Configuración de AAA y autenticación de certificado para Secure Client en FTD a través de FMC

Contenido

Introducción

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

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Firepower Management Center (FMC)
- Firewall Threat Defence Virtual (FTD)
- Flujo de autenticación VPN

Componentes Utilizados

- Cisco Firepower Management Center para VMWare 7.4.1
- Cisco Firewall Threat Defence Virtual 7.4.1

- Cisco Secure Client 5.1.3.62

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

A medida que las organizaciones adoptan medidas de seguridad más estrictas, la combinación de la autenticación de dos factores (2FA) con la autenticación basada en certificados se ha convertido en una práctica habitual para mejorar la seguridad y proteger frente al acceso no autorizado. Una de las funciones que puede mejorar significativamente la experiencia del usuario y la seguridad es la capacidad de rellenar previamente el nombre de usuario en Cisco Secure Client. Esta función simplifica el proceso de inicio de sesión y mejora la eficacia general del acceso remoto.
Este documento describe cómo integrar el nombre de usuario preconfigurado con Cisco Secure Client en FTD, asegurando que los usuarios puedan conectarse de forma rápida y segura a la red.

Estos certificados contienen un nombre común que se utiliza para fines de autorización.

- 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.

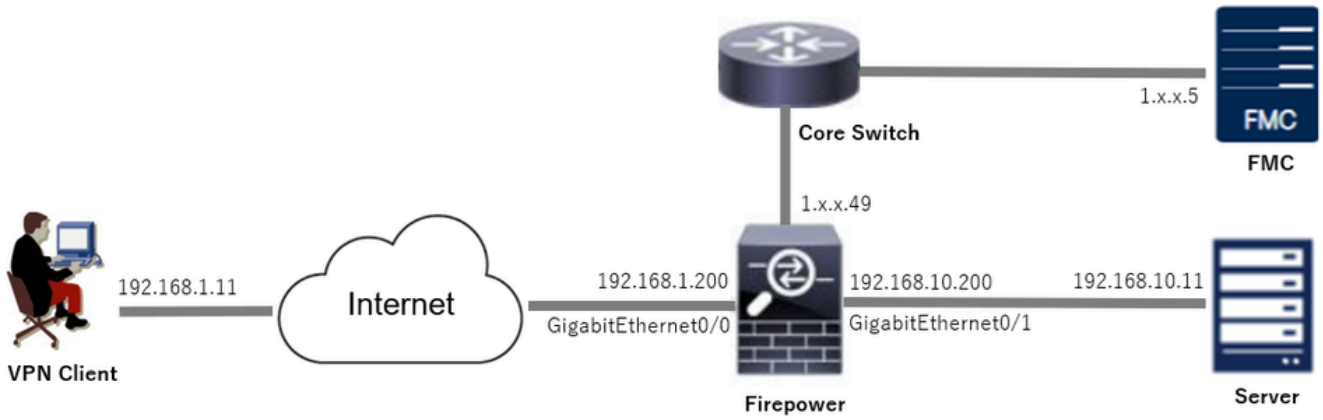


Diagrama de la red

Configuraciones

Configuración en FMC

Paso 1. Configuración de la interfaz FTD

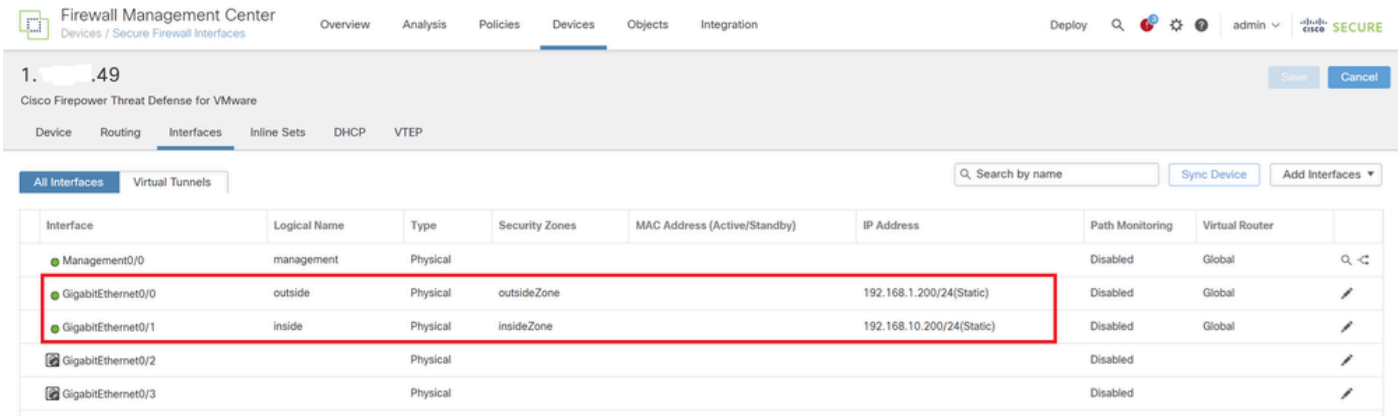
Navegue hasta Devices > Device Management, edite el dispositivo FTD de destino, configure la interfaz interna y externa para FTD en la pestaña Interfaces.

Para GigabitEthernet0/0,

- Nombre: externo
- Zona de seguridad: outsideZone
- Dirección IP: 192.168.1.200/24

Para GigabitEthernet0/1,

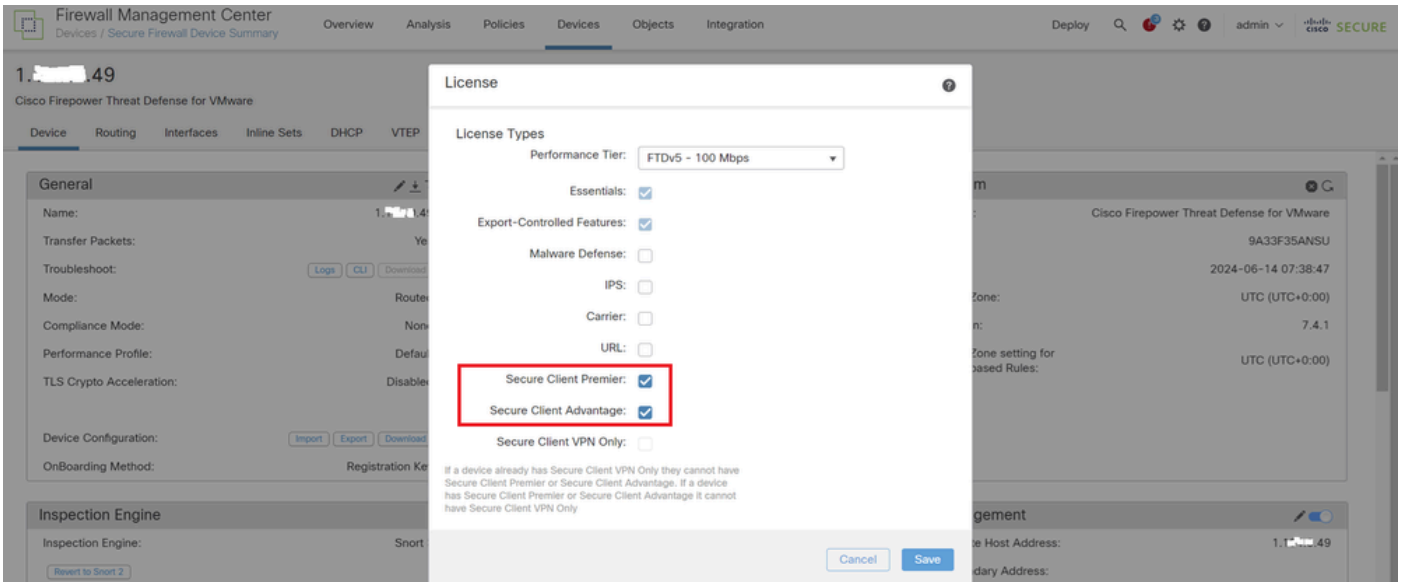
- Nombre: inside
- Zona de seguridad: insideZone
- Dirección IP: 192.168.10.200/24



Interfaz FTD

Paso 2. Confirmar licencia de cliente seguro de Cisco

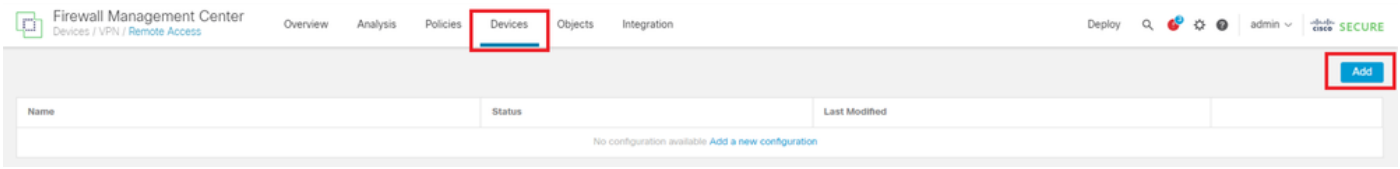
Navegue hasta Devices > Device Management, edite el dispositivo FTD de destino, confirme la licencia de Cisco Secure Client en la pestaña Device.



