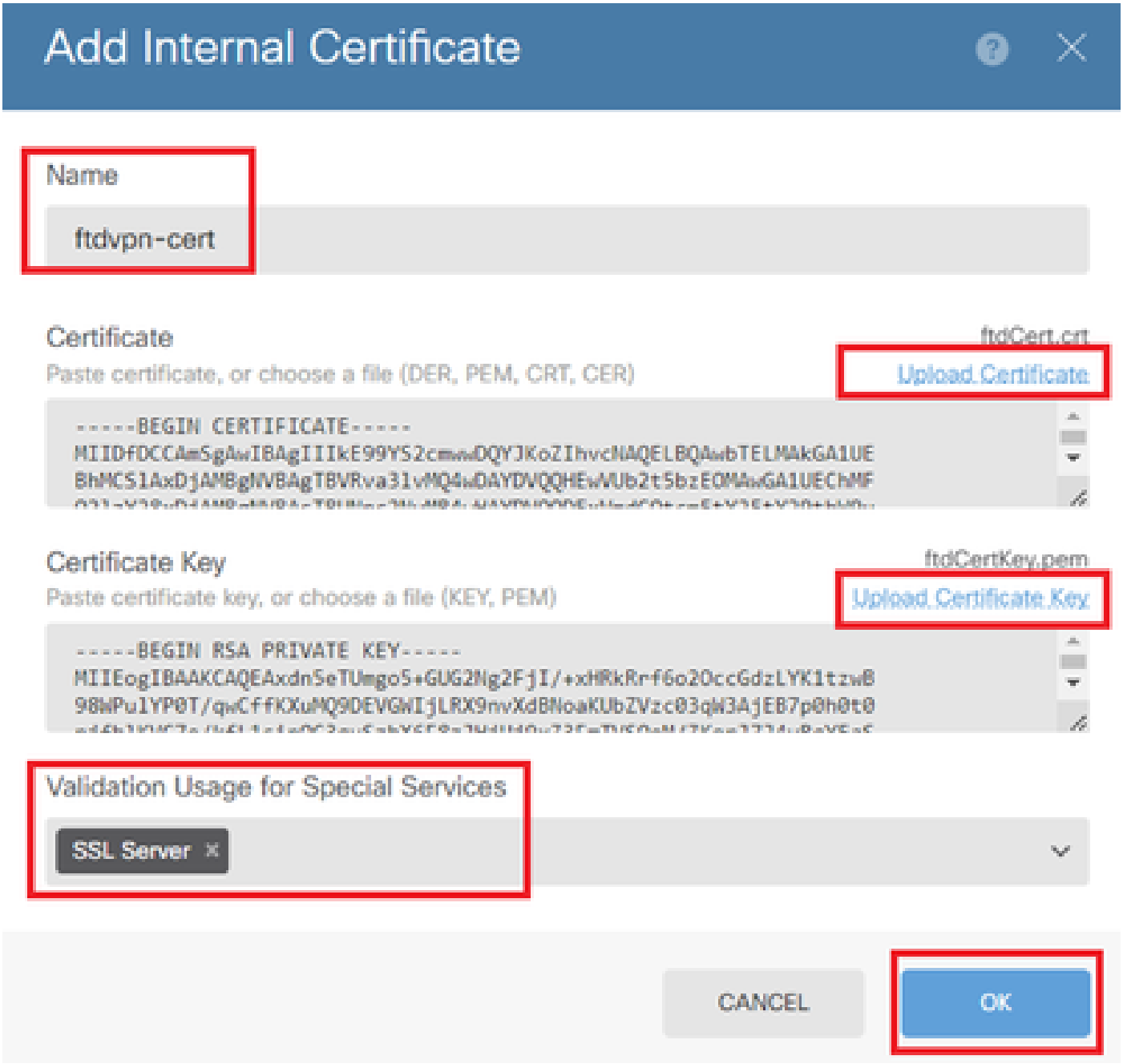


Cargar certificado y clave

Introduzca la información necesaria para el certificado FTD, importe un certificado y una clave de

certificado desde el equipo local y, a continuación, haga clic en el botón Aceptar.

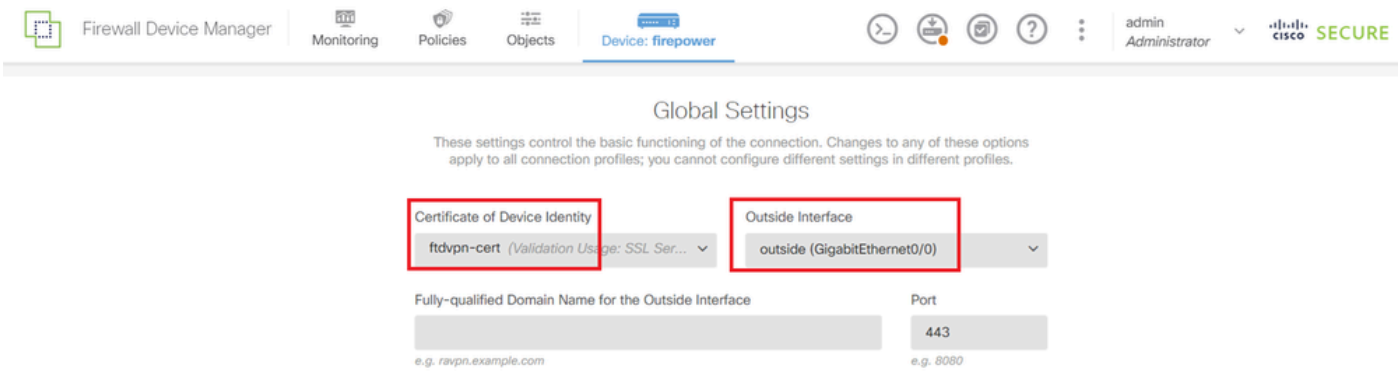
- Nombre: ftdvpn-cert
- Uso de validación para servicios especiales: servidor SSL



