# Configurar o mapeamento de certificados para autenticação de cliente seguro no FTD via FMC

## Contents

## Introdução

Este documento descreve como configurar o Cisco Secure Client com SSL no FTD via FMC usando o mapeamento de certificado para autenticação.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Firepower Management Center (FMC)
- Firewall Threat Defense (FTD) Virtual
- Fluxo de autenticação de VPN

### Componentes Utilizados

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

- Cisco Secure Client 5.1.3.62

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

O mapeamento de certificado é um método usado em conexões VPN em que um certificado de cliente é mapeado para uma conta de usuário local, ou os atributos dentro do certificado são usados para fins de autorização. Esse é um processo em que um certificado digital é usado como meio de identificar um usuário ou dispositivo. Ao usar o mapeamento de certificado, ele aproveita o protocolo SSL para autenticar usuários sem a necessidade de inserir credenciais.

Este documento descreve como autenticar o Cisco Secure Client usando o nome comum de um certificado SSL.

Estes certificados contêm um nome comum, que é utilizado para efeitos de autorização.

- CA: ftd-ra-ca-common-name
- Certificado de cliente VPN do engenheiro: vpnEngineerClientCN
- Certificado de cliente VPN do gerenciador: vpnManagerClientCN
- Certificado do servidor: 192.168.1.200

## Diagrama de Rede

Esta imagem mostra a topologia usada para o exemplo deste documento.

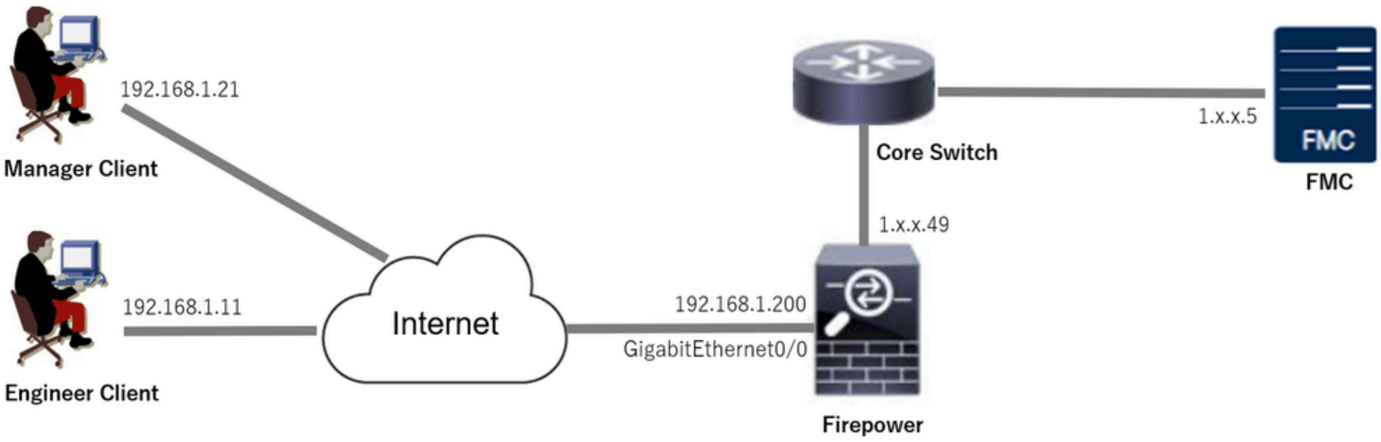


Diagrama de Rede

# Configurações

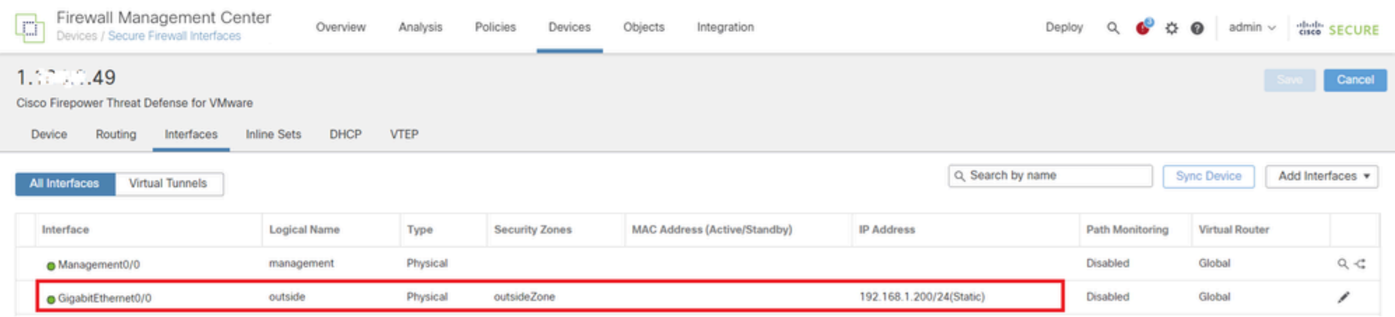
## Configuração no FMC

### Etapa 1. Configurar a interface FTD

Navegue até Dispositivos > Gerenciamento de dispositivos, edite o dispositivo FTD de destino, configure a interface externa para FTD na guia Interfaces.

Para GigabitEthernet0/0,

- Nome: externo
- Zona de segurança: outsideZone
- Endereço IP: 192.168.1.200/24



1.[redacted].49

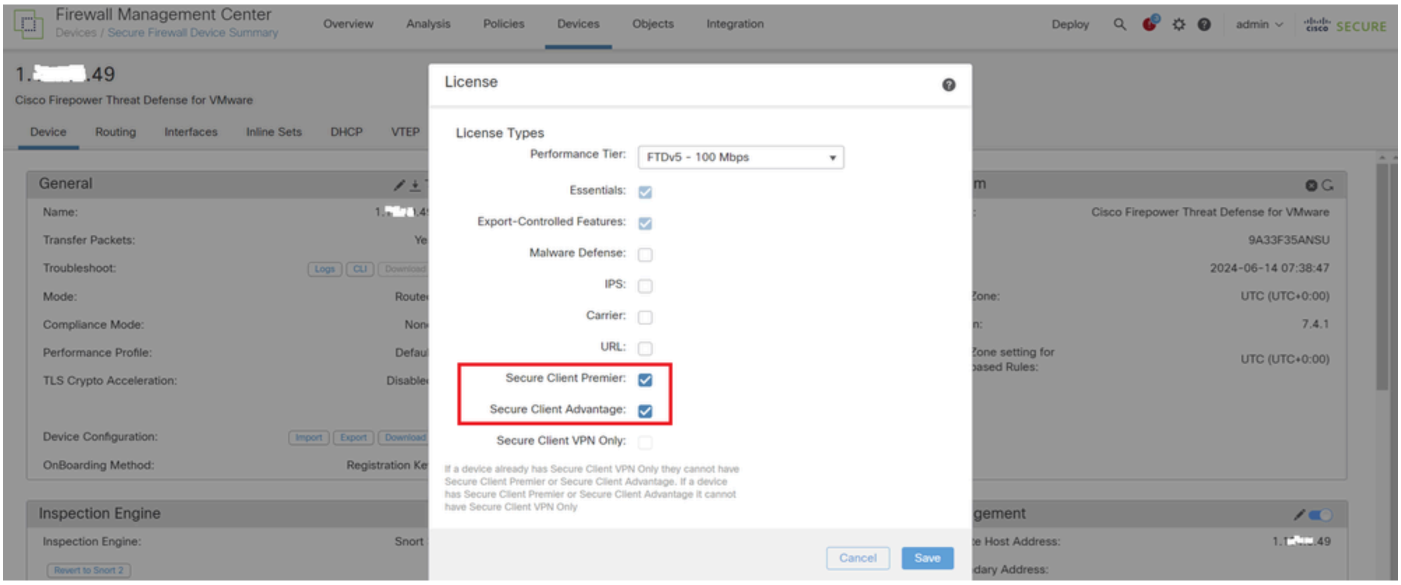
Cisco Firepower Threat Defense for VMware

| Interface | Logical Name | Type | Security Zones | MAC Address (Active/Standby) | IP Address | Path Monitoring | Virtual Router |
|---|---|---|---|---|---|---|---|
| Management0/0 | management | Physical | | | | Disabled | Global |
| GigabitEthernet0/0 | outside | Physical | outsideZone | | 192.168.1.200/24(Static) | Disabled | Global |

Interface FTD

### Etapa 2. Confirmar licença do Cisco Secure Client

Navegue até Dispositivos > Gerenciamento de dispositivos, edite o dispositivo FTD de destino, confirme a licença do Cisco Secure Client na guia Dispositivo.



License

License Types

Performance Tier: FTDv5 - 100 Mbps

Essentials: ☑

Export-Controlled Features: ☑

Malware Defense: □

IPS: □

Carrier: □

URL: □

Secure Client Premier: ☑

Secure Client Advantage: ☑

Secure Client VPN Only: □

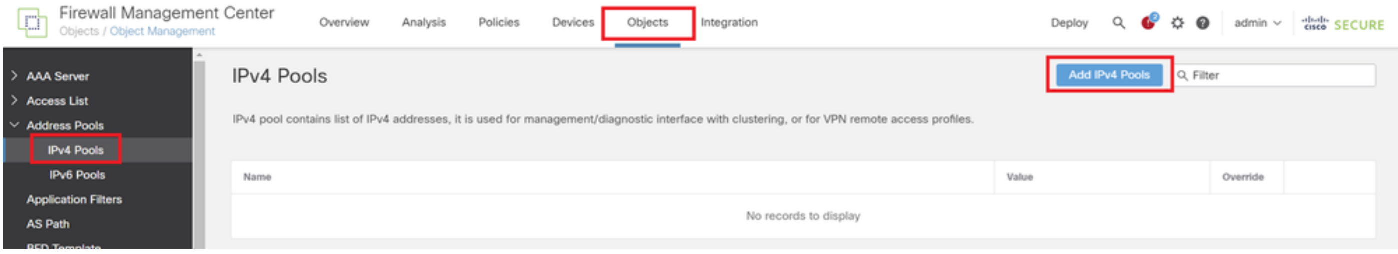
If a device already has Secure Client VPN Only they cannot have Secure Client Premier or Secure Client Advantage. If a device has Secure Client Premier or Secure Client Advantage it cannot have Secure Client VPN Only

Cancel | Save

Licença de cliente seguro

## Etapa 3. Adicionar Pool de Endereços IPv4

Navegue atéObject > Object Management > Address Pools > IPv4 Pools, clique no botão Add IPv4 Pools.



IPv4 Pools

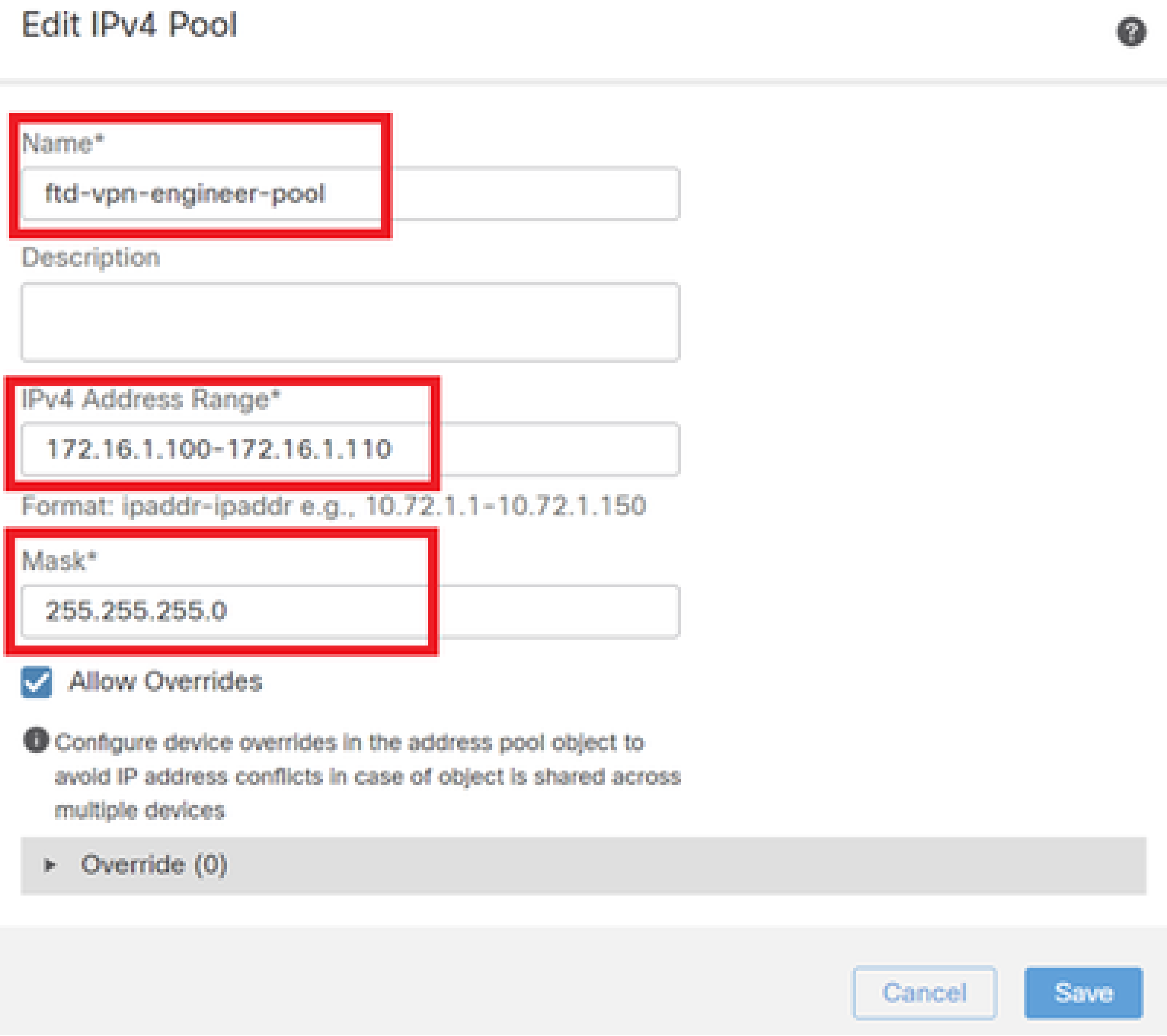
IPv4 pool contains list of IPv4 addresses, it is used for management/diagnostic interface with clustering, or for VPN remote access profiles.

| Name | Value | Override |
|---|---|---|
| No records to display | | |

Adicionar Pool de Endereços IPv4

Insira as informações necessárias para criar um pool de endereços IPv4 para o cliente VPN do engenheiro.