Licencia de cliente seguro

Paso 3. Agregar asignación de directiva

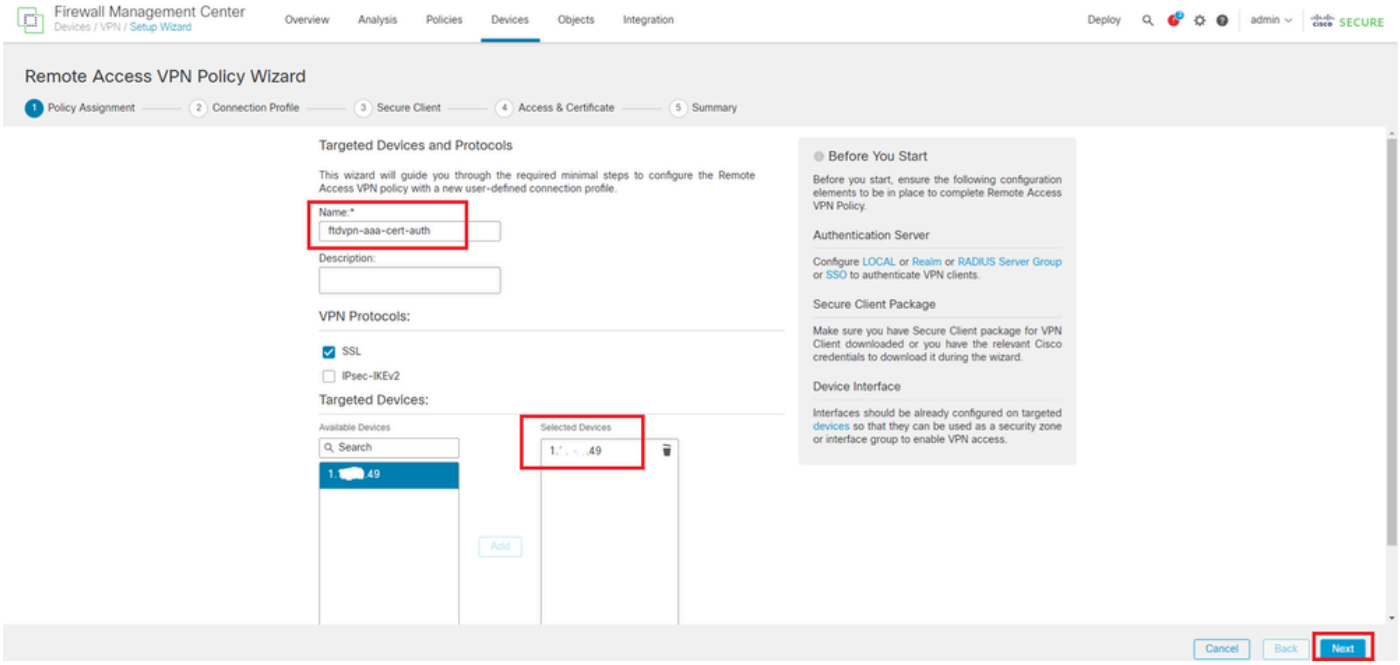
Navegue hasta Devices > VPN > Remote Access, haga clic en el botón Add.



Agregar VPN de acceso remoto

Introduzca la información necesaria y haga clic en el botón Next.

- Nombre: ftdvpn-aaa-cert-auth
- Protocolos VPN: SSL
- Dispositivos objetivo: 1.x.x.49

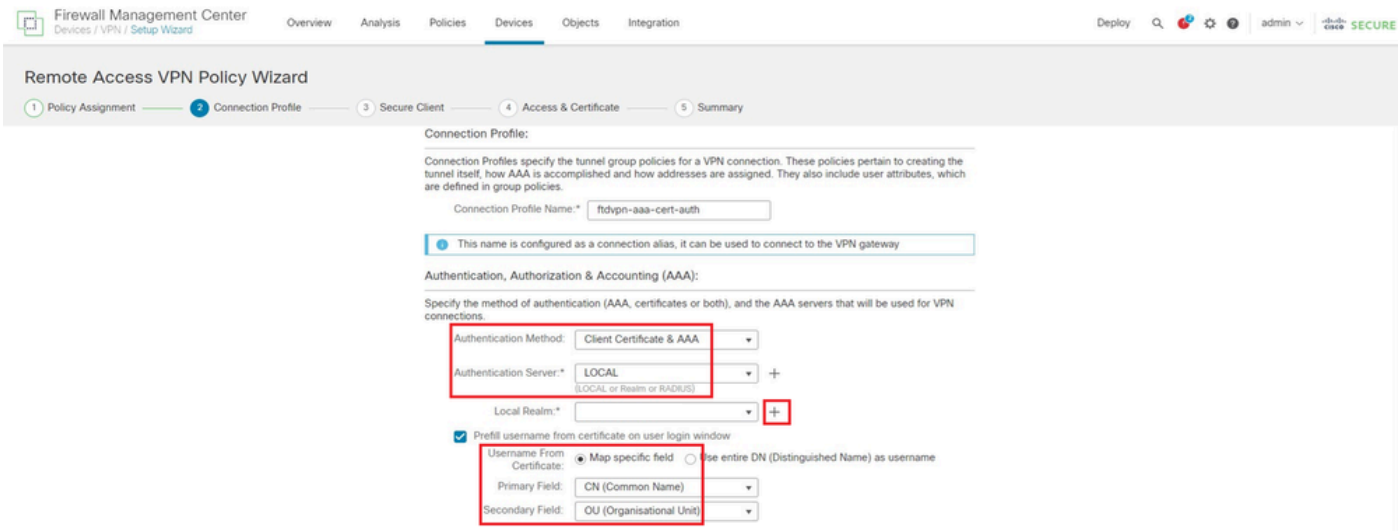


Asignación de políticas

Paso 4. Detalles de configuración para el perfil de conexión

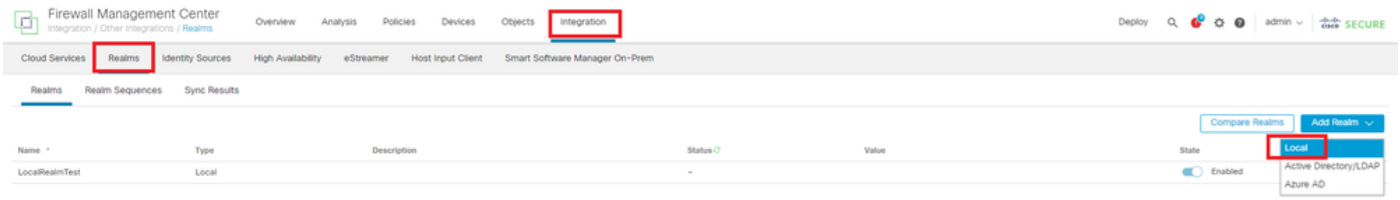
Introduzca la información necesaria para el perfil de conexión y haga clic en el botón + situado junto al elemento Dominio local.

- Método de autenticación: certificado de cliente y AAA
- Servidor de autenticación: LOCAL
- Nombre de usuario del certificado: campo específico de asignación
- Campo principal: CN (nombre común)
- Campo secundario: OU (unidad organizativa)