Detalles del certificado interno

Seleccione Certificate of Device Identity and Outside Interface para la conexión VPN.

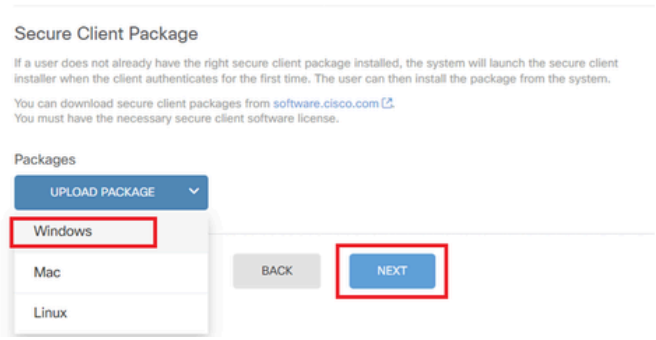
- Certificado de identidad del dispositivo: ftdvpn-cert
- Interfaz externa: externa (GigabitEthernet0/0)



Detalles de la configuración global

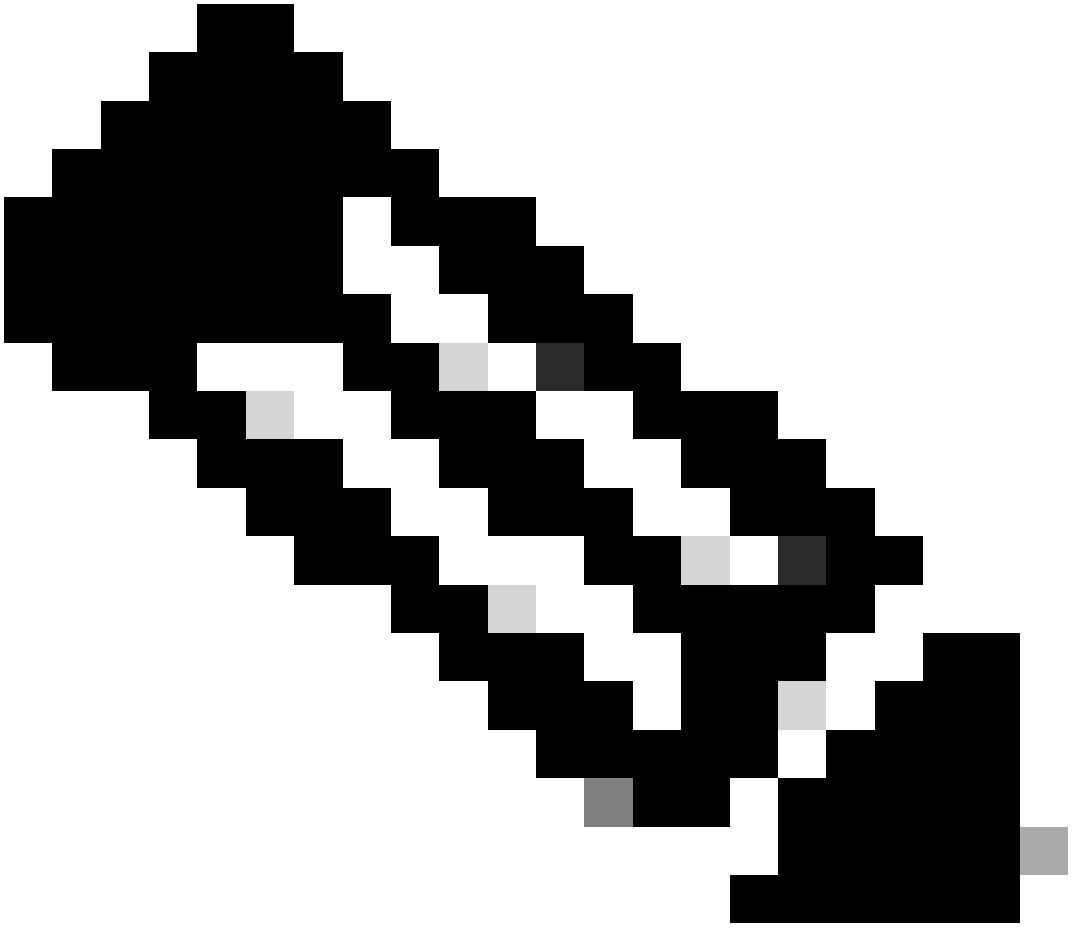
Paso 7. Configurar imagen de cliente seguro para perfil de conexión

Seleccione Windows en el elemento Packages.