- Nome: ftd-vpn-engineering-pool
- Intervalo de endereços IPv4: 172.16.1.100-172.16.1.110
- Máscara: 255.255.255.0



Edit IPv4 Pool

Name*

ftd-vpn-engineer-pool

Description

IPv4 Address Range*

172.16.1.100-172.16.1.110

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*

255.255.255.0

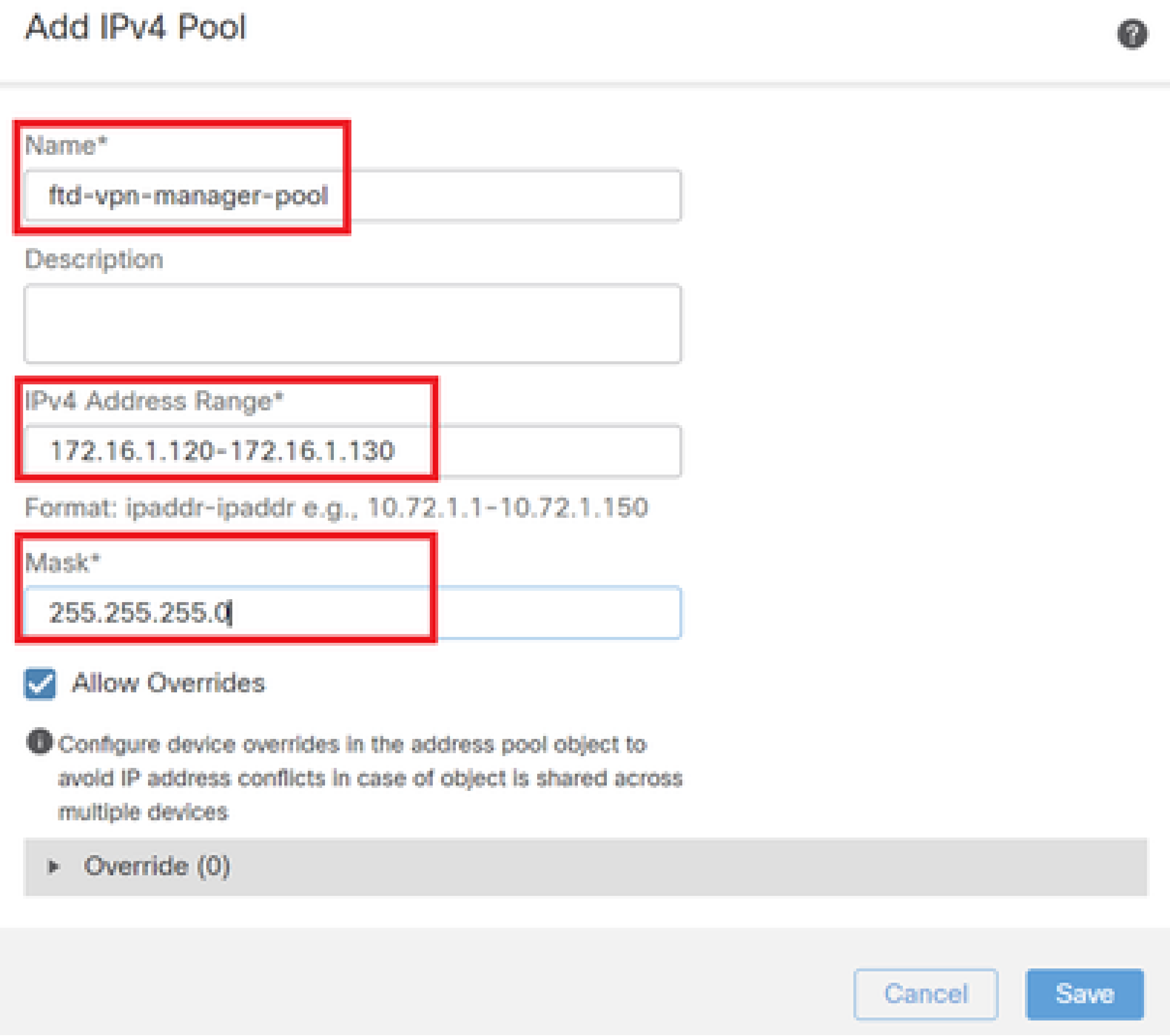
☑ Allow Overrides

Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

Pool de Endereços IPv4 para o VPN Client do Engenheiro

Insira as informações necessárias para criar um pool de endereços IPv4 para o cliente VPN do gerenciador.

- Nome: ftd-vpn-manager-pool
- Intervalo de endereços IPv4: 172.16.1.120-172.16.1.130
- Máscara: 255.255.255.0



Add IPv4 Pool

Name*

ftd-vpn-manager-pool

Description

IPv4 Address Range*

172.16.1.120-172.16.1.130

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*

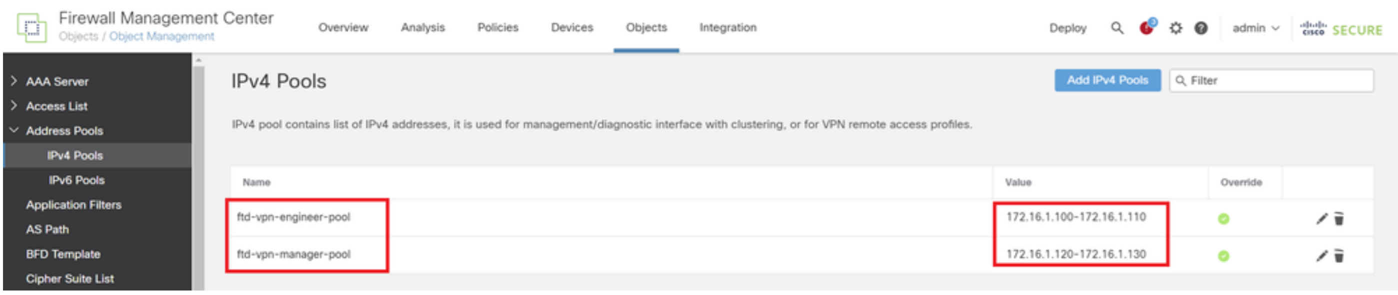
255.255.255.0

☑ Allow Overrides

Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

Pool de Endereços IPv4 para o Cliente VPN do Gerenciador

Confirme os novos pools de endereços IPv4.



IPv4 Pools

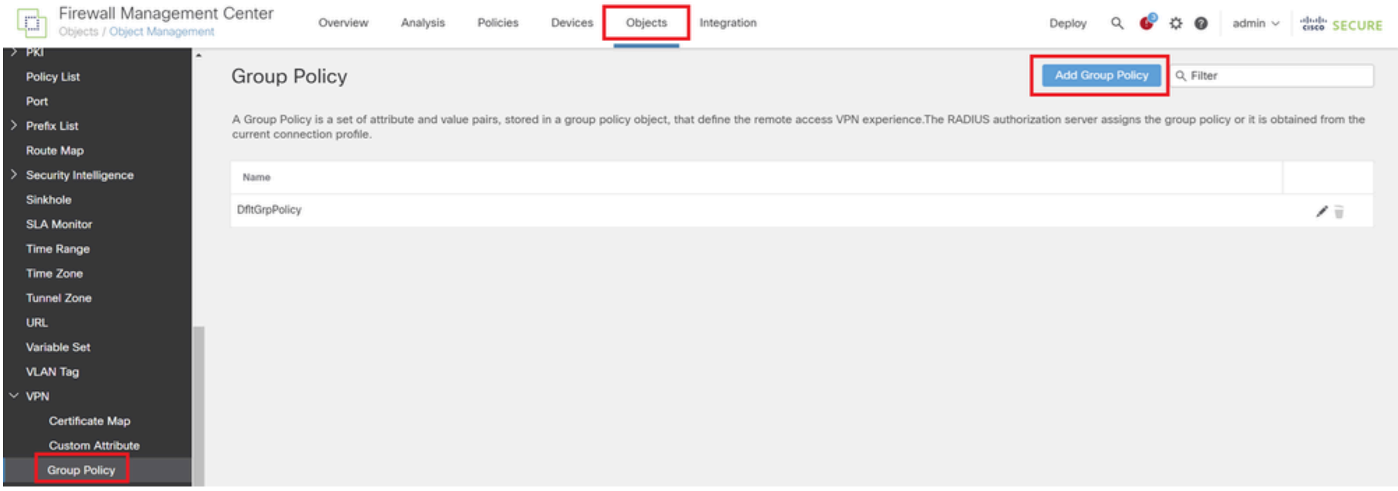
IPv4 pool contains list of IPv4 addresses, it is used for management/diagnostic interface with clustering, or for VPN remote access profiles.

| Name | Value | Override |
|---|---|---|
| ftd-vpn-engineer-pool | 172.16.1.100-172.16.1.110 | ● |
| ftd-vpn-manager-pool | 172.16.1.120-172.16.1.130 | ● |

Novos pools de endereços IPv4

Etapa 4. Adicionar Política de Grupo

Navegue atéObject > Object Management > VPN > Group Policy, clique em Add Group Policy.



Group Policy

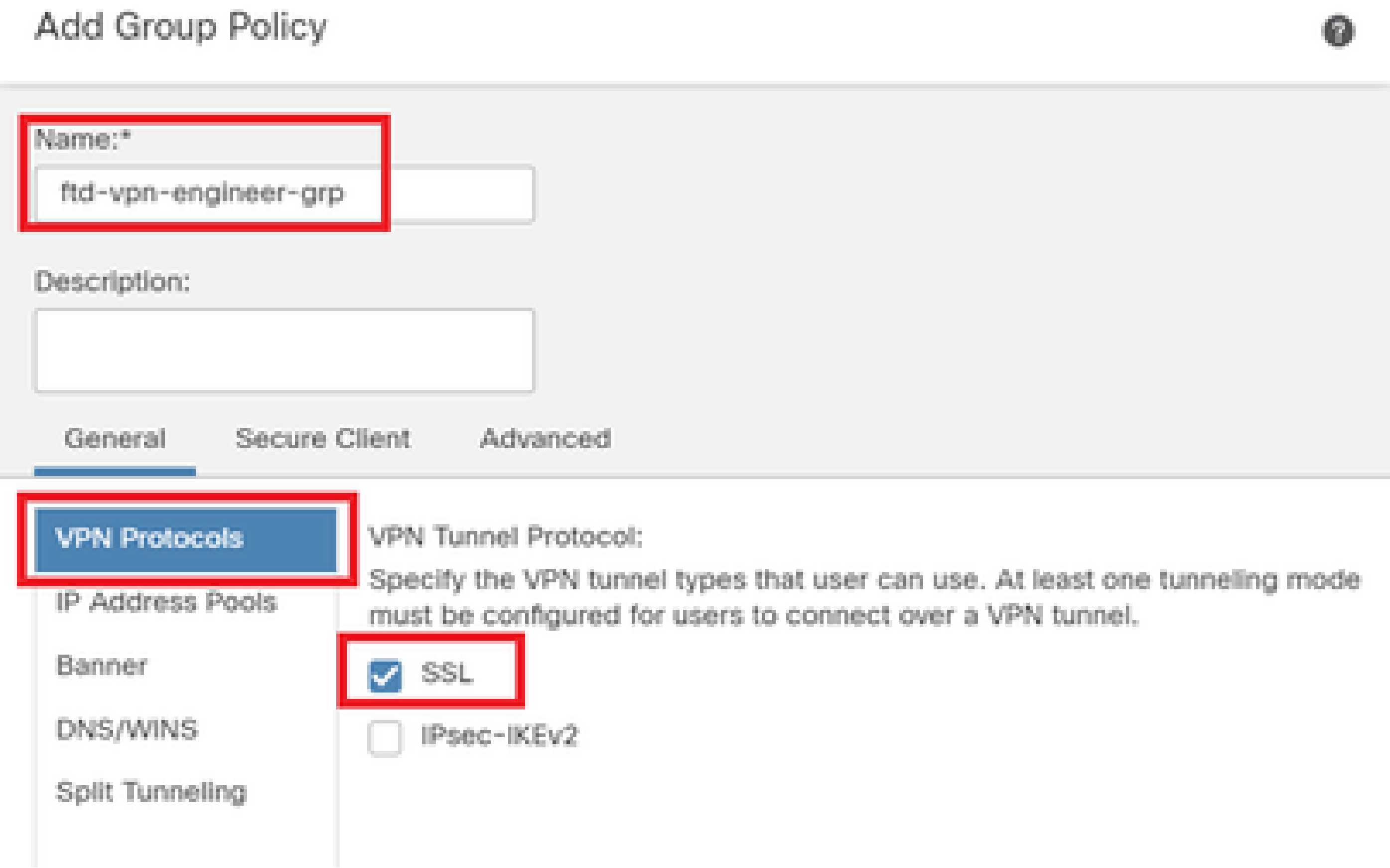
A Group Policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience.The RADIUS authorization server assigns the group policy or it is obtained from the current connection profile.

| Name |
|---|
| DfltGrpPolicy |

Adicionar Política de Grupo

Insira as informações necessárias para criar uma política de grupo para o cliente VPN do engenheiro.