Detalles del perfil de conexión

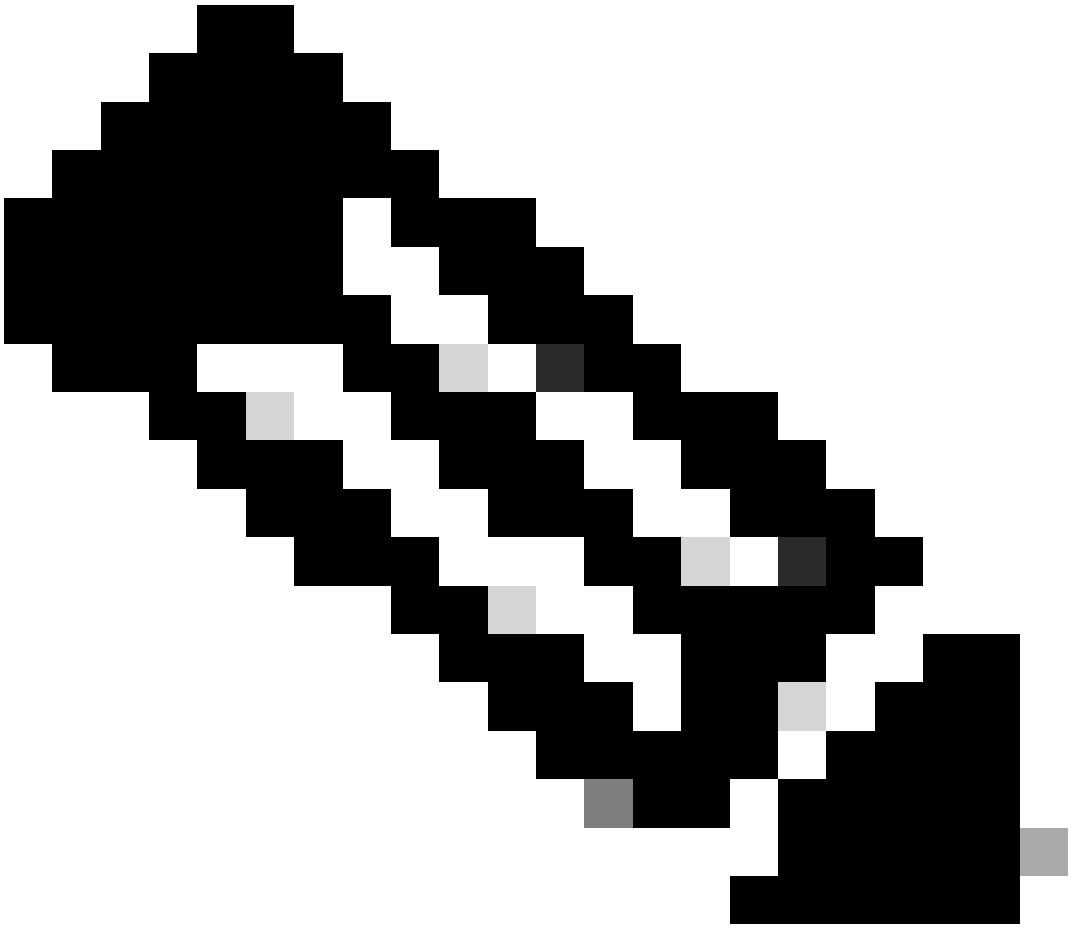
Haga clic en Local de la lista desplegable Add Realm para agregar un nuevo rango local.



Agregar rango local

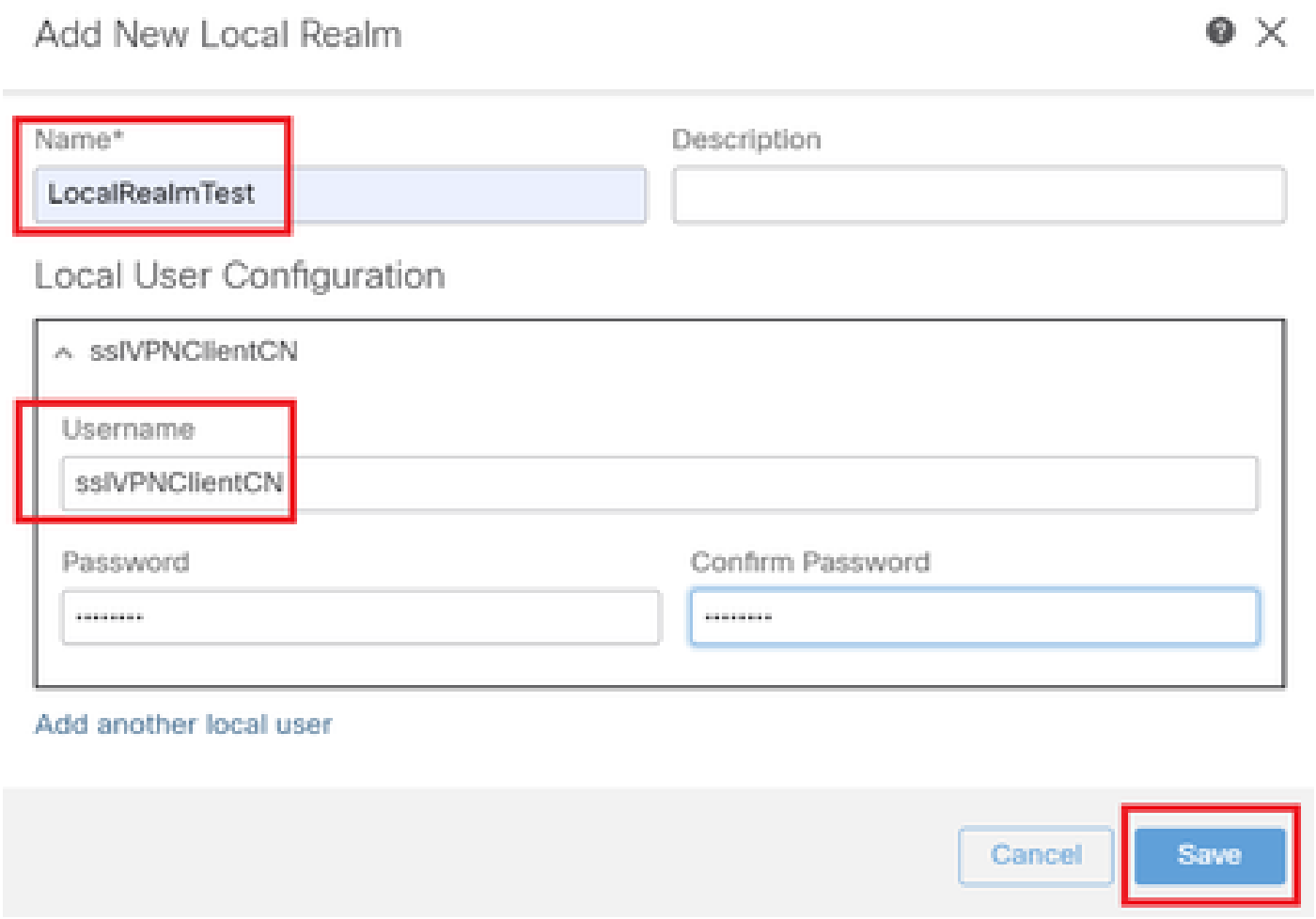
Introduzca la información necesaria para el rango local y haga clic en el botón Save.

- Nombre: LocalRealmTest
- Nombre de usuario: sslVPNClientCN



Nota: El nombre de usuario es igual al nombre común dentro del certificado del cliente

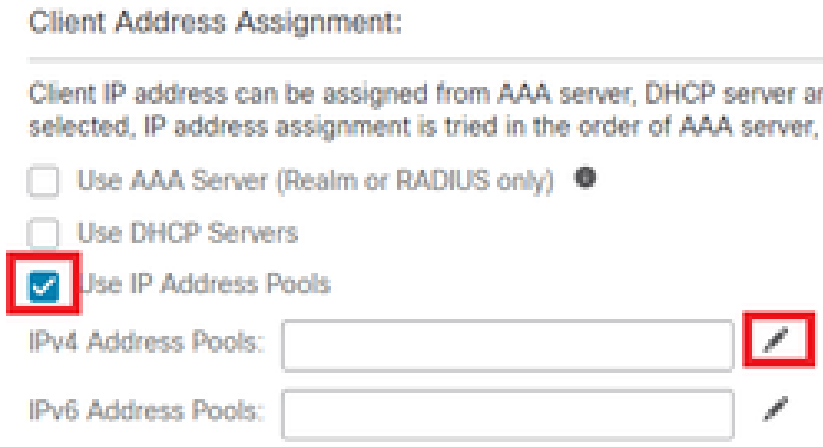
---



Detalles del rango local

Paso 5. Agregar conjunto de direcciones para el perfil de conexión

Haga clic en el botón edit junto al elemento IPv4 Address Pools.