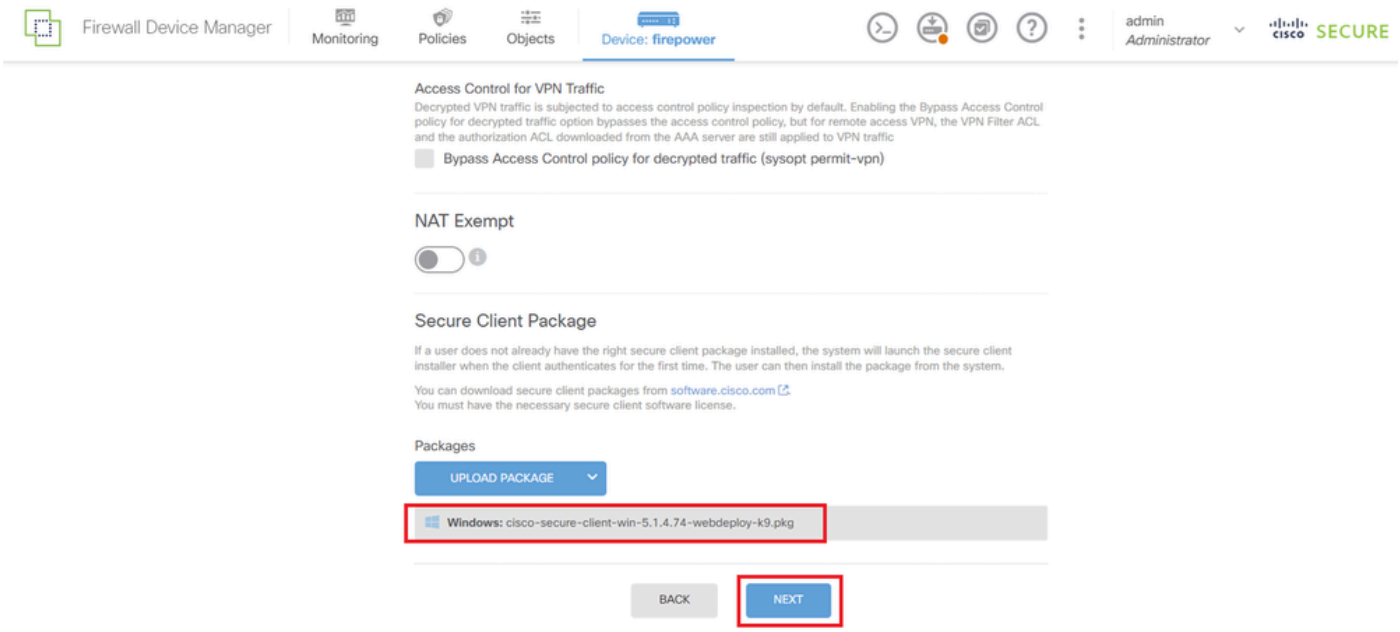


Cargar paquete de imágenes de Secure Client

Cargue el archivo de imagen de cliente seguro desde el equipo local y haga clic en el botón Siguiente.



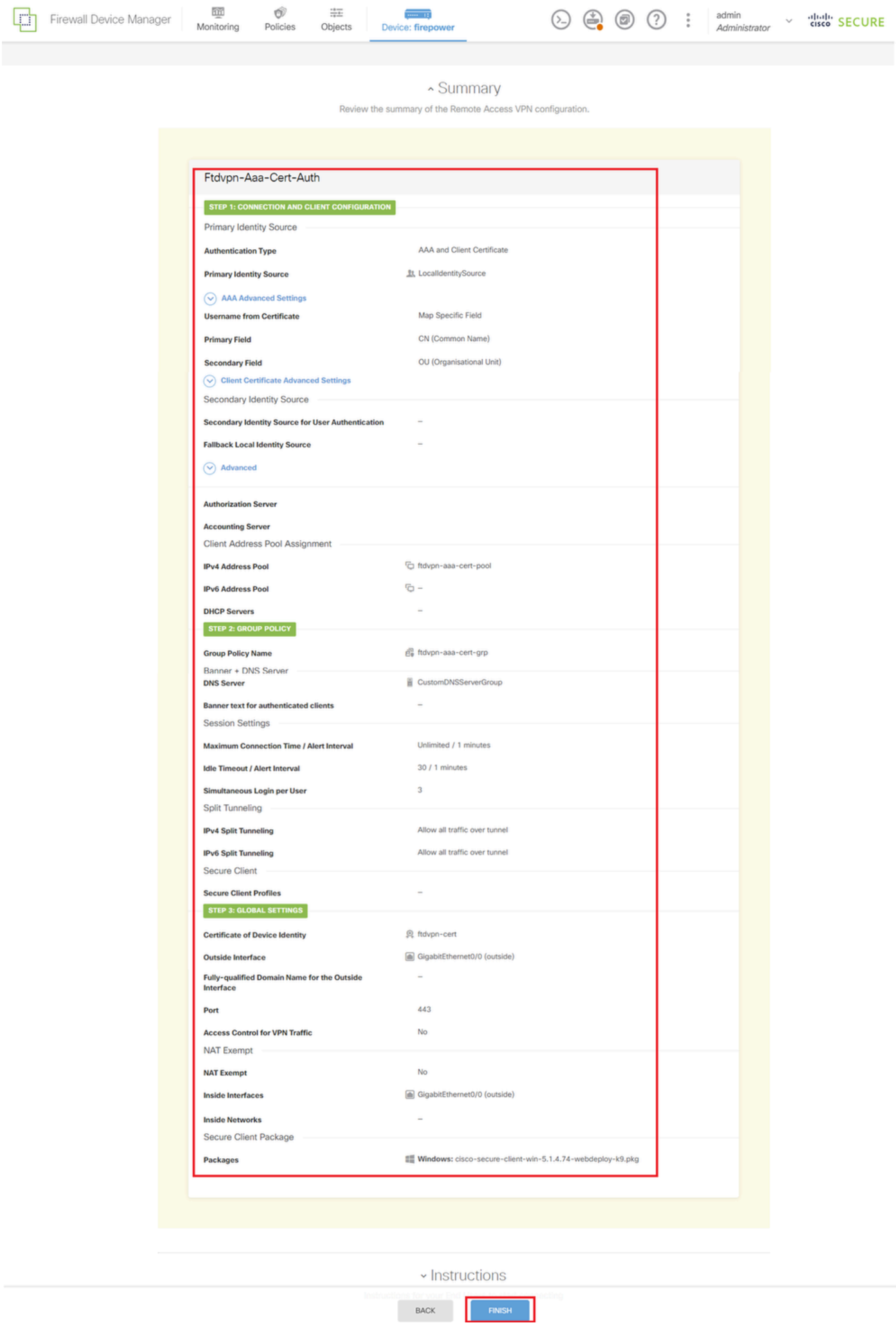
Nota: La función NAT Exempt está inhabilitada en este documento. De forma predeterminada, la opción Omitir directiva de control de acceso para tráfico descifrado (sysopt permit-vpn) está deshabilitada, lo que significa que el tráfico VPN descifrado está sujeto a la inspección de la directiva de control de acceso.