- Nome: ftd-vpn-engineering-grp
- Protocolos VPN: SSL



Name:* ftd-vpn-engineer-grp

Description:

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

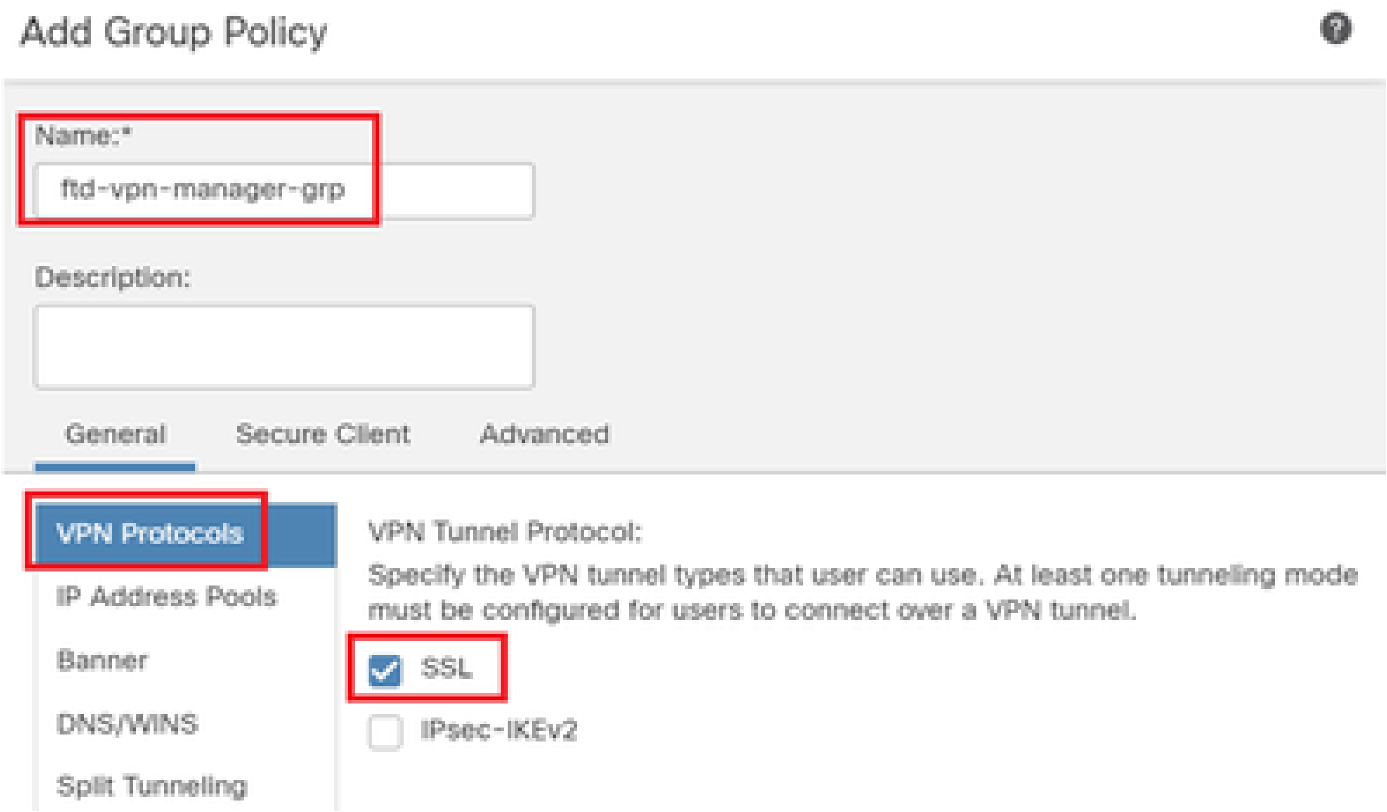
☑ SSL

□ IPsec-IKEv2

Política de Grupo para o VPN Client do Engenheiro

Insira as informações necessárias para criar uma política de grupo para o cliente VPN do gerenciador.

- Nome: ftd-vpn-manager-grp
- Protocolos VPN: SSL



Add Group Policy

Name:*

ftd-vpn-manager-grp

Description:

VPN Tunnel Protocol:

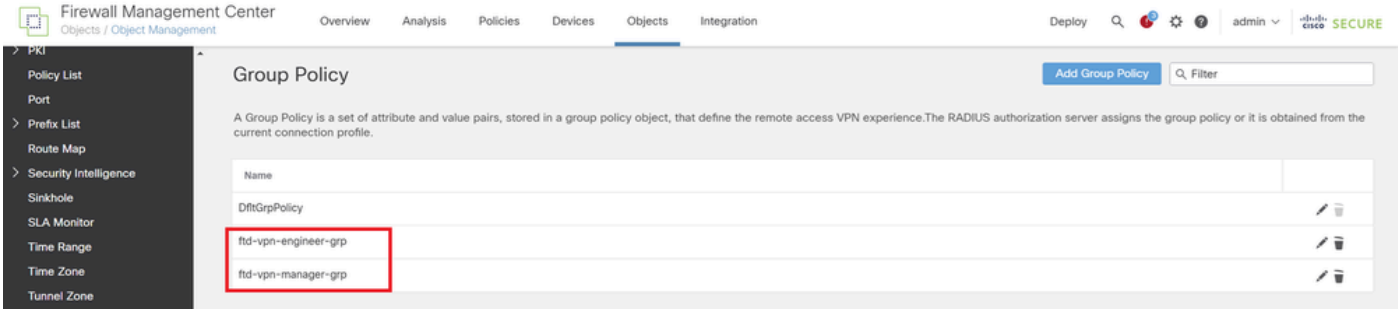
Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

☑ SSL

□ IPsec-IKEv2

Política de Grupo para o Cliente VPN do Gerente

Confirme as novas diretivas de grupo.



Group Policy

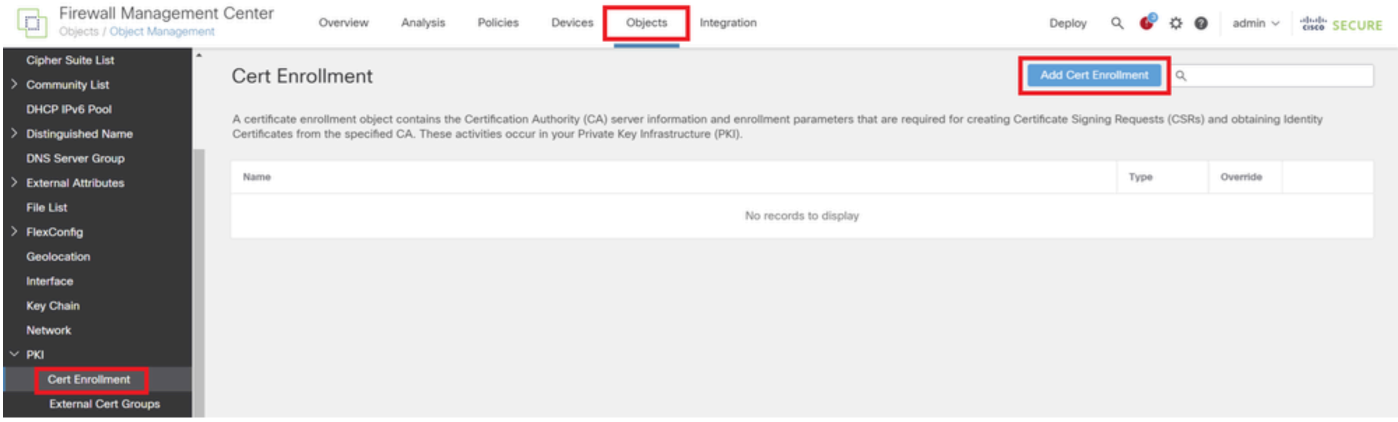
A Group Policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience.The RADIUS authorization server assigns the group policy or it is obtained from the current connection profile.

| Name |
|---|
| DfltGrpPolicy |
| ftd-vpn-engineer-grp |
| ftd-vpn-manager-grp |

Novas políticas de grupo

Etapa 5. Adicionar Certificado FTD

Navegue atéObject > Object Management > PKI > Cert Enrollment, clique no botão Add Cert Enrollment.



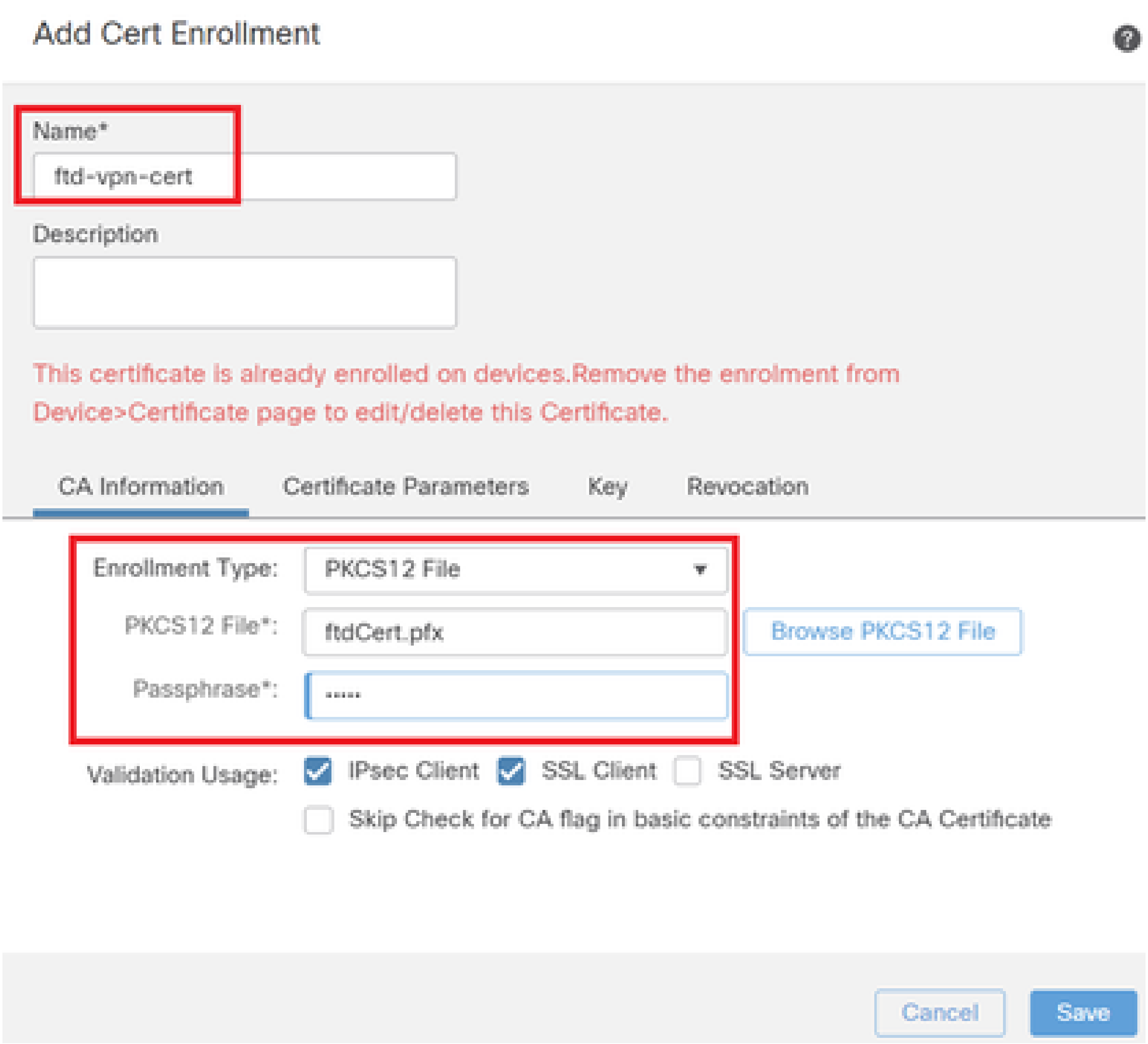
A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).

| Name | Type | Override |
|---|---|---|
| No records to display | | |

Adicionar Registro de Certificado

Insira as informações necessárias para o certificado FTD e importe um arquivo PKCS12 do computador local.

- Nome: ftd-vpn-cert
- Tipo de inscrição: PKCS12 File



Name*: ftd-vpn-cert

Description:

This certificate is already enrolled on devices.Remove the enrolment from Device>Certificate page to edit/delete this Certificate.

Enrollment Type: PKCS12 File

PKCS12 File*: ftdCert.pfx

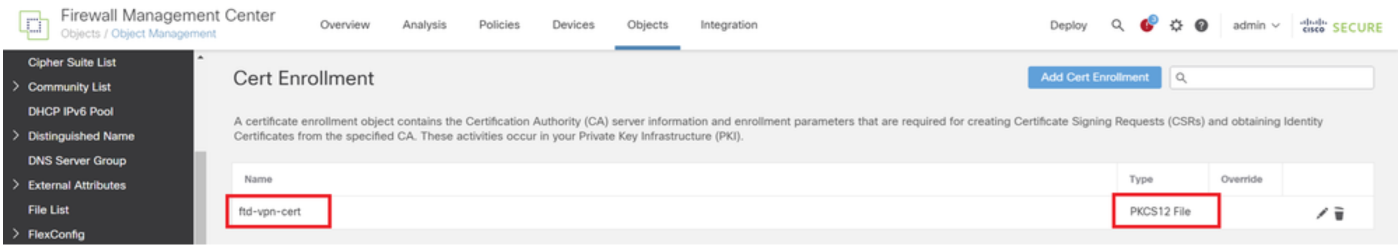
Passphrase*: •••••

Validation Usage: ☑ IPsec Client ☑ SSL Client □ SSL Server

□ Skip Check for CA flag in basic constraints of the CA Certificate

Detalhes da Inscrição de Certificado

Confirme a inscrição do novo certificado.