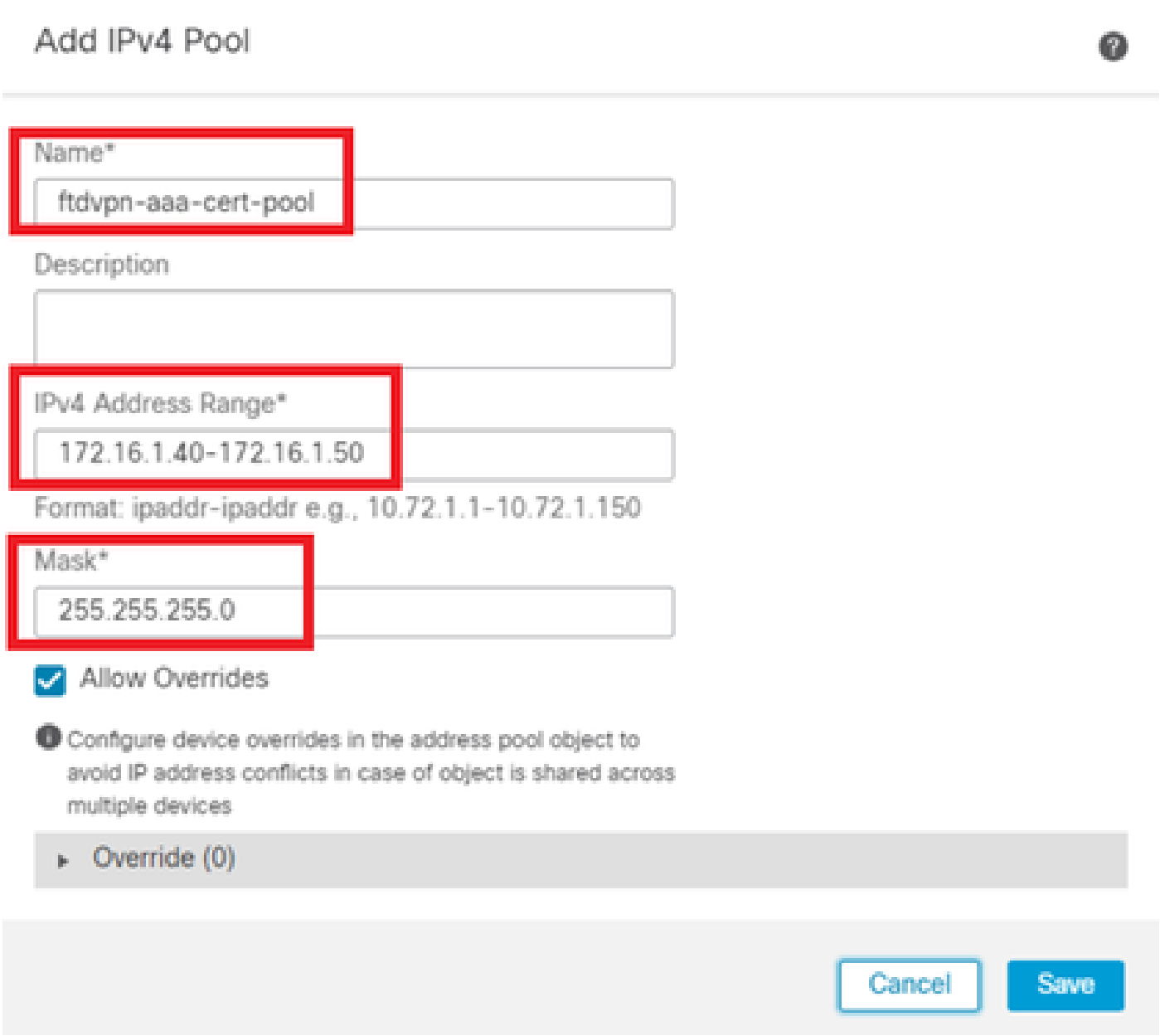


Agregar conjunto de direcciones IPv4

Introduzca la información necesaria para agregar un nuevo conjunto de direcciones IPv4. Seleccione el nuevo conjunto de direcciones IPv4 para el perfil de conexión.

- Nombre: ftdvpn-aaa-cert-pool
- Intervalo de direcciones IPv4: 172.16.1.40-172.16.1.50

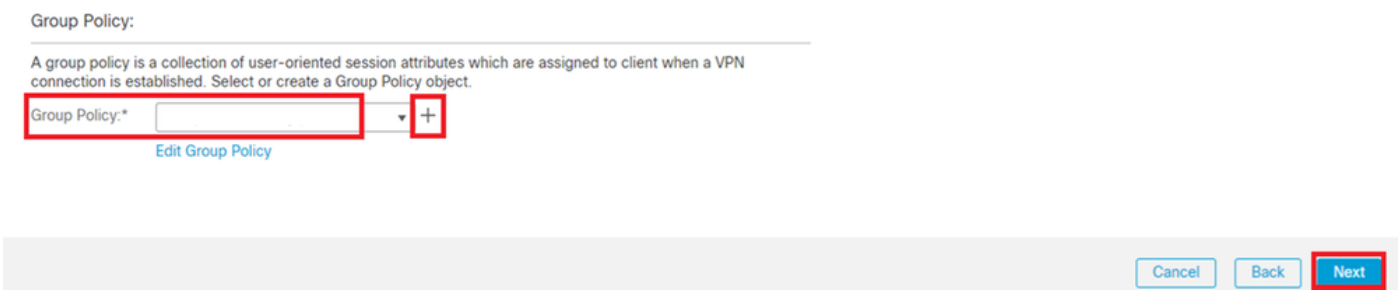
- Máscara: 255.255.255.0



Detalles del conjunto de direcciones IPv4

Paso 6. Agregar directiva de grupo para el perfil de conexión

Haga clic en el botón + situado junto al elemento Directiva de grupo.

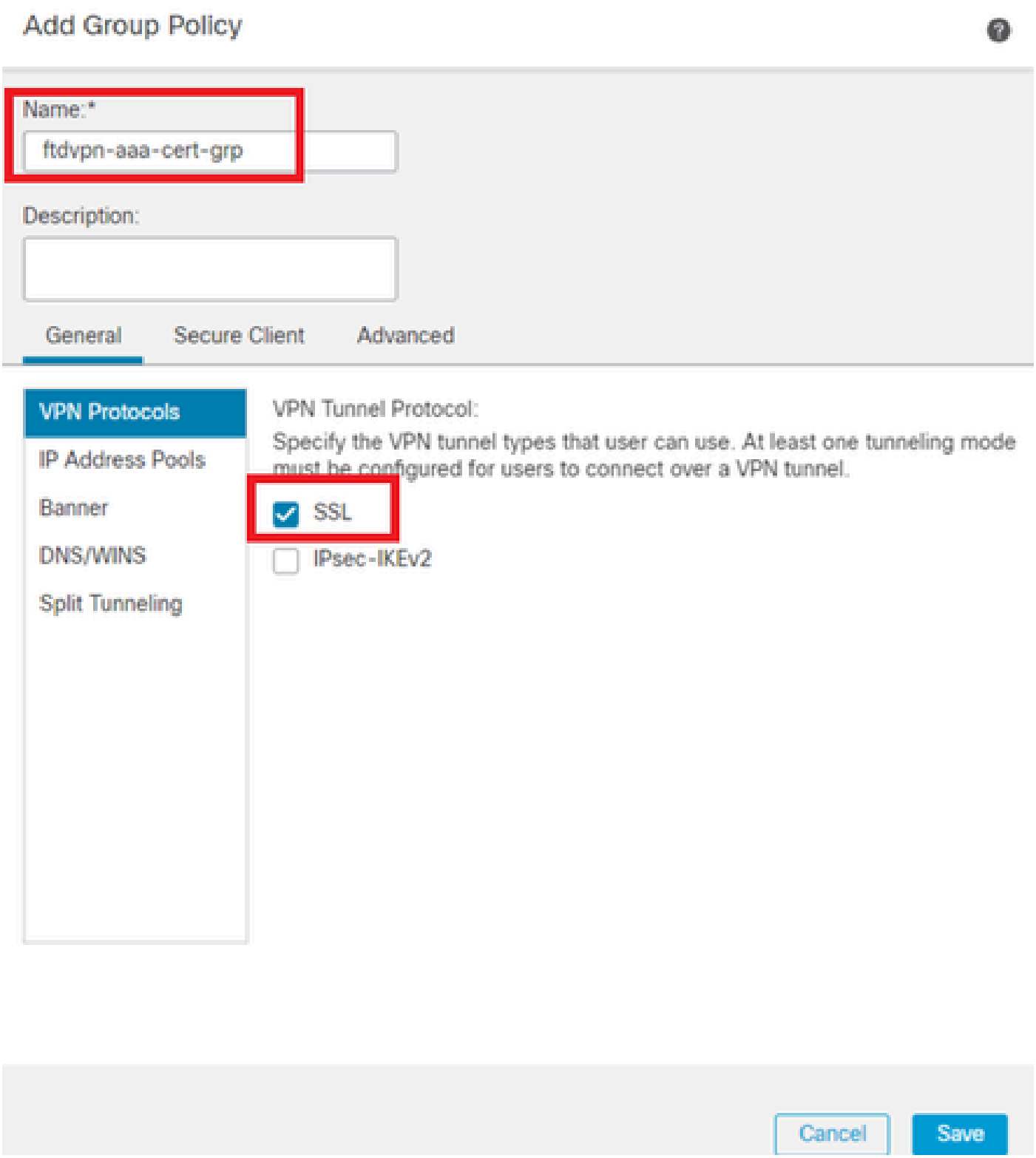


Agregar directiva de grupo

Introduzca la información necesaria para agregar una nueva directiva de grupo. Seleccione la

nueva directiva de grupo para el perfil de conexión.