Seleccionar paquete de imágenes de cliente seguro

Paso 8. Confirmar resumen para perfil de conexión

Confirme la información introducida para la conexión VPN y haga clic en el botón FINISH.



Confirmar configuración para el perfil de conexión

```
interface GigabitEthernet0/0
speed auto
nameif outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.1.200 255.255.255.0
!
interface GigabitEthernet0/1
speed auto
nameif inside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.10.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftdvpn-aaa-cert-pool 172.16.1.40-172.16.1.50

// Defines a local user
username sslVPNClientCN password ***** pbkdf2

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftdvpn-cert
enrollment terminal
keypair ftdvpn-cert
validation-usage ssl-server
crl configure

// Server Certificate
crypto ca certificate chain ftdvpn-cert
certificate 22413df584b6726c
3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7
......
quit

// Defines Trustpoint for CA
crypto ca trustpoint ftdvpn-ca-cert
enrollment terminal
validation-usage ssl-client ssl-server
crl configure

// CA
crypto ca certificate chain ftdvpn-ca-cert
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
......
quit

// Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
```

```
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/anyconnpkgs/cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg 2
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Configures the group-policy to allow SSL connections
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-grp attributes
dns-server value 64.x.x.245 64.x.x.184
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
webvpn
anyconnect ssl dtls none
anyconnect mtu 1406
anyconnect ssl keepalive none
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client none
anyconnect dpd-interval gateway none
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules none
anyconnect profiles none
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting

// Configures the tunnel-group to use the aaa & certificate authentication
tunnel-group ftdvpn-aaa-cert-auth type remote-access
tunnel-group ftdvpn-aaa-cert-auth general-attributes
address-pool ftdvpn-aaa-cert-pool
default-group-policy ftdvpn-aaa-cert-grp
// These settings are displayed in the 'show run all' command output. Start
authentication-server-group LOCAL
secondary-authentication-server-group none
no accounting-server-group
default-group-policy ftdvpn-aaa-cert-grp
username-from-certificate CN OU
secondary-username-from-certificate CN OU
authentication-attr-from-server primary
authenticated-session-username primary
username-from-certificate-choice second-certificate
```

```
secondary-username-from-certificate-choice second-certificate
// These settings are displayed in the 'show run all' command output. End
tunnel-group ftdvpn-aaa-cert-auth webvpn-attributes
authentication aaa certificate
pre-fill-username client
group-alias ftdvpn-aaa-cert-auth enable
```