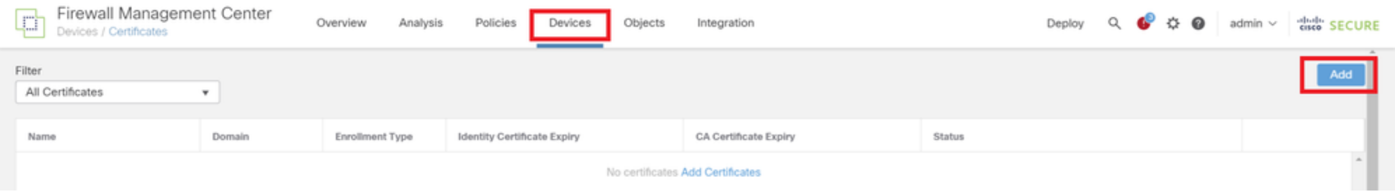
Cert Enrollment

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).

| Name | Type | Override |
|---|---|---|
| ftd-vpn-cert | PKCS12 File | |

Nova inscrição de certificado

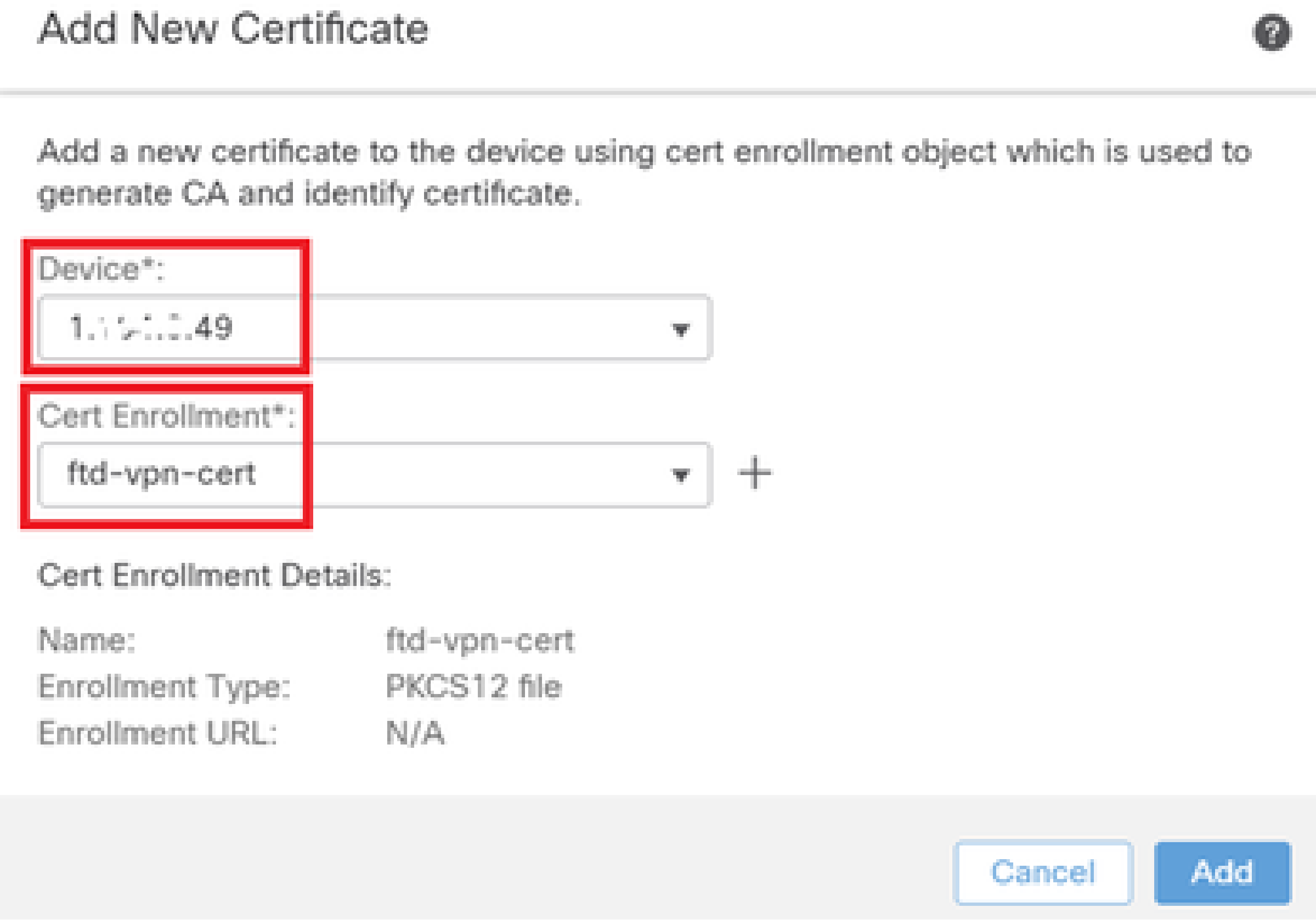
Navegue até Dispositivos > Certificados, clique no botão Adicionar.



Adicionar Certificado FTD

Insira as informações necessárias para associar o novo registro de certificado ao FTD.

- Dispositivo: 1.x.x.49
- Registro de certificado: ftd-vpn-cert



## Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: 1.[redacted].49

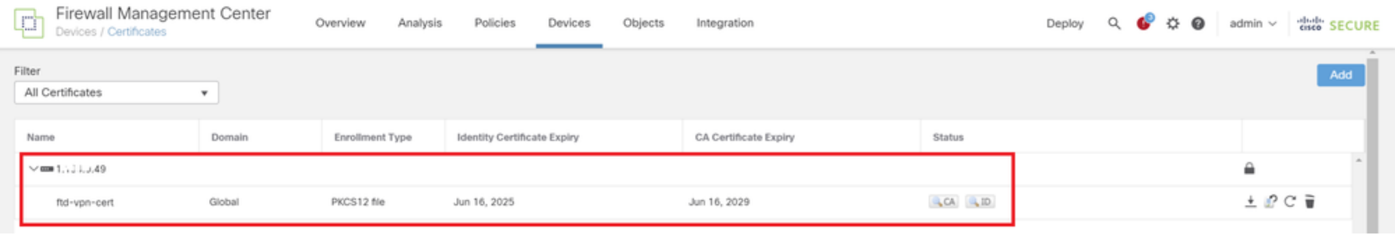
Cert Enrollment*: ftd-vpn-cert

Cert Enrollment Details:

| | |
|---|---|
| Name: | ftd-vpn-cert |
| Enrollment Type: | PKCS12 file |
| Enrollment URL: | N/A |

Vincular certificado ao FTD

Confirme o status da associação de certificado.

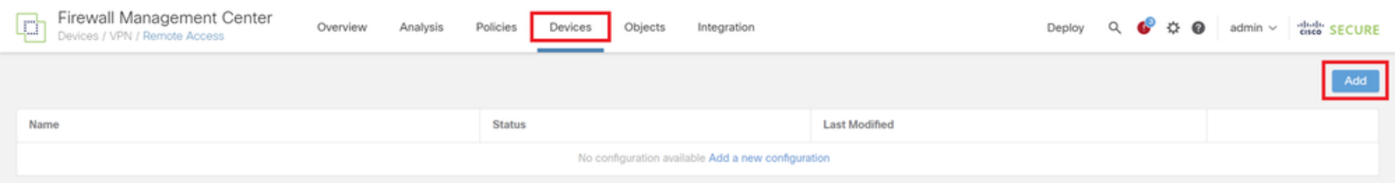


| Name | Domain | Enrollment Type | Identity Certificate Expiry | CA Certificate Expiry | Status |
|---|---|---|---|---|---|
| 1.[redacted].49 | | | | | |
| ftd-vpn-cert | Global | PKCS12 file | Jun 16, 2025 | Jun 16, 2029 | CA ID |

Status da Associação de Certificado

Etapa 6. Adicionar Atribuição de Política para Perfil de Conexão do Engenheiro

Navegue até Dispositivos > VPN > Acesso remoto e clique no botão Adicionar.

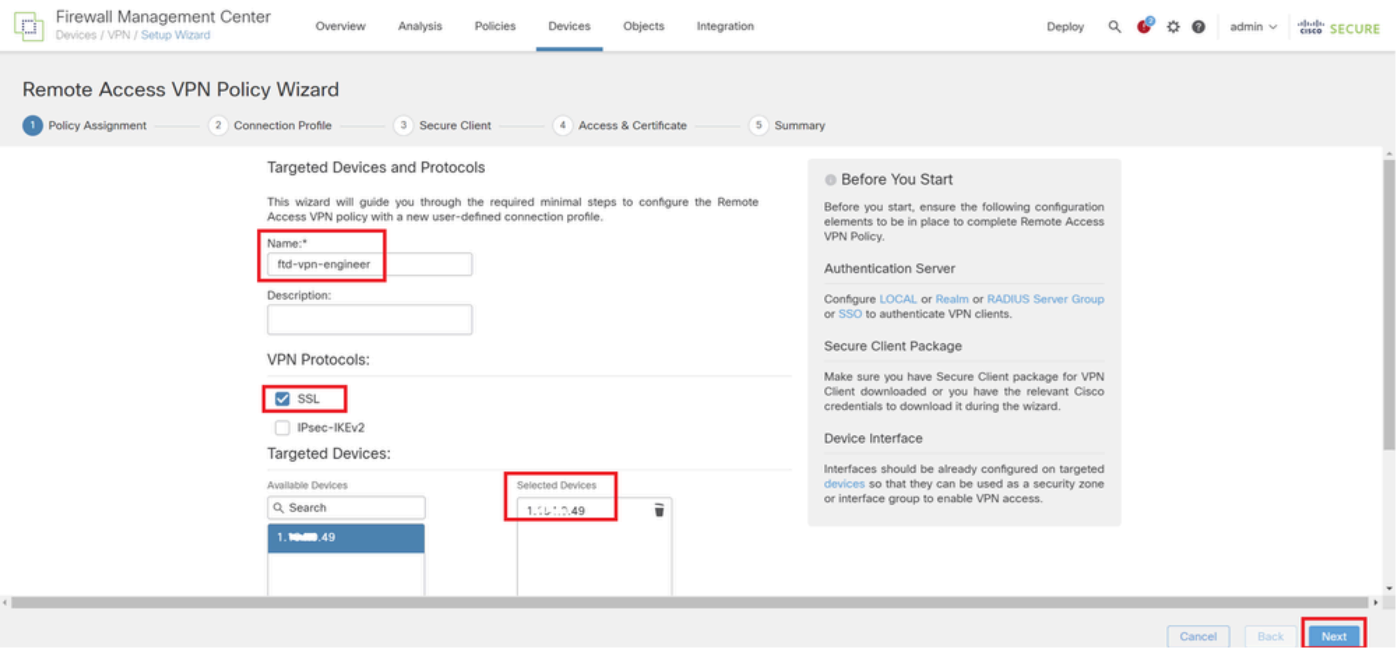


| Name | Status | Last Modified |
|---|---|---|
| No configuration available Add a new configuration | | |

Adicionar VPN de acesso remoto

Insira as informações necessárias e clique no botão Avançar.

- Nome: ftd-vpn-engineering
- Protocolos VPN: SSL
- Dispositivos de destino: 1.x.x.49



Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:* ftd-vpn-engineer

Description:

VPN Protocols:

☑ SSL

□ IPsec-IKEv2

Targeted Devices:

Available Devices: Search; 1.[redacted].49

Selected Devices: 1.[redacted].49

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure LOCAL or Realm or RADIUS Server Group or SSO to authenticate VPN clients.