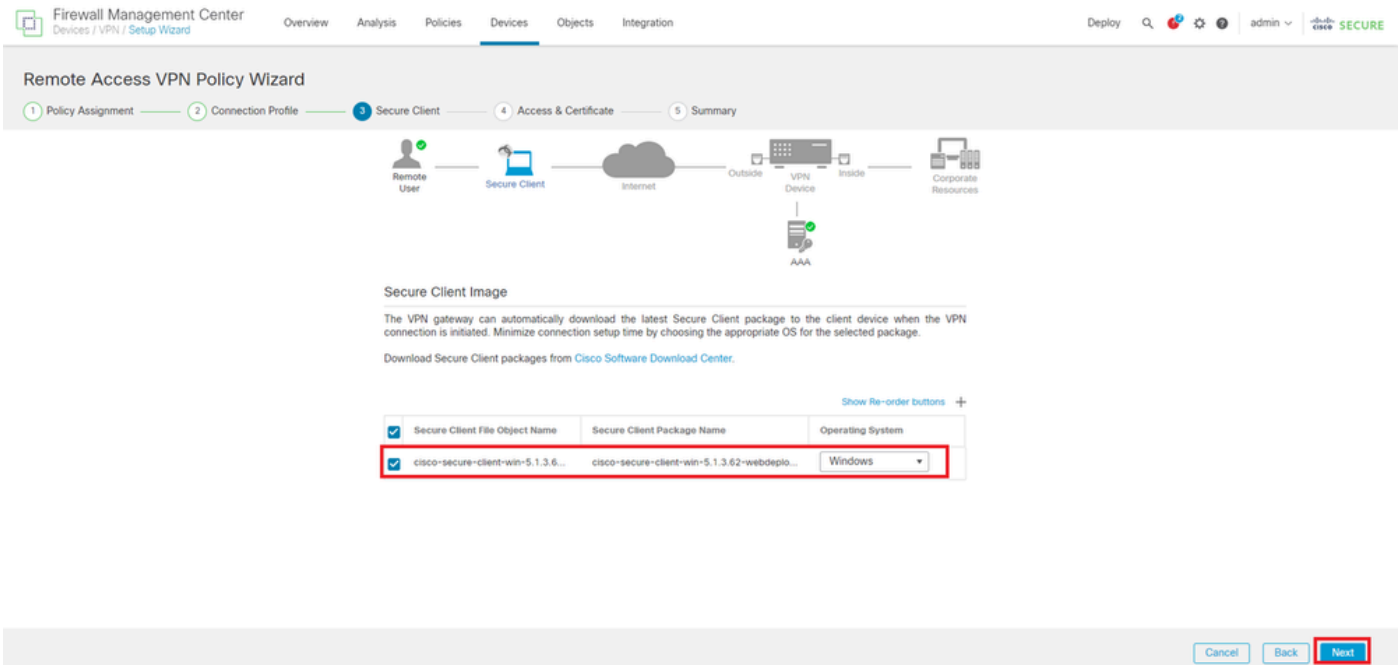
- Nombre: ftdvpn-aaa-cert-grp
- Protocolos VPN: SSL



Detalles de la directiva de grupo

Paso 7. Configurar imagen de Secure Client para perfil de conexión

Seleccione el archivo de imagen de cliente seguro y haga clic en el botón Next.



Seleccionar imagen de cliente seguro

Paso 8. Configurar acceso y certificado para el perfil de conexión

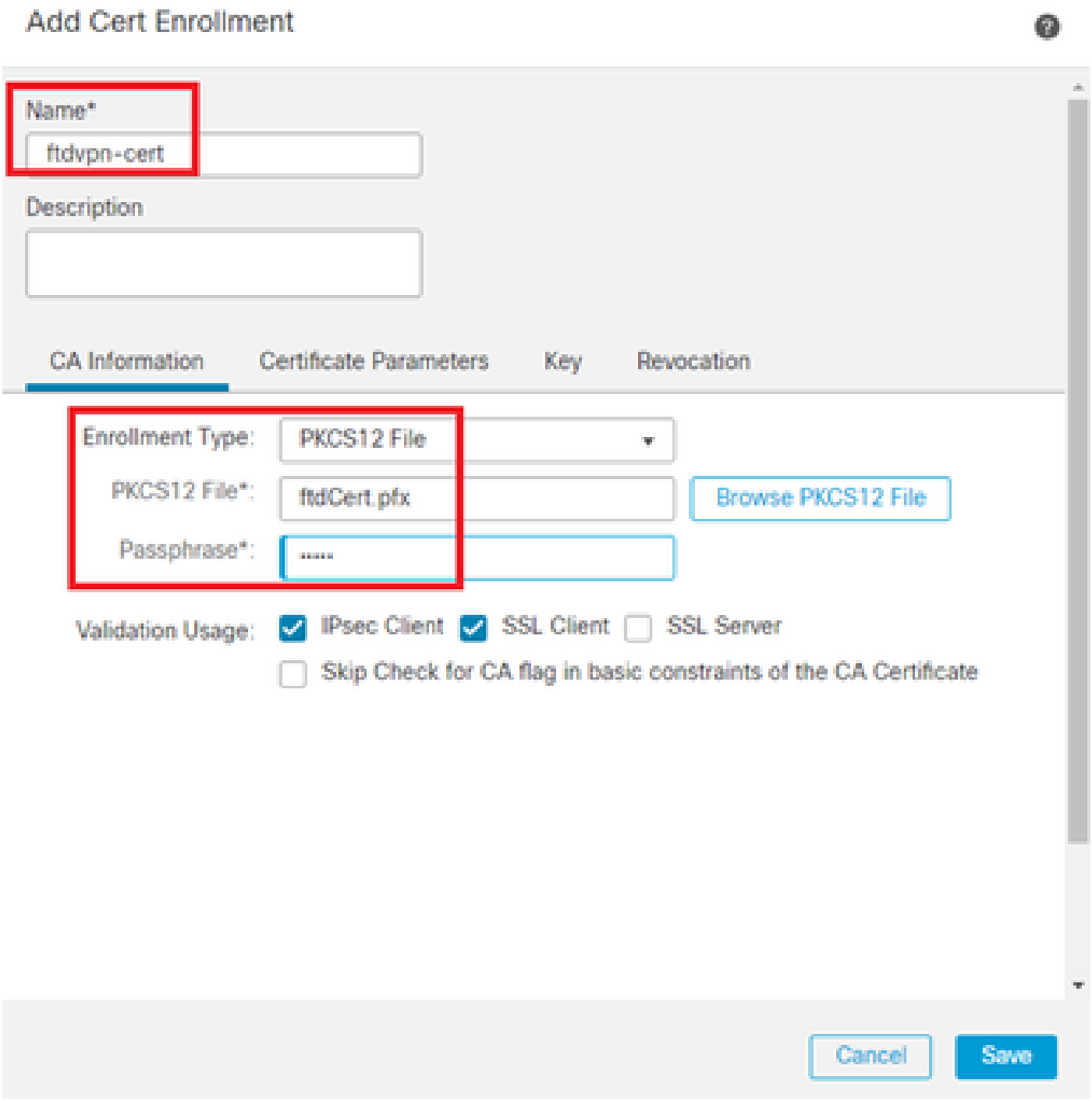
Seleccione Security Zone para la conexión VPN y haga clic en el botón + junto al elemento Certificate Enrollment.