Confirmar en cliente VPN

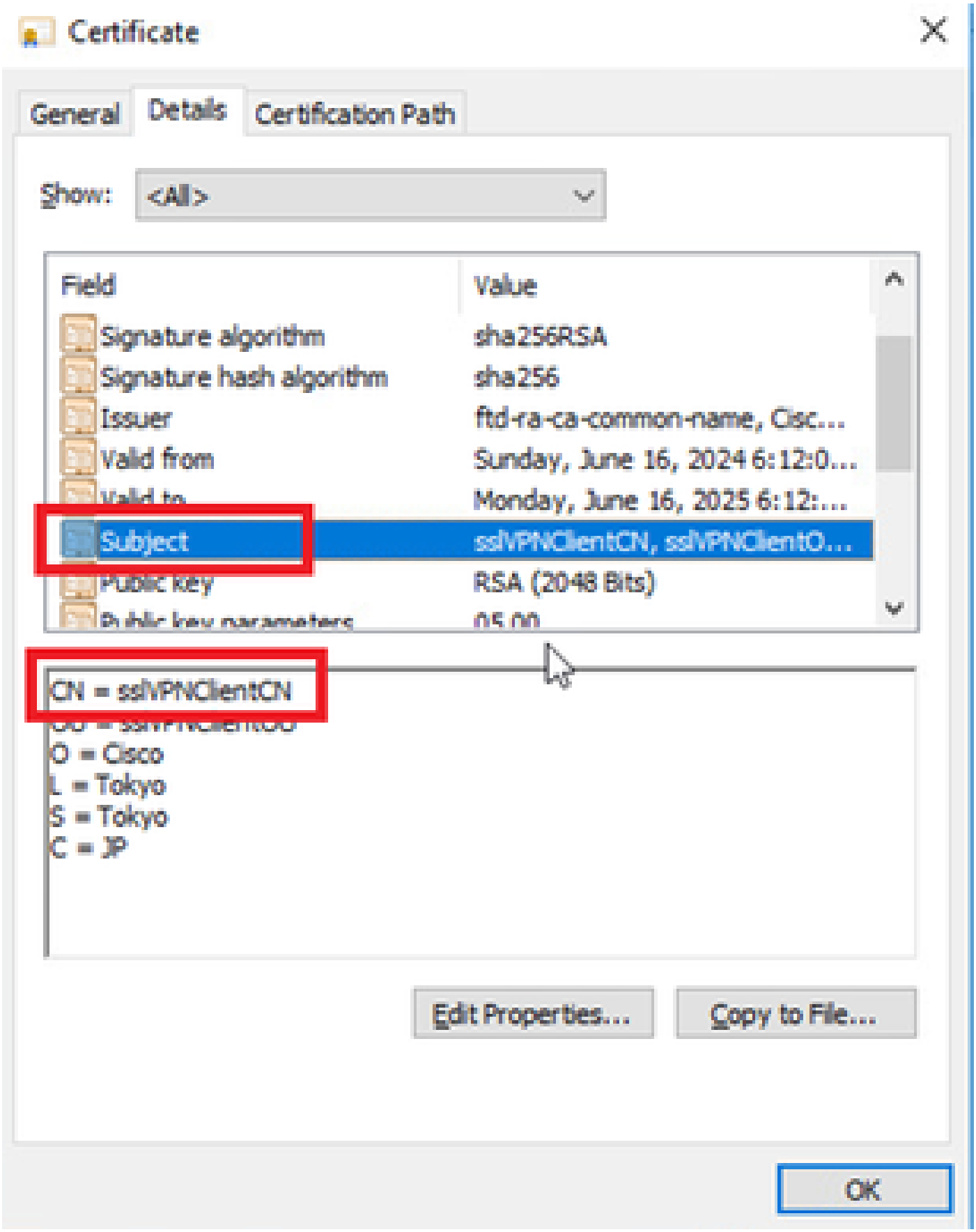
Paso 1. Confirmar certificado de cliente

Navegue hasta Certificados - Usuario actual > Personal > Certificados, verifique el certificado de cliente utilizado para la autenticación.

Confirmar certificado de cliente

Haga doble clic en el certificado de cliente, navegue hastaDetalles, verifique los detalles deAsunto.