Secure Client Package

Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

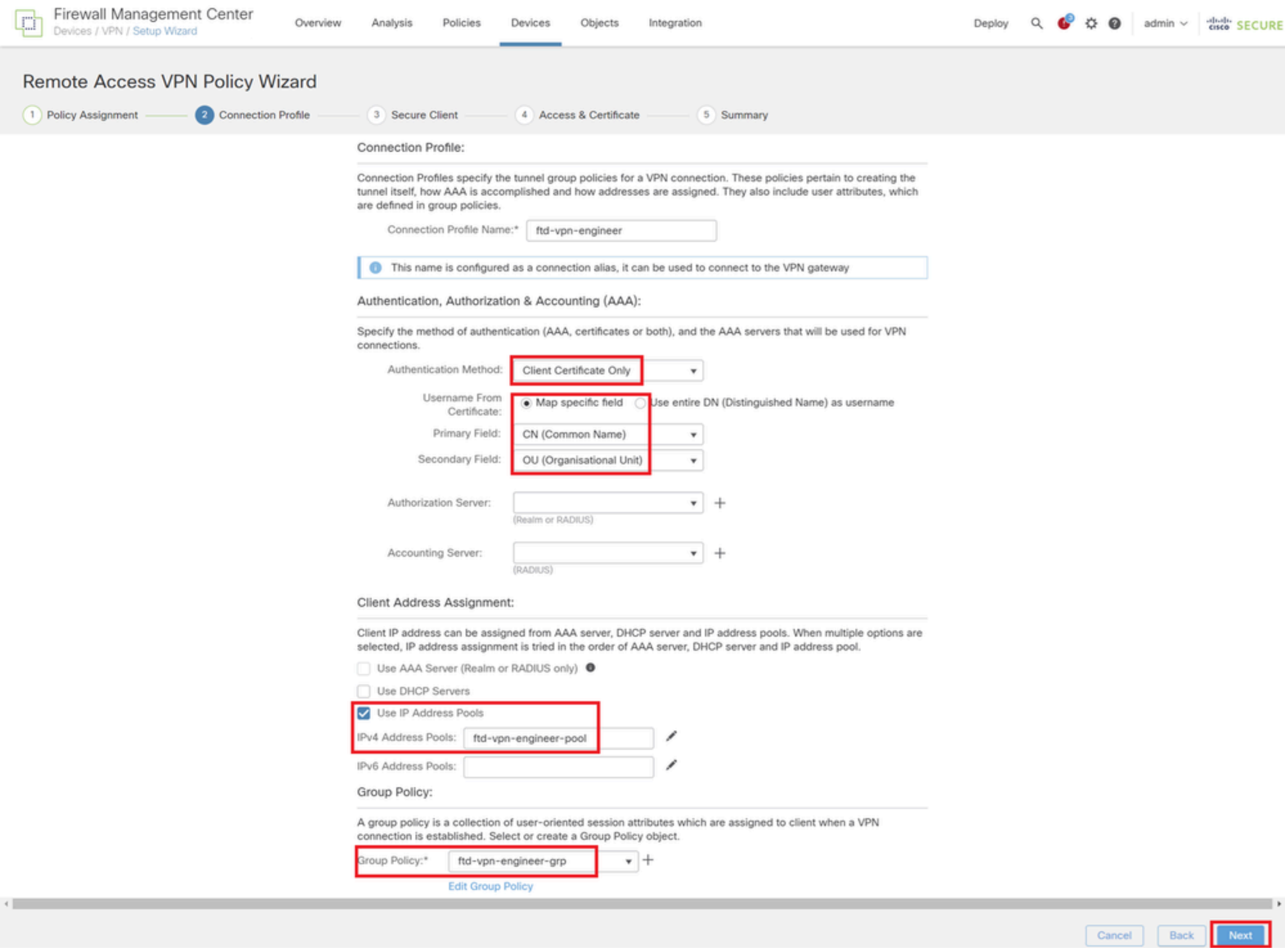
Atribuição de política

Passo 7. Configurar Detalhes do Perfil de Conexão do Engenheiro

Insira as informações necessárias e clique no botão Avançar.

- Método de Autenticação: Somente Certificado do Cliente
- Nome de usuário do certificado: Mapear campo específico
- Campo Primário: CN (Nome Comum)
- Campo Secundário: OU (Unidade Organizacional)

- Pools de Endereços IPv4: ftd-vpn-engineering-pool
- Política de Grupo: ftd-vpn-engineering-grp



Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:* ftd-vpn-engineer

This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: Client Certificate Only

Username From Certificate: ● Map specific field ○ Use entire DN (Distinguished Name) as username

Primary Field: CN (Common Name)

Secondary Field: OU (Organisational Unit)

Authorization Server: (Realm or RADIUS)

Accounting Server: (RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

□ Use AAA Server (Realm or RADIUS only)

□ Use DHCP Servers

☑ Use IP Address Pools

IPv4 Address Pools: ftd-vpn-engineer-pool

IPv6 Address Pools:

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

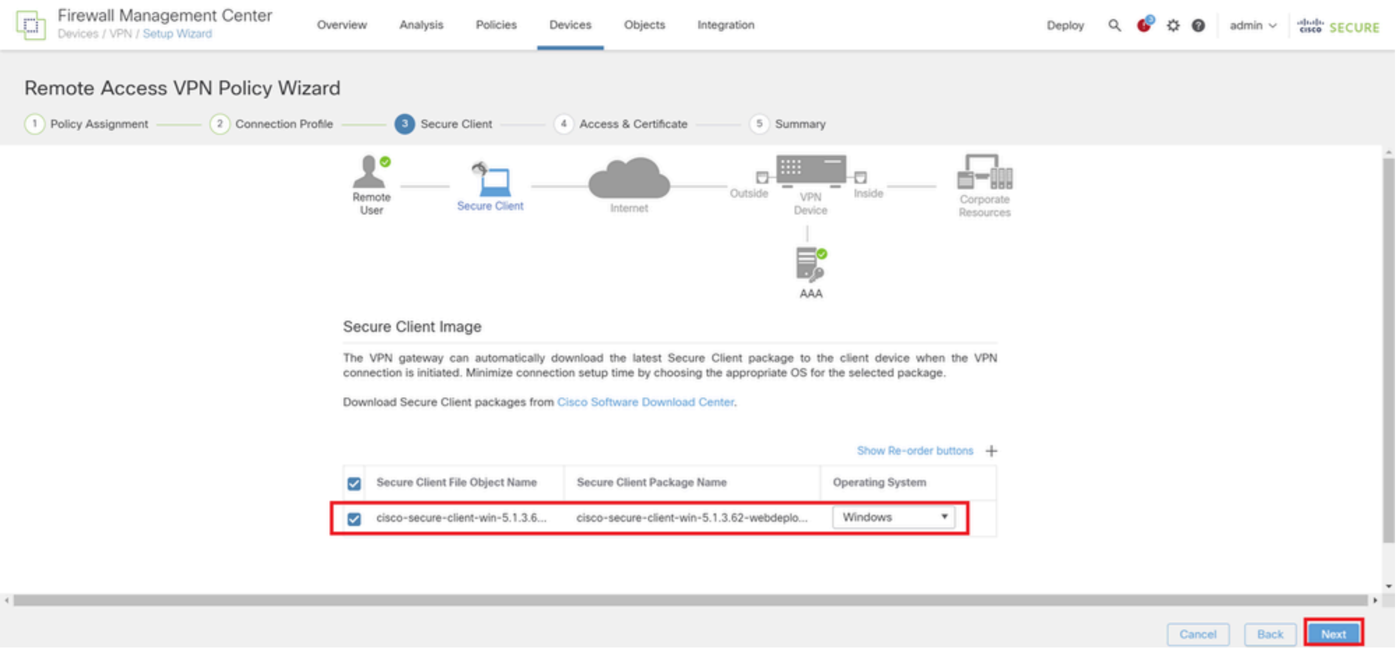
Group Policy:* ftd-vpn-engineer-grp

Edit Group Policy

Detalhes do Perfil de Conexão

## Etapa 8. Configurar Imagem de Cliente Segura para Perfil de Conexão do Engenheiro

Selecione secure client image file e clique no botão Next.



Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from Cisco Software Download Center.

Show Re-order buttons +

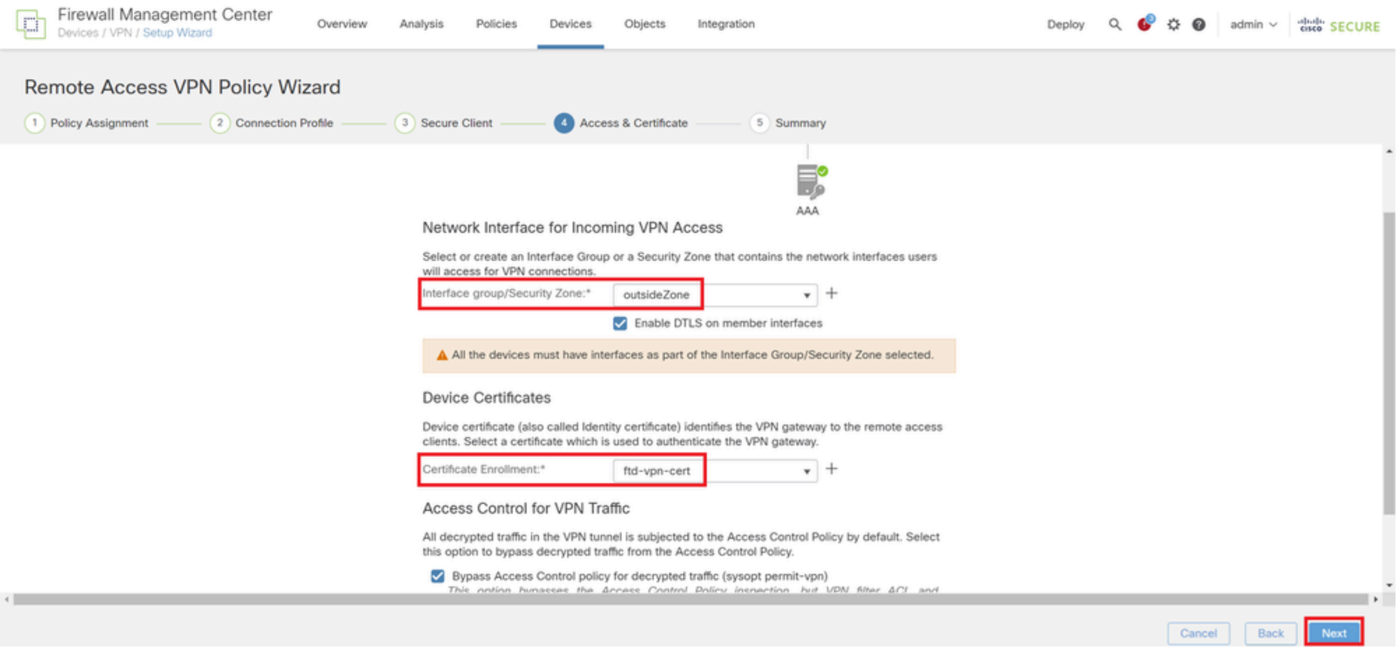
| ☑ | Secure Client File Object Name | Secure Client Package Name | Operating System |
|---|---|---|---|
| ☑ | cisco-secure-client-win-5.1.3.6... | cisco-secure-client-win-5.1.3.62-webdeplo... | Windows |

Selecionar cliente seguro

Etapa 9. Configurar acesso e certificado para o perfil de conexão do engenheiro

Selecione o valor para os itens Grupo de interface/Zona de segurança e Registro de certificado, clique no botão Avançar.

- Grupo de interface/Zona de segurança: outsideZone
- Inscrição de certificado: ftd-vpn-cert



Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* outsideZone

☑ Enable DTLS on member interfaces

⚠ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* ftd-vpn-cert

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

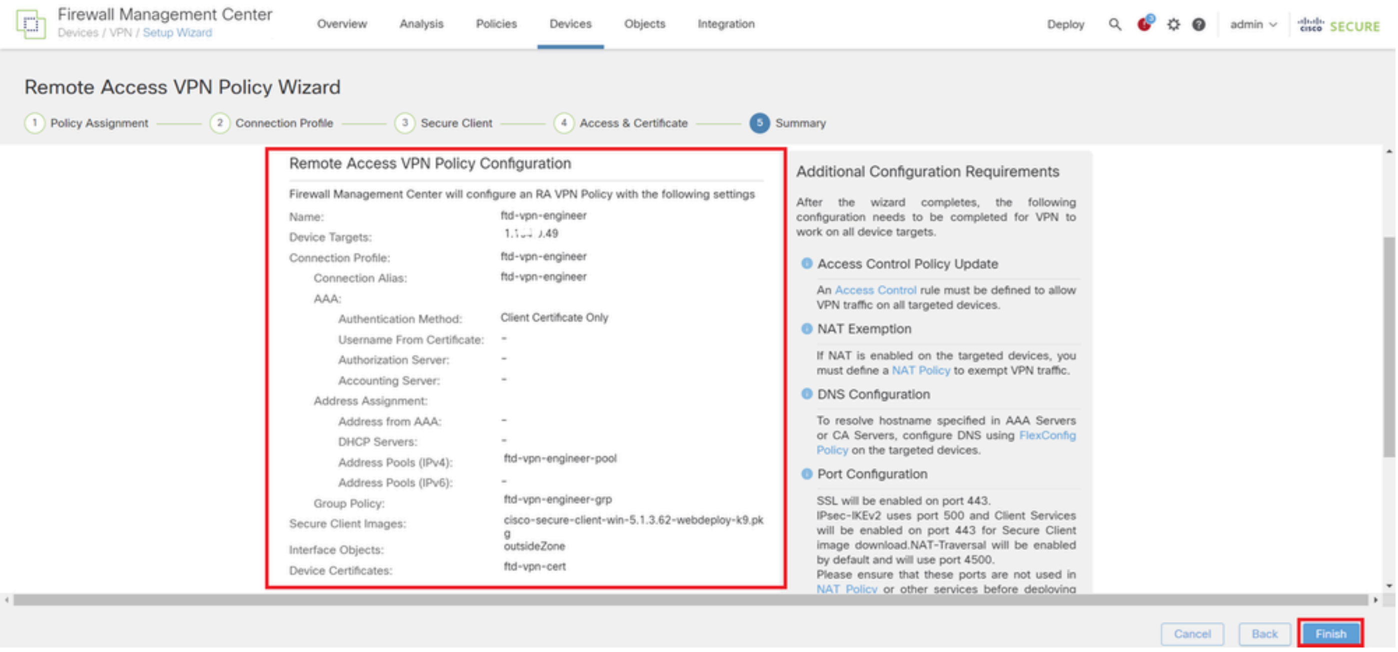
☑ Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

This option bypasses the Access Control Policy inspection, but VPN filter ACL and

Detalhes de acesso e certificado

Etapa 10. Confirmar resumo do perfil de conexão do engenheiro

Confirme as informações inseridas para a política de VPN de acesso remoto e clique no botão Finish.



Remote Access VPN Policy Configuration

Firewall Management Center will configure an RA VPN Policy with the following settings

Name: ftd-vpn-engineer
Device Targets: 1.[redacted].49
Connection Profile: ftd-vpn-engineer
Connection Alias: ftd-vpn-engineer
AAA:
Authentication Method: Client Certificate Only
Username From Certificate: -
Authorization Server: -
Accounting Server: -
Address Assignment:
Address from AAA: -
DHCP Servers: -
Address Pools (IPv4): ftd-vpn-engineer-pool
Address Pools (IPv6): -
Group Policy: ftd-vpn-engineer-grp
Secure Client Images: cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg
Interface Objects: outsideZone
Device Certificates: ftd-vpn-cert

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

Access Control Policy Update

An Access Control rule must be defined to allow VPN traffic on all targeted devices.