- Grupo de interfaz/Zona de seguridad: outsideZone

Seleccionar zona de seguridad

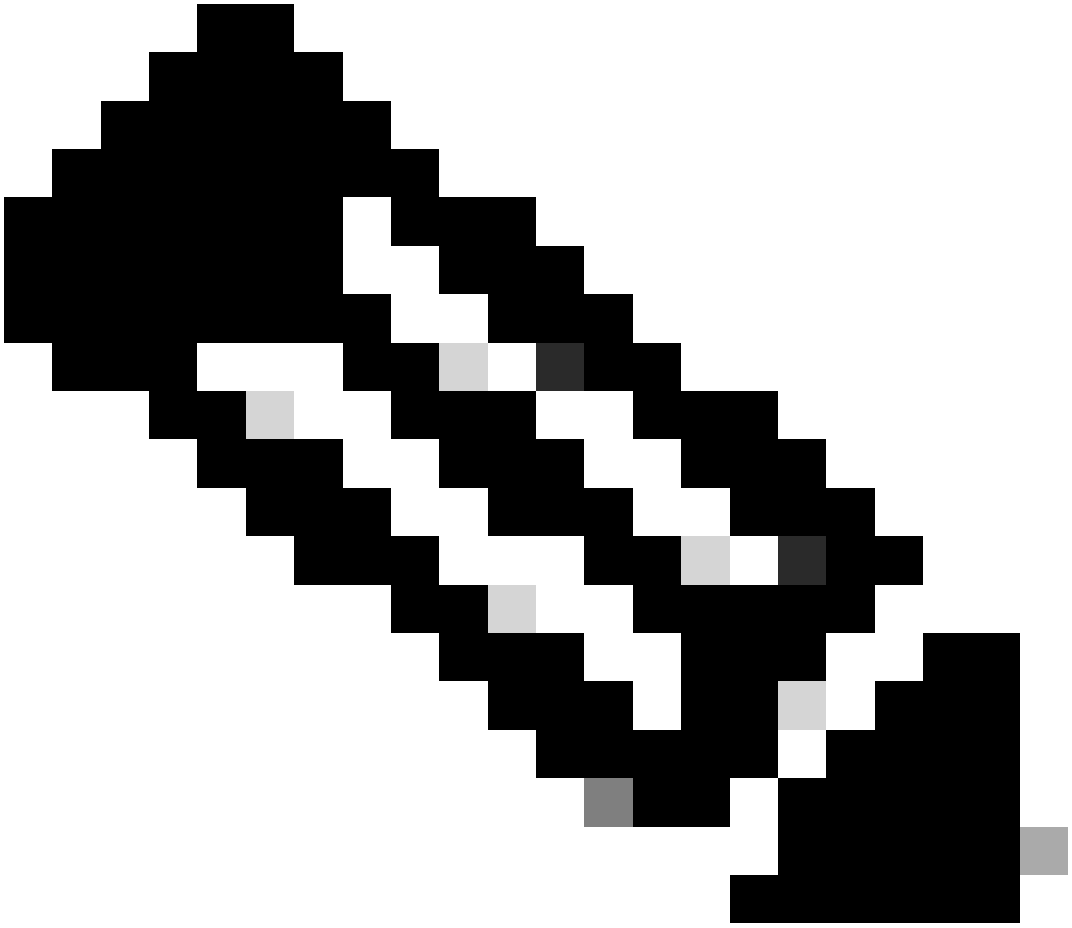
Introduzca la información necesaria para el certificado de FTD e importe un archivo PKCS12 desde el equipo local.

- Nombre: ftdvpn-cert
- Tipo de inscripción: archivo PKCS12

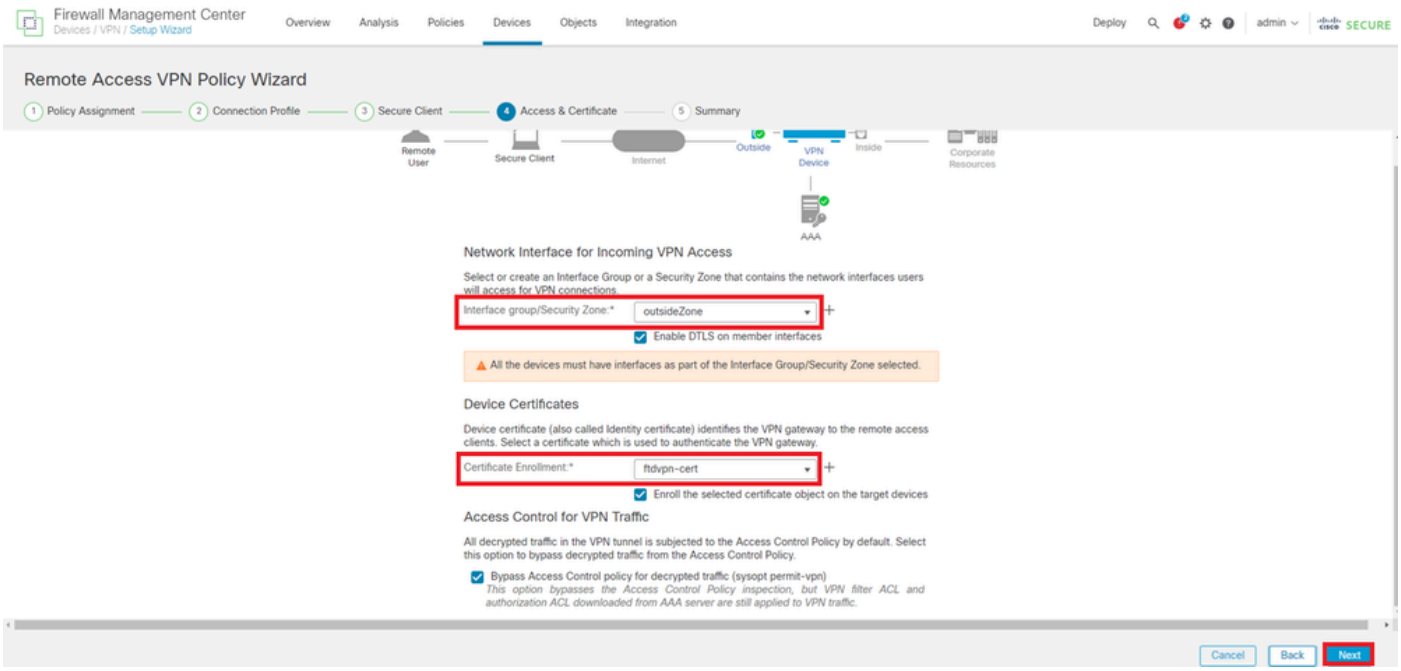


Agregar certificado FTD

Confirme la información ingresada en el asistente Access & Certificate y haga clic en el botón Next.



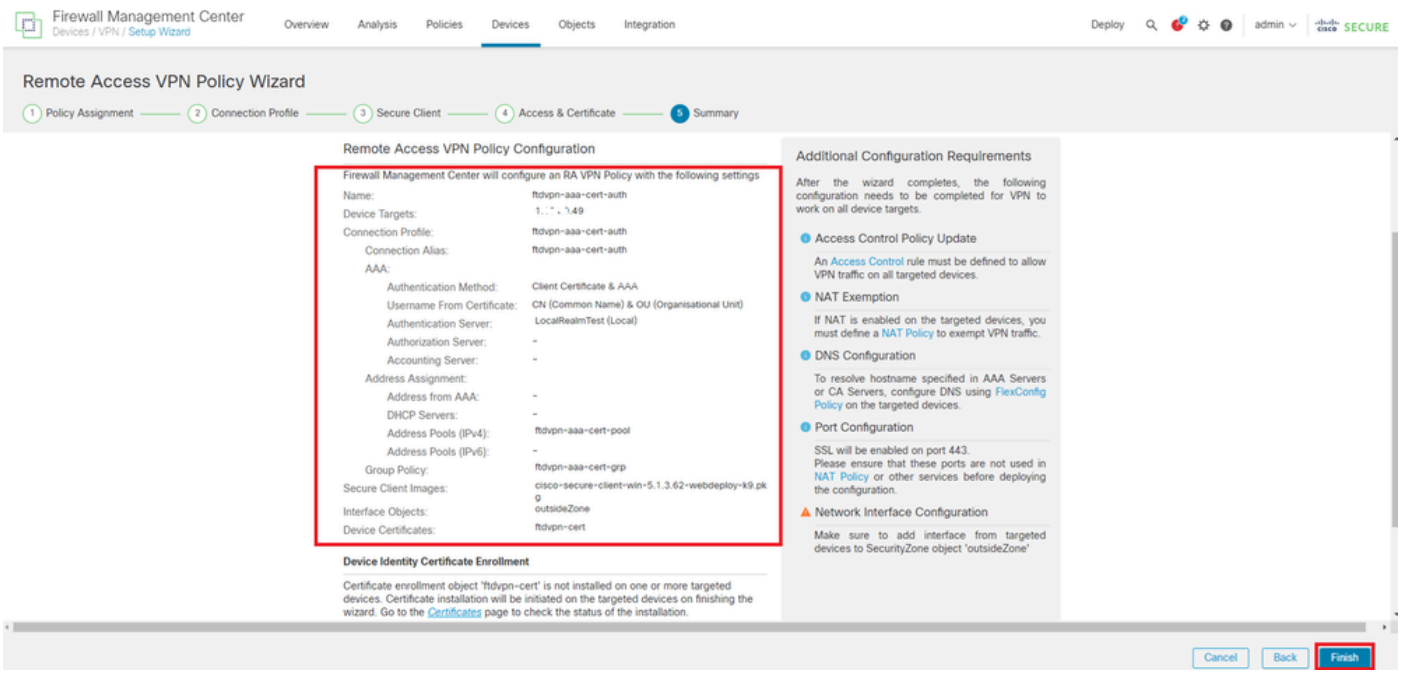
Nota: habilite la política de omisión del control de acceso para el tráfico descifrado (sysopt permit-vpn), de modo que el tráfico VPN descifrado no esté sujeto a la inspección de la política de control de acceso.