- Asunto: CN = sslVPNClientCN



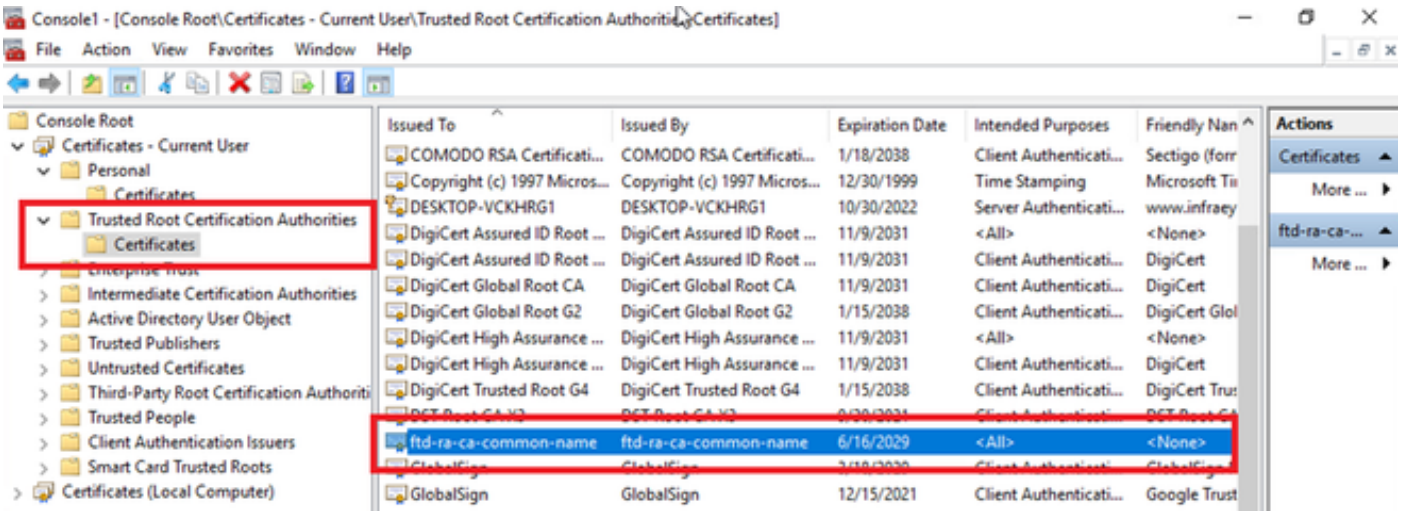
Detalles del certificado de cliente

Paso 2. Confirmar CA

Navegue hasta Certificados - Usuario actual > Entidades de certificación raíz de confianza >

Certificados, verifique la CA utilizada para la autenticación.

- Emitido por: ftd-ra-ca-common-name

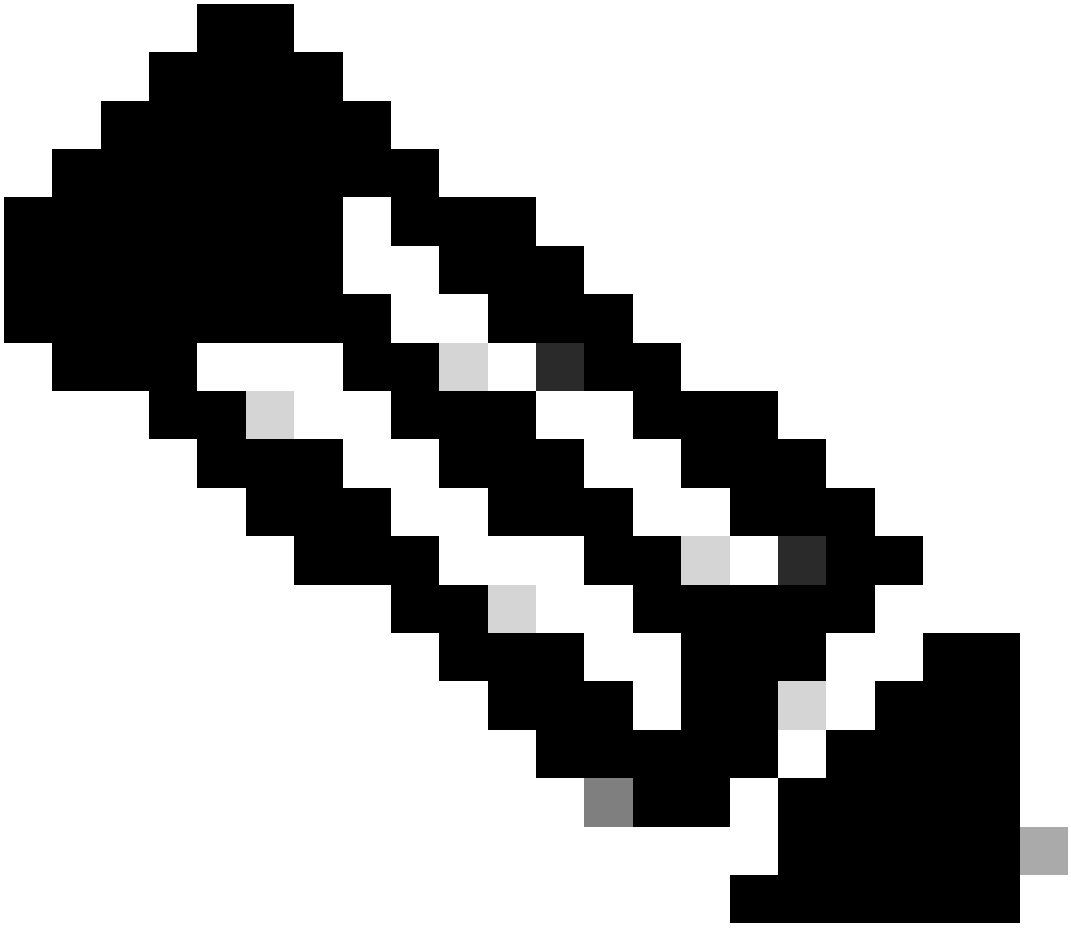


Confirmar CA

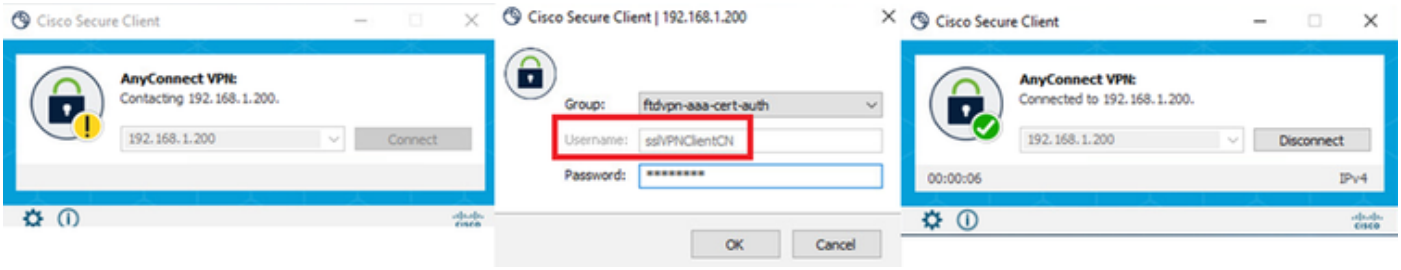
Verificación

Paso 1. Iniciar conexión VPN

En el terminal, inicie la conexión de Cisco Secure Client. El nombre de usuario se extrae del certificado del cliente, debe ingresar la contraseña para la autenticación VPN.