NAT Exemption

If NAT is enabled on the targeted devices, you must define a NAT Policy to exempt VPN traffic.

DNS Configuration

To resolve hostname specified in AAA Servers or CA Servers, configure DNS using FlexConfig Policy on the targeted devices.

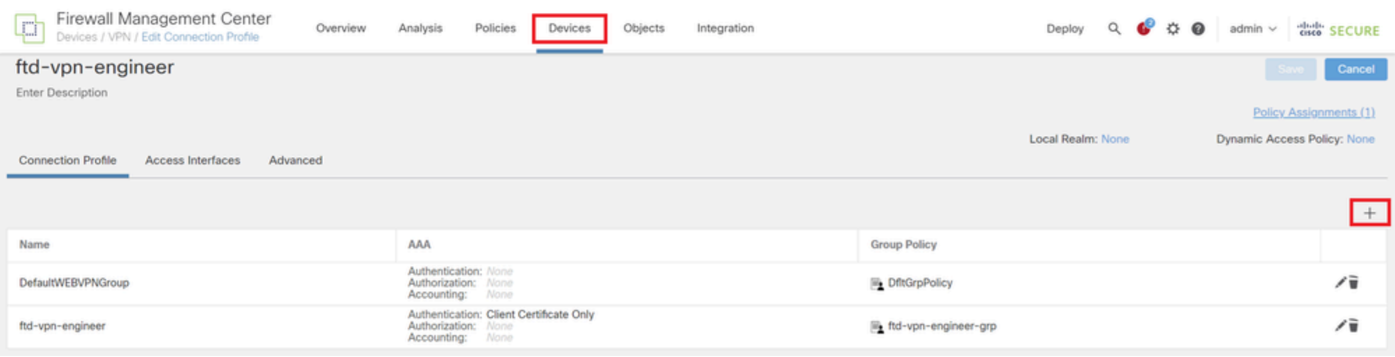
Port Configuration

SSL will be enabled on port 443.
IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Secure Client image download.NAT-Traversal will be enabled by default and will use port 4500.
Please ensure that these ports are not used in NAT Policy or other services before deploving

Detalhes da Política de VPN de Acesso Remoto

Etapa 11. Adicionar perfil de conexão para o Manager VPN Client

Navegue até Devices > VPN > Remote Access > Connection Profile, clique no botão +.



ftd-vpn-engineer

Enter Description

Policy Assignments (1)

Local Realm: None

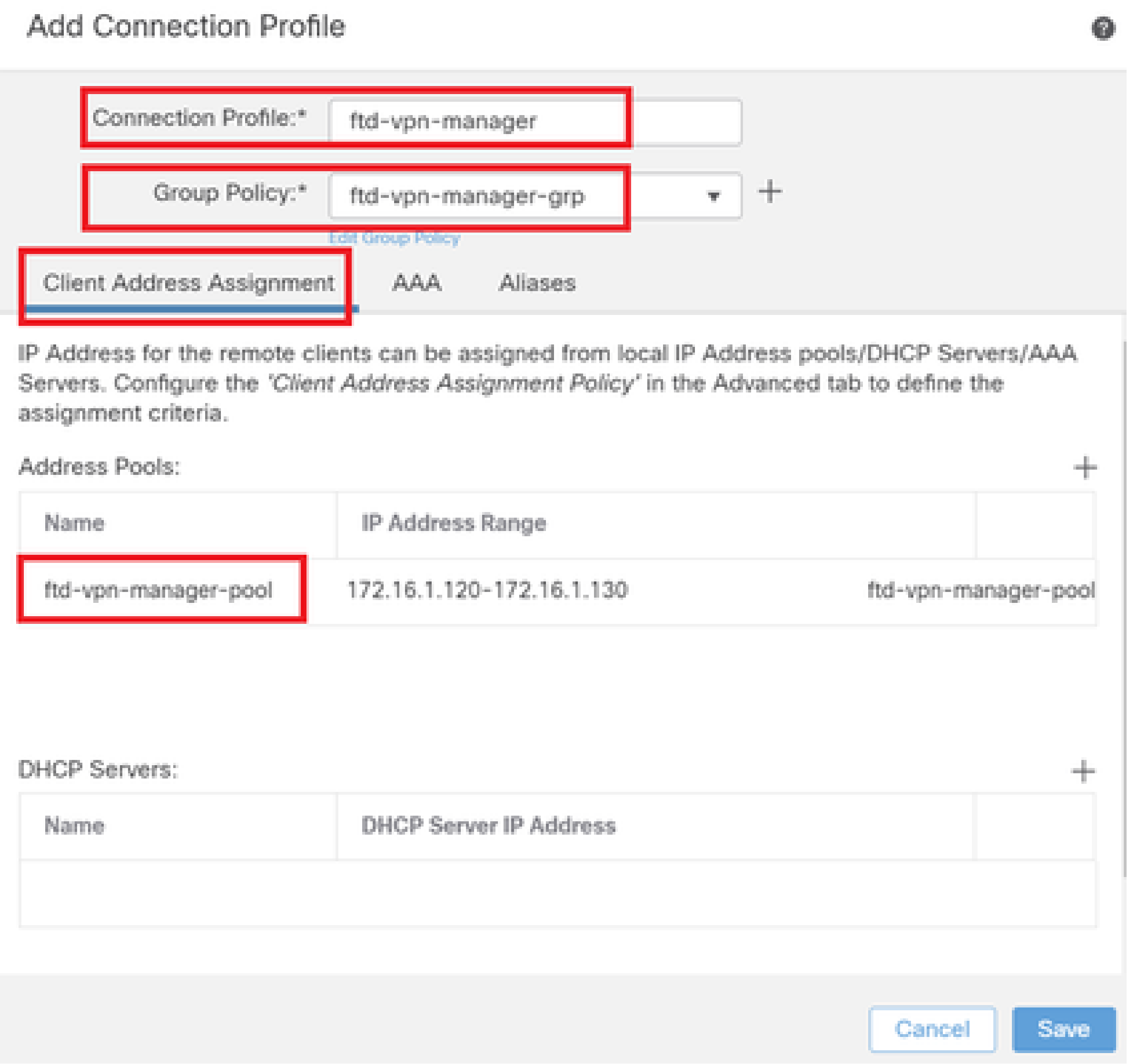
Dynamic Access Policy: None

| Name | AAA | Group Policy | |
|---|---|---|---|
| DefaultWEBVPNGroup | Authentication: None<br>Authorization: None<br>Accounting: None | DfltGrpPolicy | |
| ftd-vpn-engineer | Authentication: Client Certificate Only<br>Authorization: None<br>Accounting: None | ftd-vpn-engineer-grp | |

Adicionar perfil de conexão para o Manager VPN Client

Insira as informações necessárias para o perfil de conexão e clique no botão Save.

- Nome: ftd-vpn-manager
- Política de Grupo: ftd-vpn-manager-grp
- Pools de Endereços IPv4: ftd-vpn-manager-pool



Add Connection Profile

Connection Profile:* ftd-vpn-manager

Group Policy:* ftd-vpn-manager-grp

Edit Group Policy

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the *'Client Address Assignment Policy'* in the Advanced tab to define the assignment criteria.

Address Pools:

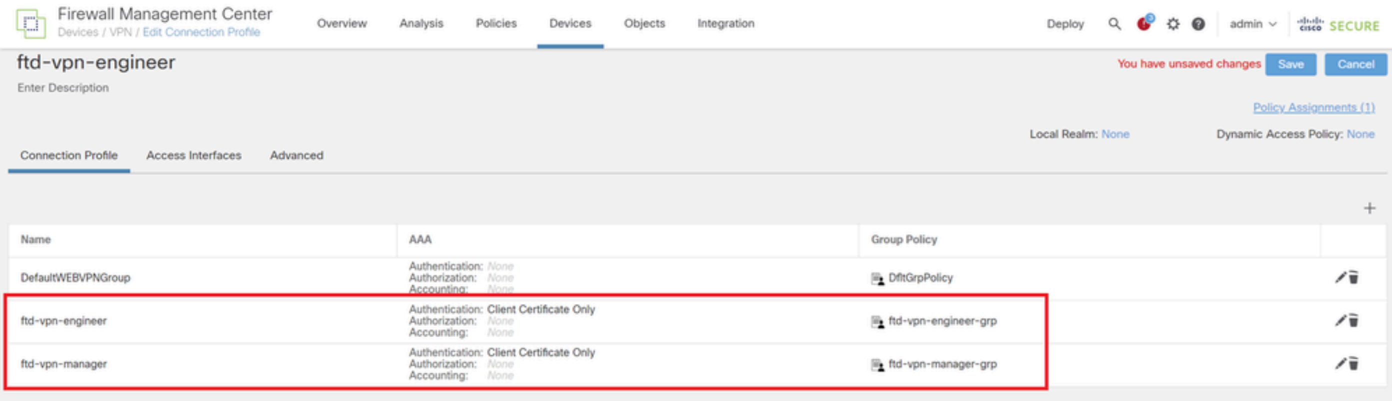
| Name | IP Address Range | |
|---|---|---|
| ftd-vpn-manager-pool | 172.16.1.120-172.16.1.130 | ftd-vpn-manager-pool |

DHCP Servers:

| Name | DHCP Server IP Address | |
|---|---|---|
| | | |

Detalhes do perfil de conexão para o Manager VPN Client

Confirme os novos perfis de conexão adicionados.



ftd-vpn-engineer

Enter Description

You have unsaved changes

Local Realm: None

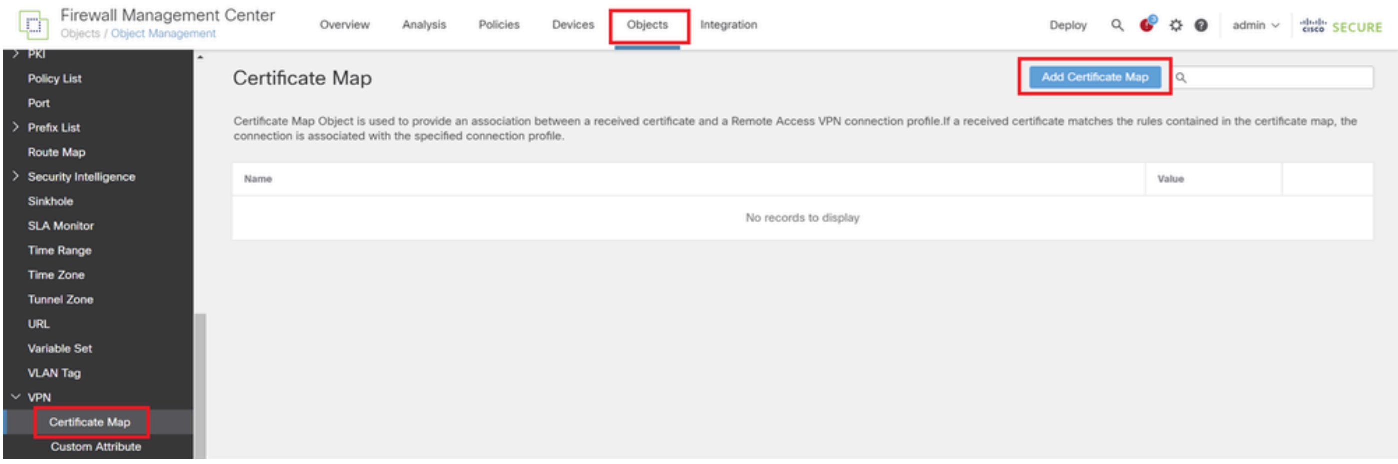
Dynamic Access Policy: None

| Name | AAA | Group Policy |
|---|---|---|
| DefaultWEBVPNGroup | Authentication: None<br>Authorization: None<br>Accounting: None | DfltGrpPolicy |
| ftd-vpn-engineer | Authentication: Client Certificate Only<br>Authorization: None<br>Accounting: None | ftd-vpn-engineer-grp |
| ftd-vpn-manager | Authentication: Client Certificate Only<br>Authorization: None<br>Accounting: None | ftd-vpn-manager-grp |

Confirmar perfis de conexão adicionados

Etapa 12. Adicionar mapa de certificado

Navegue até Objetos > Gerenciamento de objetos > VPN > Mapa de certificados, clique no botão Adicionar mapa de certificados.