Confirmar configuración en Acceso y certificado

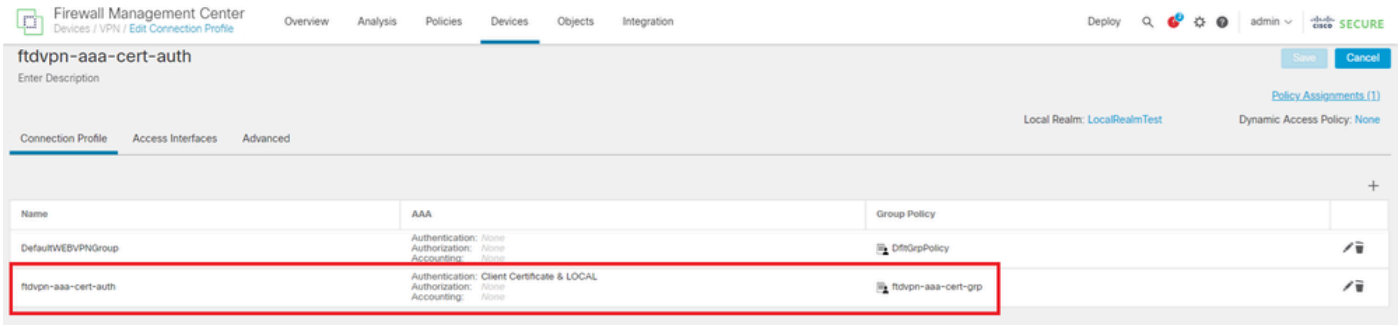
Paso 9. Confirmar resumen para perfil de conexión

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



Confirmar configuración para la conexión VPN

Confirme el resumen de la directiva VPN de acceso remoto e implemente la configuración en FTD.



Resumen de la directiva VPN de acceso remoto

Confirmar en CLI de FTD

Confirme la configuración de la conexión VPN en la CLI de FTD después de la implementación desde el FMC.

```
// Defines IP of interface
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 192.168.1.200 255.255.255.0
interface GigabitEthernet0/1
nameif inside
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 mask 255.255.255.0

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

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftdvpn-cert
keypair ftdvpn-cert
crl configure

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

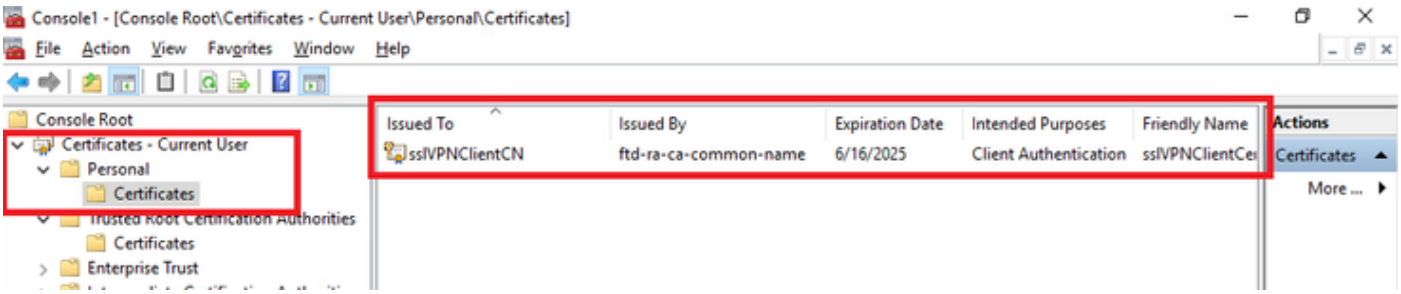
```
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Bypass Access Control policy for decrypted traffic
// This setting is displayed in the 'show run all' command output
sysopt connection permit-vpn

// Configures the group-policy to allow SSL connections
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-grp attributes
banner none
wins-server none
dns-server none
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-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools none
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
anyconnect ssl keepalive 20
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable

// 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

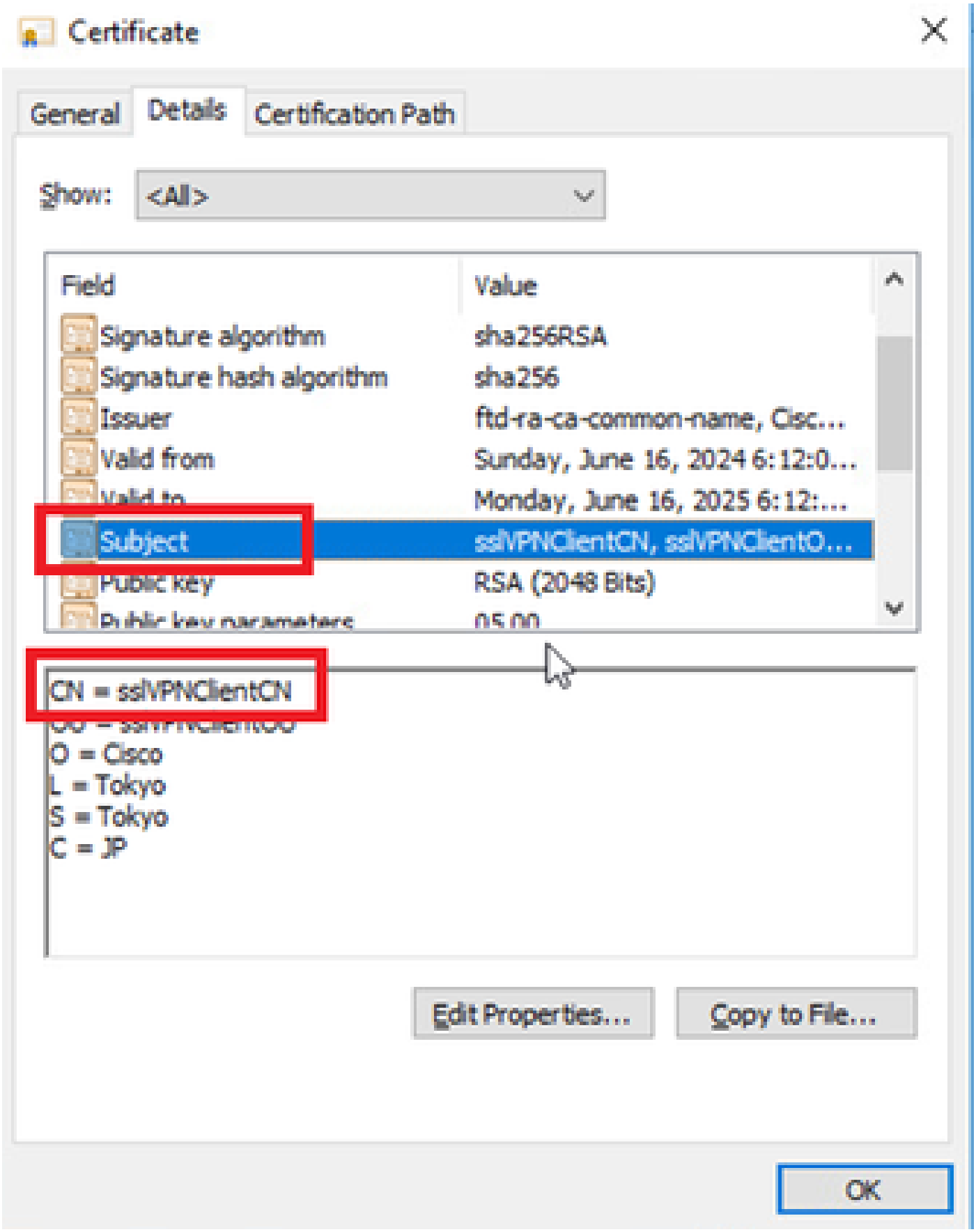
Vaya a Certificates - Current User > Personal > Certificates, verifique el certificado de cliente utilizado para la autenticación.



Confirmar certificado de cliente

Haga doble clic en el certificado de cliente, navegue hasta Detalles, verifique los detalles de Asunto.