Nota: El nombre de usuario se extrae del campo Common Name (CN) del certificado de cliente de este documento.



Iniciar conexión VPN

Paso 2. Confirmar sesión VPN en CLI de FTD

Ejecuteshow vpn-sessiondb detail anyconnect el comando en la CLI de FTD (Line) para confirmar la sesión VPN.

```
firepower# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 4
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Protocol : AnyConnect-Parent SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384
Bytes Tx : 29072 Bytes Rx : 44412
Pkts Tx : 10 Pkts Rx : 442
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth
Login Time : 11:47:42 UTC Sat Jun 29 2024
Duration : 1h:09m:30s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 000000000004000667ff45e
Security Grp : none Tunnel Zone : 0

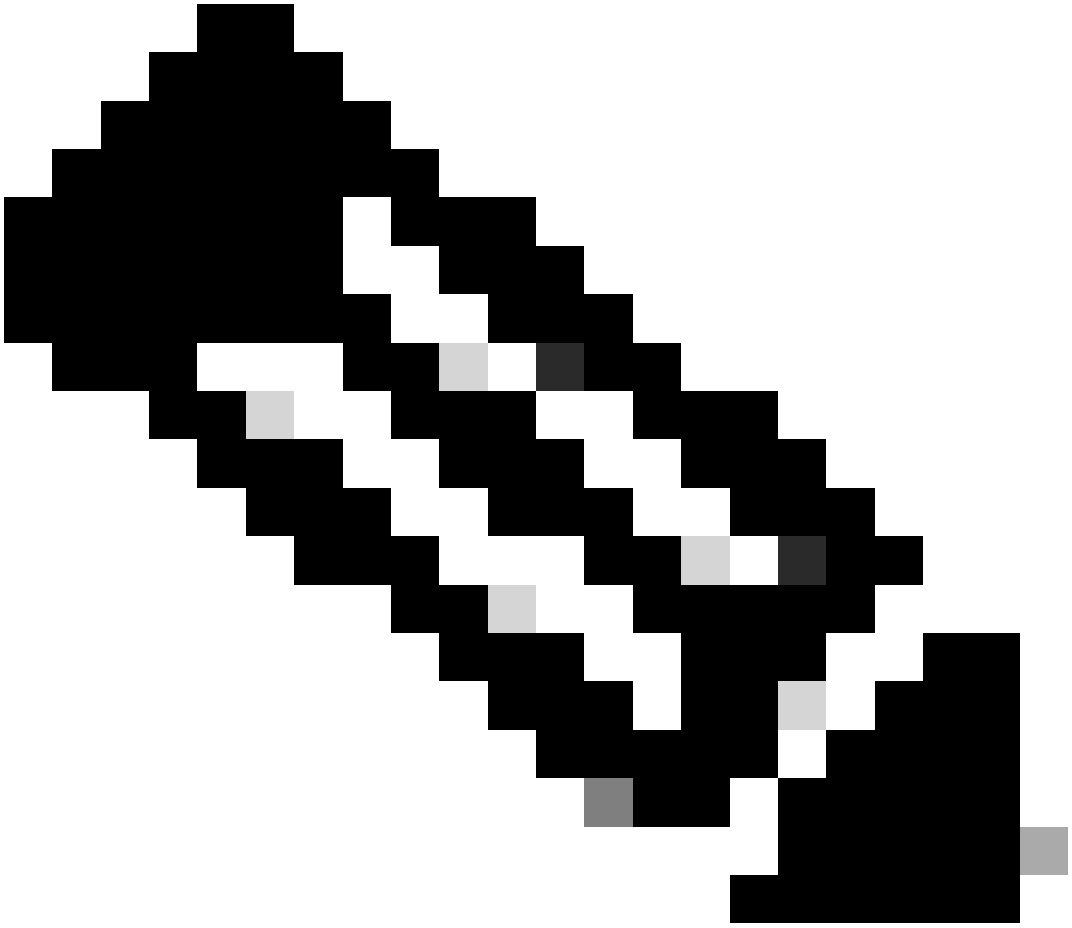
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 4.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 49779 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 7 Minutes
Client OS : win
Client OS Ver: 10.0.17763
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 14356 Bytes Rx : 0
Pkts Tx : 2 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

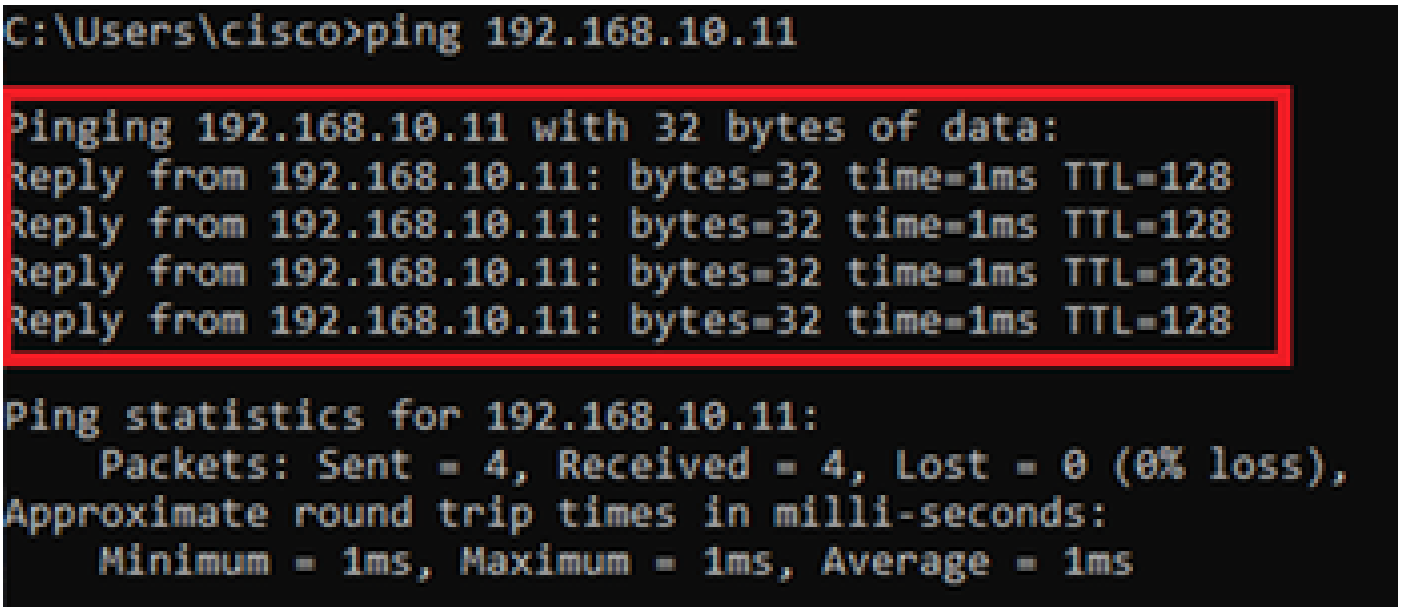
SSL-Tunnel:
Tunnel ID : 4.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 49788
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 7178 Bytes Rx : 10358
Pkts Tx : 1 Pkts Rx : 118
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Paso 3. Confirmar comunicación con el servidor

Inicie el ping desde el cliente VPN al servidor, confirme que la comunicación entre el cliente VPN y el servidor es exitosa.



Nota: dado que la opción Omitir la directiva de control de acceso para tráfico descifrado (sysopt permit-vpn) está deshabilitada en el paso 7, debe crear reglas de control de acceso que permitan el acceso del grupo de direcciones IPv4 al servidor.



Ping correcto

capture in interface inside real-timeEjecute el comando en la CLI de FTD (línea) para confirmar la captura de paquetes.

firepower# capture in interface inside real-time

Warning: using this option with a slow console connection may