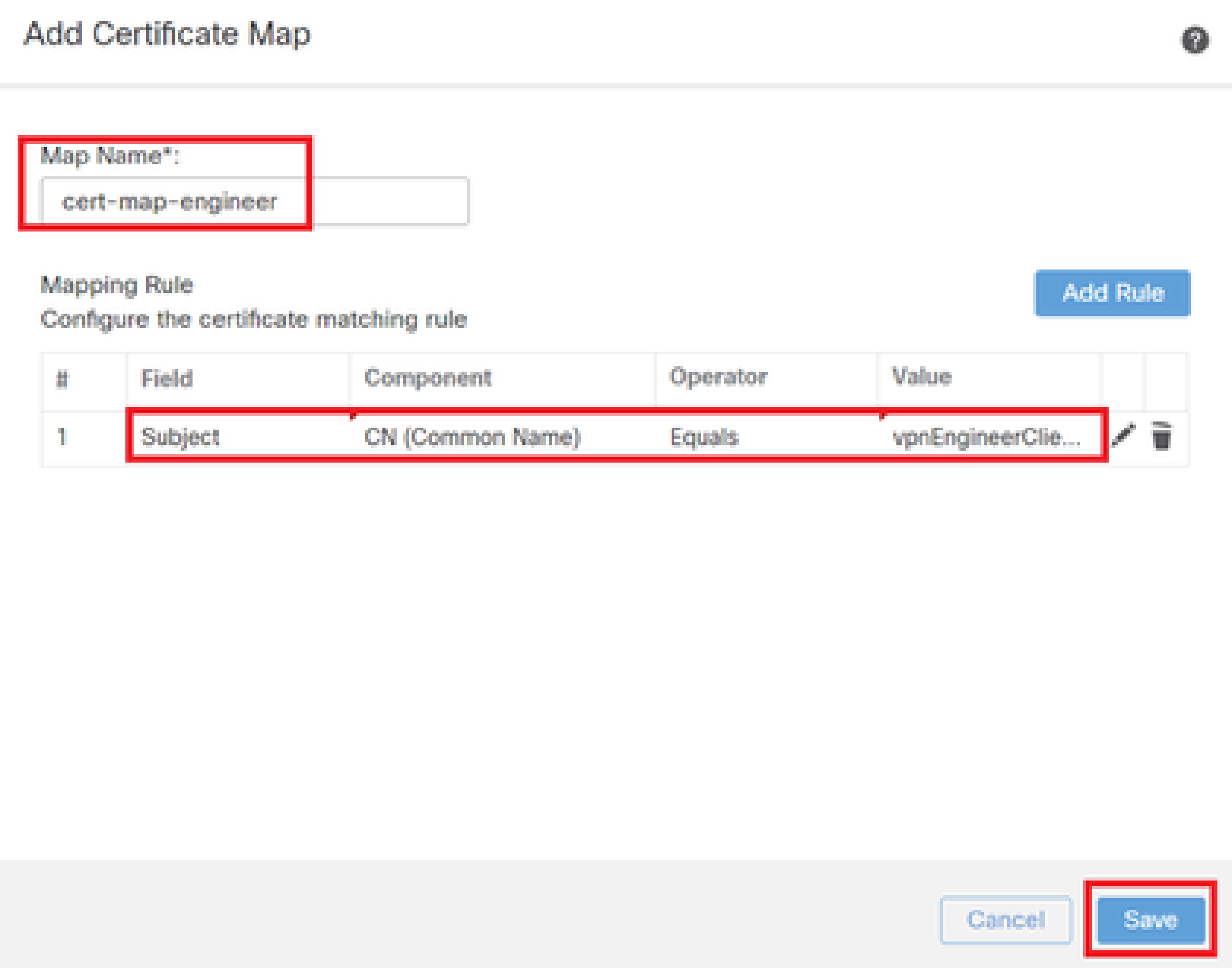
Certificate Map Object is used to provide an association between a received certificate and a Remote Access VPN connection profile.If a received certificate matches the rules contained in the certificate map, the connection is associated with the specified connection profile.

| Name | Value |
|---|---|
| No records to display | |

Adicionar mapa de certificado

Insira as informações necessárias para o mapa do certificado do cliente VPN do engenheiro e clique no botão Save.

- Nome do mapa: cert-map-engineering
- Regra de Mapeamento: CN (Nome Comum) Igual a vpnEngineerClientCN



Map Name*: cert-map-engineer

Mapping Rule

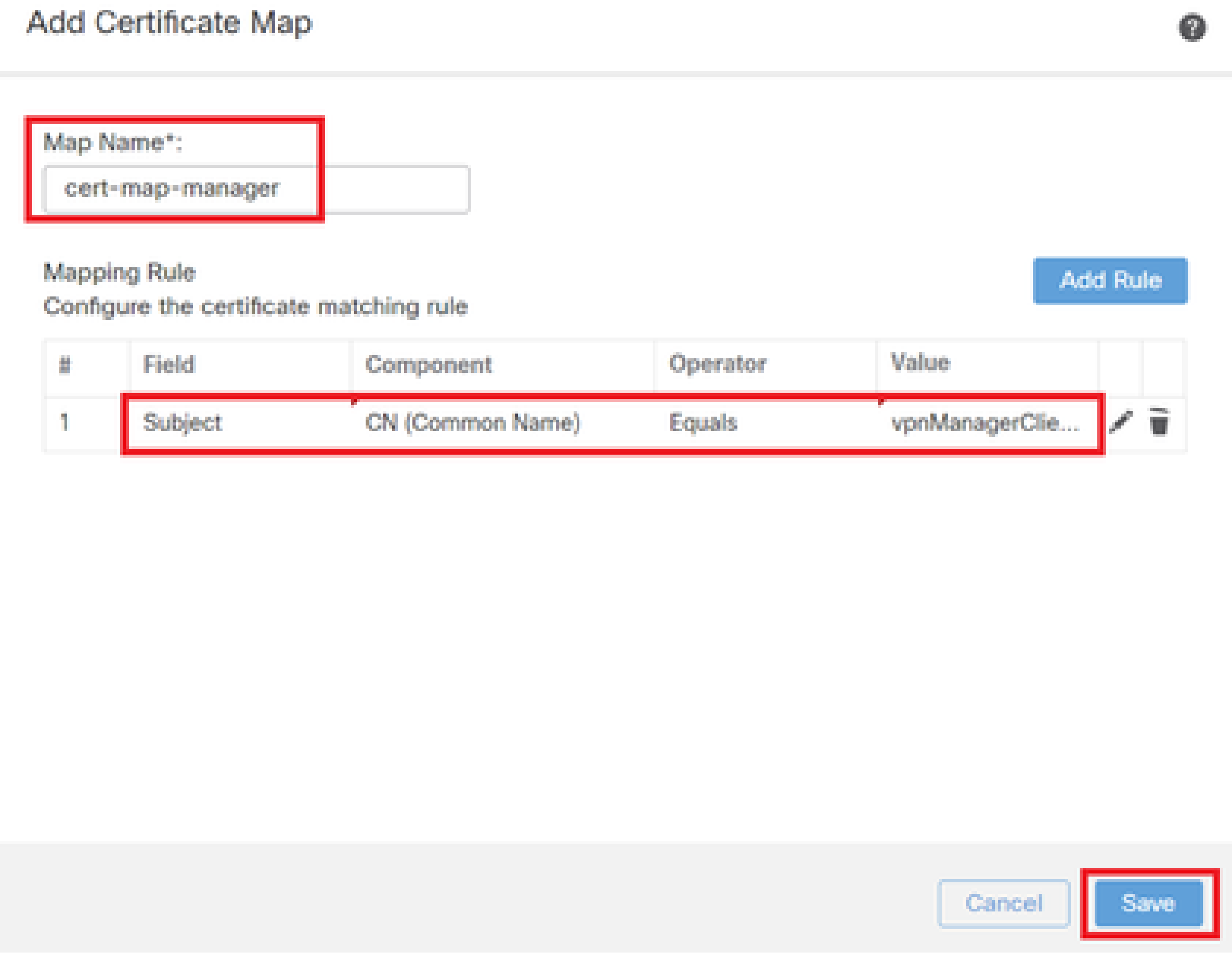
Configure the certificate matching rule

| # | Field | Component | Operator | Value |
|---|---|---|---|---|
| 1 | Subject | CN (Common Name) | Equals | vpnEngineerClie... |

Mapa do certificado para o cliente do engenheiro

Insira as informações necessárias para o mapa de certificado do cliente VPN do gerenciador e clique no botão Save.

- Nome do mapa: cert-map-manager
- Regra de Mapeamento: CN (Nome Comum) Igual a vpnManagerClientCN



Add Certificate Map

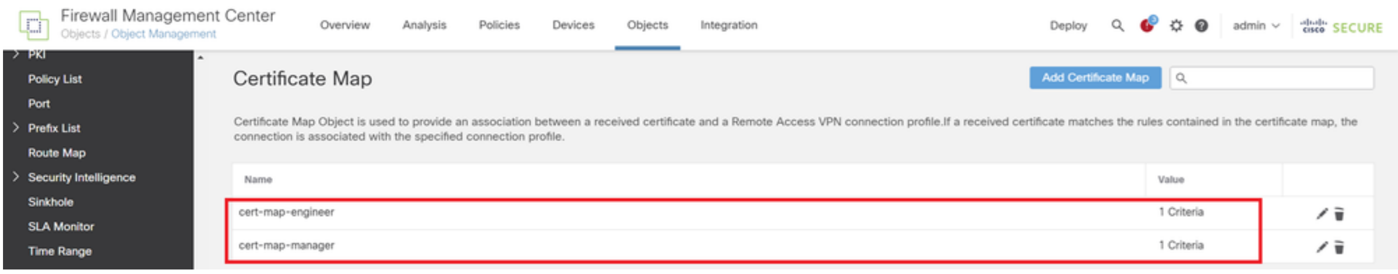
Map Name*: cert-map-manager

Mapping Rule
Configure the certificate matching rule

| # | Field | Component | Operator | Value |
|---|---|---|---|---|
| 1 | Subject | CN (Common Name) | Equals | vpnManagerClie... |

Mapa de Certificado para Cliente do Gerenciador

Confirme os novos mapas de certificados adicionados.



Certificate Map

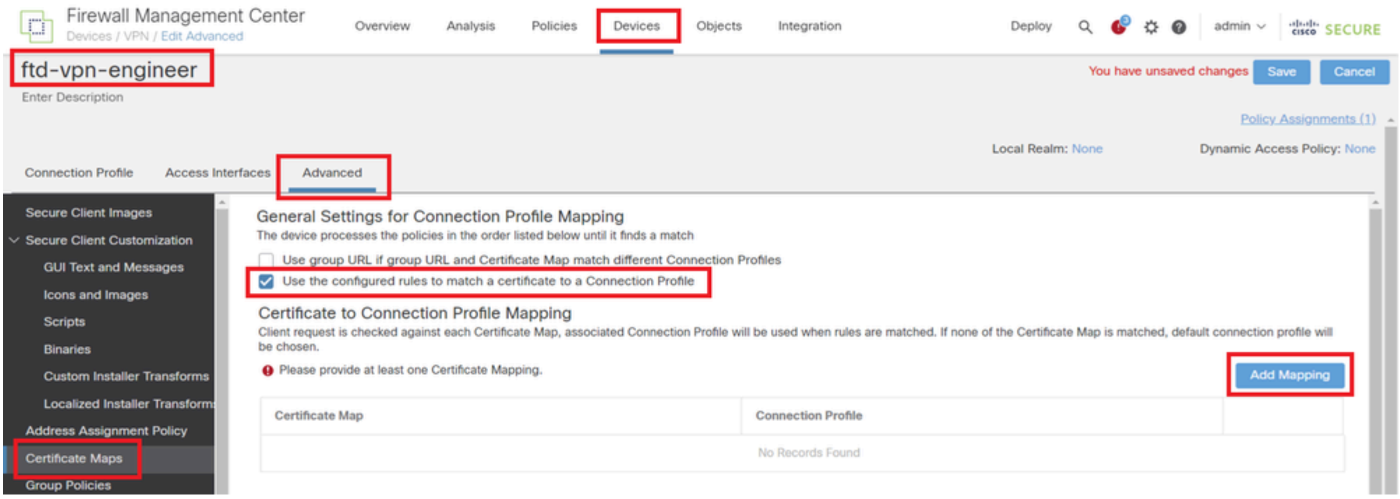
Certificate Map Object is used to provide an association between a received certificate and a Remote Access VPN connection profile.If a received certificate matches the rules contained in the certificate map, the connection is associated with the specified connection profile.

| Name | Value |
|---|---|
| cert-map-engineer | 1 Criteria |
| cert-map-manager | 1 Criteria |

Novos Mapas de Certificados

Etapa 13. Associar Mapa de Certificado ao Perfil de Conexão

Navegue até Devices > VPN > Remote Access, edite ftd-vpn-engineering. Em seguida, navegue até Avançado > Mapas de certificados, clique no botão Adicionar mapeamento.



ftd-vpn-engineer

Enter Description

You have unsaved changes

Local Realm: None

Dynamic Access Policy: None

General Settings for Connection Profile Mapping

The device processes the policies in the order listed below until it finds a match

□ Use group URL if group URL and Certificate Map match different Connection Profiles

☑ Use the configured rules to match a certificate to a Connection Profile

Certificate to Connection Profile Mapping

Client request is checked against each Certificate Map, associated Connection Profile will be used when rules are matched. If none of the Certificate Map is matched, default connection profile will be chosen.