- Asunto: CN = sslVPNClientCN



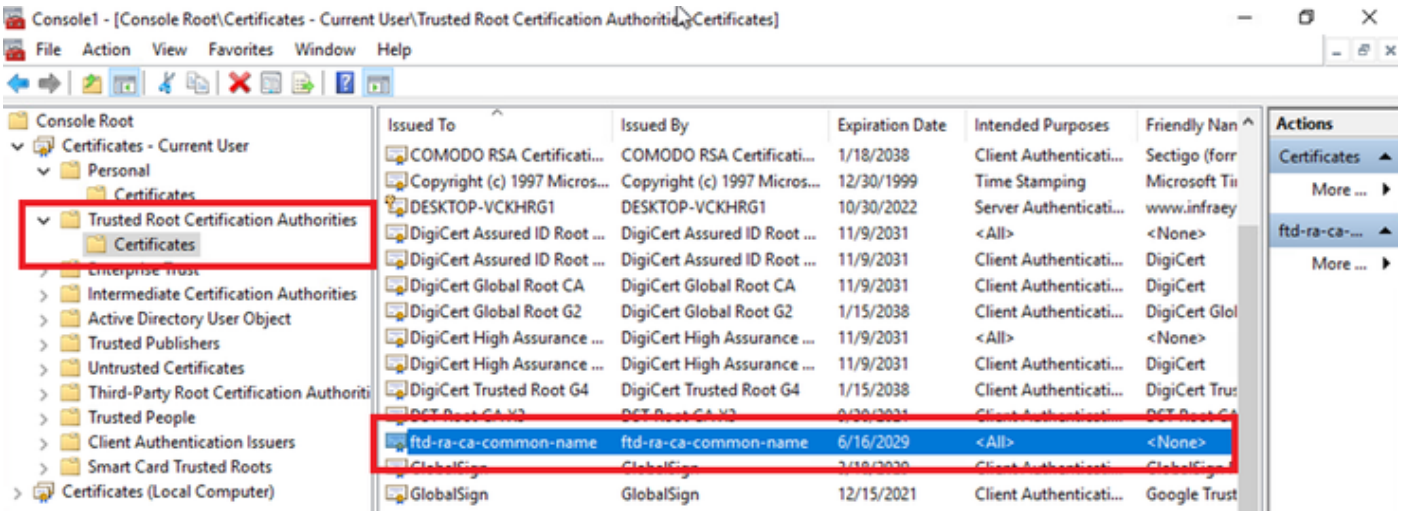
Detalles del certificado de cliente

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



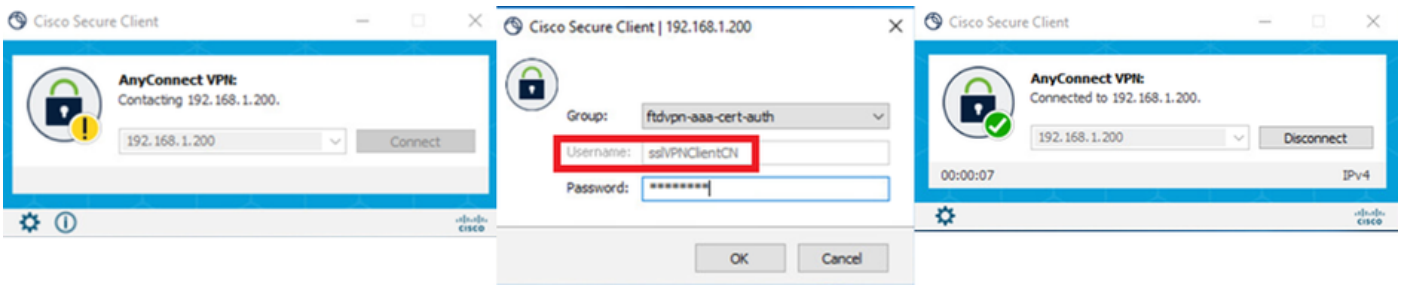
Confirmar CA

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.

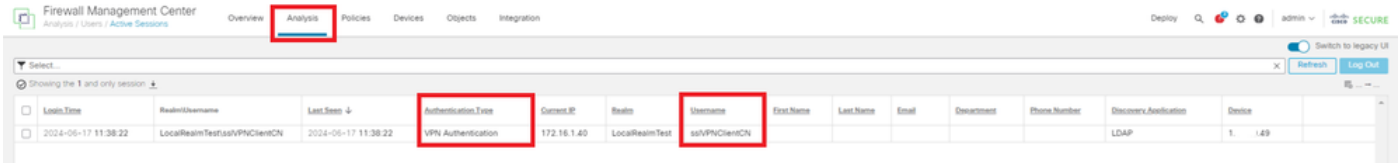
Nota: El nombre de usuario se extrae del campo CN (Common Name) del certificado de cliente en este documento.



Iniciar conexión VPN

Paso 2. Confirmar sesiones activas en FMC

Navegue hasta Análisis > Usuarios > Sesiones activas, verifique la sesión activa para la autenticación VPN.



Confirmar sesión activa

Paso 3. 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.

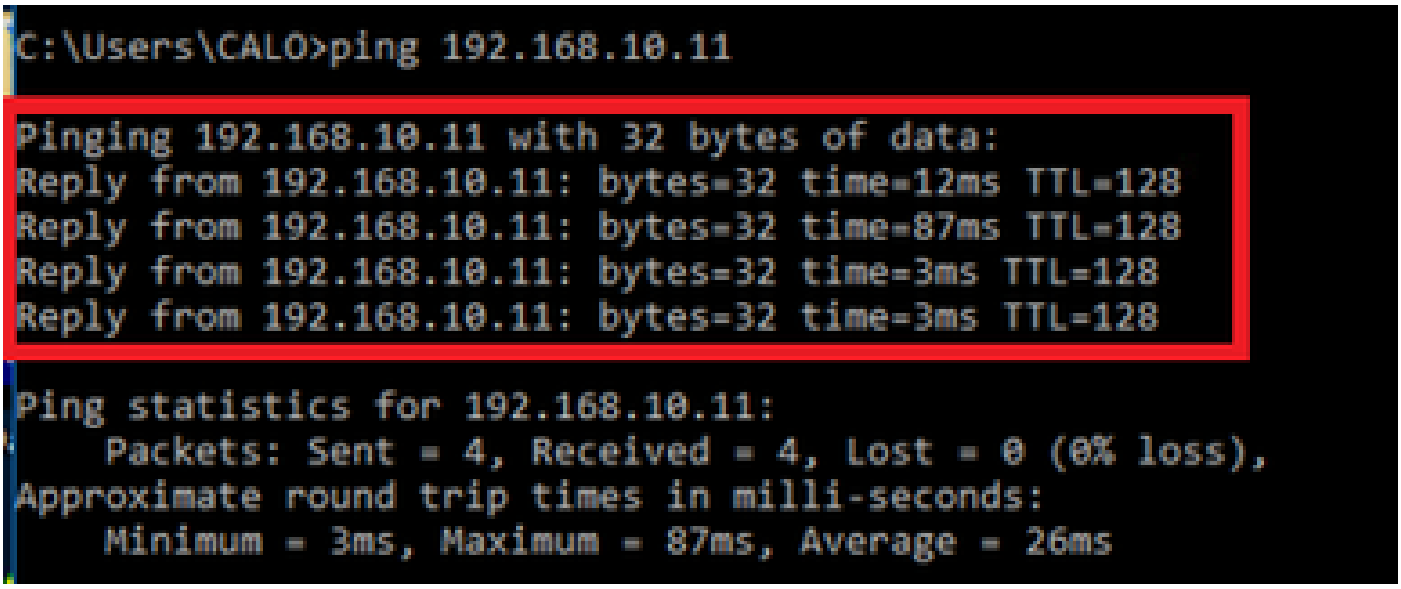
```
ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 7
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
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 : 14780 Bytes Rx : 15386
Pkts Tx : 2 Pkts Rx : 37
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth
Login Time : 02:38:22 UTC Mon Jun 17 2024
Duration : 0h:01m:22s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb00718200007000666fa19e
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 7.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50035 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7390 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 7.2
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-128 Hashing : SHA256
```

Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 50042
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7390 Bytes Rx : 2292
Pkts Tx : 1 Pkts Rx : 3
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 7.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 56382
UDP Dst Port : 443 Auth Mode : Certificate and 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 5.1.3.62
Bytes Tx : 0 Bytes Rx : 13094
Pkts Tx : 0 Pkts Rx : 34
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Paso 4. 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.



Ping correcto

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

ftd702#

```
capture in interface inside real-time


Use ctrl-c to terminate real-time capture

1: 03:39:25.729881 172.16.1.40 > 192.168.10.11 icmp: echo request
2: 03:39:25.730766 192.168.10.11 > 172.16.1.40 icmp: echo reply
3: 03:39:26.816211 172.16.1.40 > 192.168.10.11 icmp: echo request
4: 03:39:26.818683 192.168.10.11 > 172.16.1.40 icmp: echo reply
5: 03:39:27.791676 172.16.1.40 > 192.168.10.11 icmp: echo request
6: 03:39:27.792195 192.168.10.11 > 172.16.1.40 icmp: echo reply
7: 03:39:28.807789 172.16.1.40 > 192.168.10.11 icmp: echo request
8: 03:39:28.808399 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 la PC con Windows.

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

```
// Certificate Authentication
Jun 17 2024 02:38:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=sslV
Jun 17 2024 02:38:03: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked.
Jun 17 2024 02:38:03: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name:  CN=sslVPNClientCl

// Extract username from the CN (Common Name) field
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has been requested.  [Request 5]
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has completed.  [Request 5]

// AAA Authentication
Jun 17 2024 02:38:22: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN
Jun 17 2024 02:38:22: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN
Jun 17 2024 02:38:22: %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

Referencia

Configuración de VPN de acceso remoto AnyConnect en FTD

Configuración de la Autenticación Basada en Certificados de Anyconnect para el Acceso Móvil

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).