result in an excessive amount of non-displayed packets
due to performance limitations.

Use ctrl-c to terminate real-time capture

1: 12:03:26.626691 172.16.1.40 > 192.168.10.11 icmp: echo request
2: 12:03:26.627134 192.168.10.11 > 172.16.1.40 icmp: echo reply
3: 12:03:27.634641 172.16.1.40 > 192.168.10.11 icmp: echo request
4: 12:03:27.635144 192.168.10.11 > 172.16.1.40 icmp: echo reply
5: 12:03:28.650189 172.16.1.40 > 192.168.10.11 icmp: echo request
6: 12:03:28.650601 192.168.10.11 > 172.16.1.40 icmp: echo reply
7: 12:03:29.665813 172.16.1.40 > 192.168.10.11 icmp: echo request
8: 12:03:29.666332 192.168.10.11 > 172.16.1.40 icmp: echo reply

Troubleshoot

Puede esperar encontrar información sobre la autenticación VPN en el registro del sistema de depuración del motor de línea y en el archivo DART en el equipo con Windows.

Este es un ejemplo de los logs de debug en el motor Lina.

// Certificate Authentication
Jun 29 2024 11:29:37: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=sslV
Jun 29 2024 11:29:37: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked.
Jun 29 2024 11:29:37: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name: CN=sslVPNClientCN

// Extract username from the CN (Common Name) field
Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has been requested. [Request 3]
Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has completed. [Request 3]

// AAA Authentication
Jun 29 2024 11:29:53: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN
Jun 29 2024 11:29:53: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN
Jun 29 2024 11:29:53: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN

Estas depuraciones se pueden ejecutar desde la CLI de diagnóstico del FTD, que proporciona información que puede utilizar para solucionar problemas de configuración.

- debug crypto ca 14
- debug webvpn anyconnect 255
- debug crypto ike-common 255

Información Relacionada

Configuración del servicio de gestión integrada de FDM para Firepower 2100

Configurar VPN de acceso remoto en FTD administrado por FDM

Configuración y verificación de Syslog en el administrador de dispositivos Firepower

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).