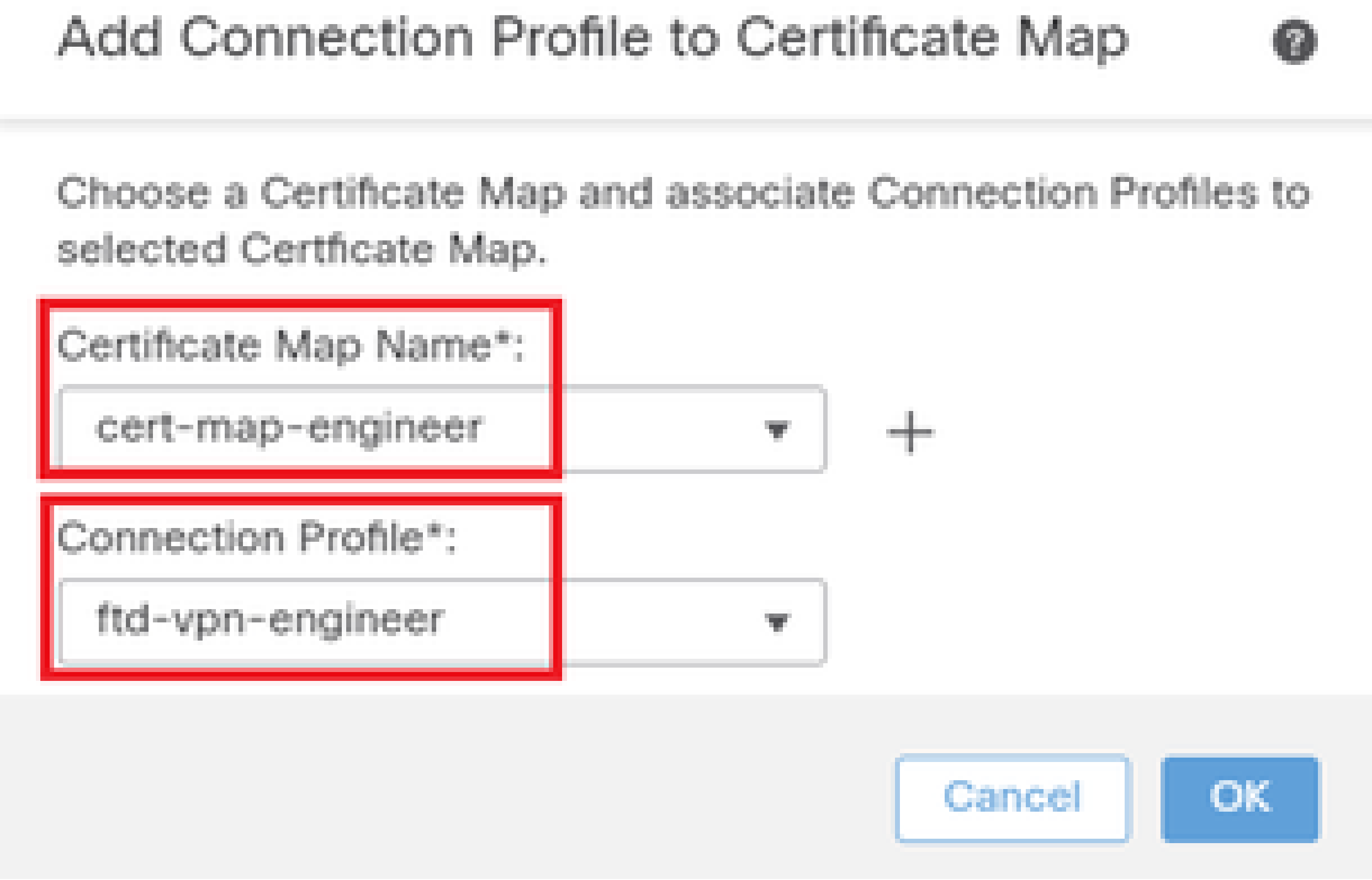
Please provide at least one Certificate Mapping.

| Certificate Map | Connection Profile | |
|---|---|---|
| | No Records Found | |

Associar Mapa de Certificado

Associando mapa de certificado ao perfil de conexão do cliente VPN do engenheiro.

- Nome do mapa do certificado: cert-map-engineering
- Conexão Profile: ftd-vpn-engineer



Add Connection Profile to Certificate Map

Choose a Certificate Map and associate Connection Profiles to selected Certficate Map.

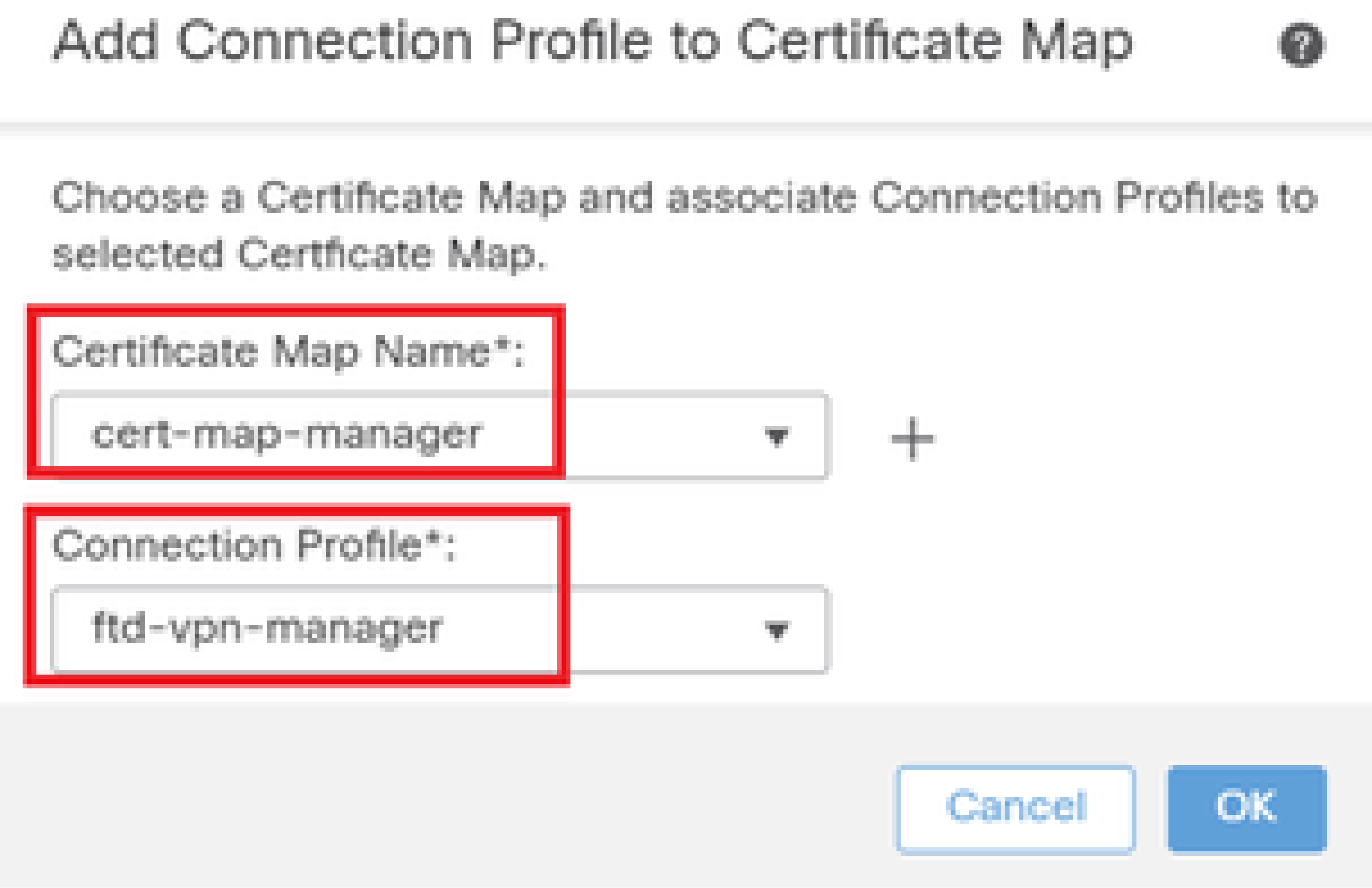
Certificate Map Name*: cert-map-engineer

Connection Profile*: ftd-vpn-engineer

Mapa do certificado de vinculação para o cliente VPN do engenheiro

Associando mapa de certificado ao perfil de conexão do cliente VPN do gerenciador.

- Nome do mapa do certificado: cert-map-manager
- Perfil de conexão: ftd-vpn-manager



Add Connection Profile to Certificate Map

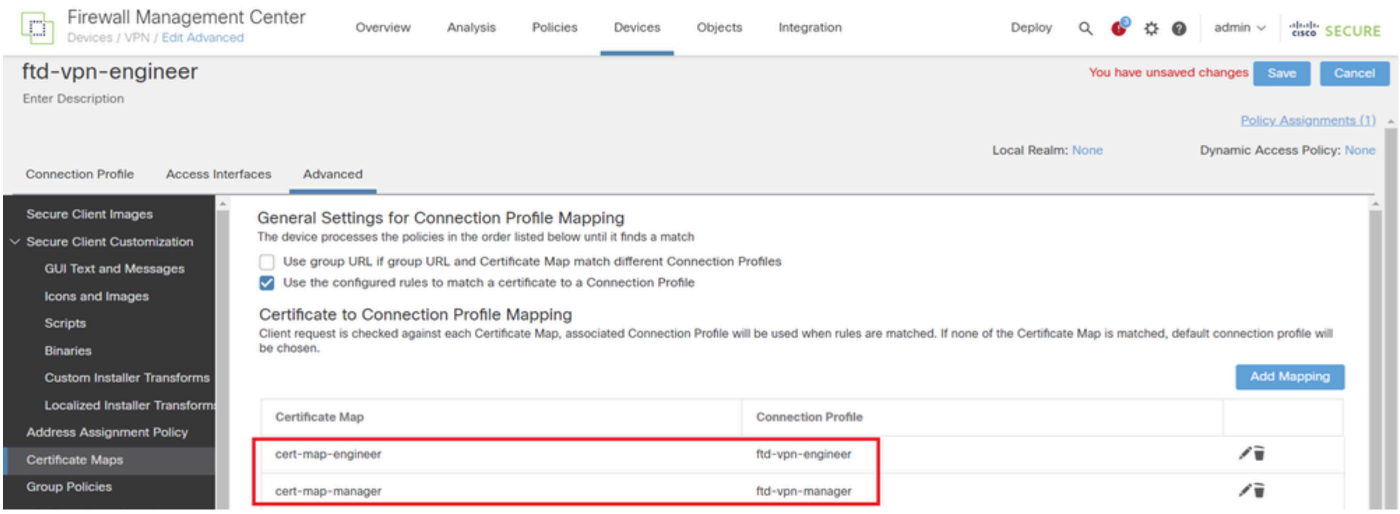
Choose a Certificate Map and associate Connection Profiles to selected Certficate Map.

Certificate Map Name*: cert-map-manager

Connection Profile*: ftd-vpn-manager

Mapa do Certificado de Vinculação para o Cliente VPN do Manager

Confirme a configuração da associação de certificado.



ftd-vpn-engineer

Enter Description

You have unsaved changes

Local Realm: None

Dynamic Access Policy: None

General Settings for Connection Profile Mapping

The device processes the policies in the order listed below until it finds a match

□ Use group URL if group URL and Certificate Map match different Connection Profiles

☑ Use the configured rules to match a certificate to a Connection Profile

Certificate to Connection Profile Mapping

Client request is checked against each Certificate Map, associated Connection Profile will be used when rules are matched. If none of the Certificate Map is matched, default connection profile will be chosen.

| Certificate Map | Connection Profile |
|---|---|
| cert-map-engineer | ftd-vpn-engineer |
| cert-map-manager | ftd-vpn-manager |

Confirmar Associação de Certificado

## Confirmar na CLI do FTD

Confirme as configurações de conexão VPN na CLI do FTD após a implantação do FMC.

```
// Defines IP of interface
interface GigabitEthernet0/0
```

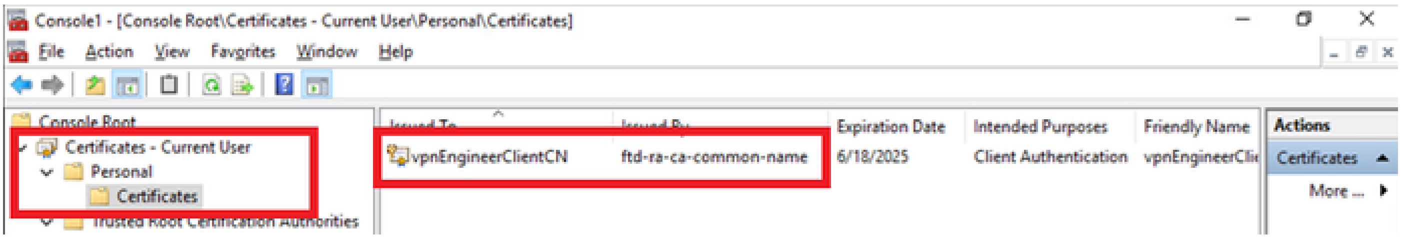
```
nameif outside
security-level 0
ip address 192.168.1.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftd-vpn-engineer-pool 172.16.1.100-172.16.1.110 mask 255.255.255.0
ip local pool ftd-vpn-manager-pool 172.16.1.120-172.16.1.130 mask 255.255.255.0

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

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

certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
......
quit

// Defines Certificate Map for Engineer VPN Clients
crypto ca certificate map cert-map-engineer 10
subject-name attr cn eq vpnEngineerClientCN

// Defines Certificate Map for Manager VPN Clients
crypto ca certificate map cert-map-manager 10
subject-name attr cn eq vpnManagerClientCN

// 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
certificate-group-map cert-map-engineer 10 ftd-vpn-engineer
certificate-group-map cert-map-manager 10 ftd-vpn-manager
error-recovery disable

// Configures the group-policy to allow SSL connections from manager VPN clients
group-policy ftd-vpn-manager-grp internal
group-policy ftd-vpn-manager-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 ikev2 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 group-policy to allow SSL connections from engineer VPN clients
group-policy ftd-vpn-engineer-grp internal
group-policy ftd-vpn-engineer-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 certificate authentication for engineer VPN clients
tunnel-group ftd-vpn-engineer type remote-access
tunnel-group ftd-vpn-engineer general-attributes
address-pool ftd-vpn-engineer-pool
default-group-policy ftd-vpn-engineer-grp
tunnel-group ftd-vpn-engineer webvpn-attributes
authentication certificate
group-alias ftd-vpn-engineer enable

// Configures the tunnel-group to use the certificate authentication for manager VPN clients
tunnel-group ftd-vpn-manager type remote-access
tunnel-group ftd-vpn-manager general-attributes
address-pool ftd-vpn-manager-pool
default-group-policy ftd-vpn-manager-grp
tunnel-group ftd-vpn-manager webvpn-attributes
authentication certificate
```

## Confirmar no cliente VPN

### Etapa 1. Confirmar certificado do cliente

No cliente VPN do engenheiro, navegue paraCertificates - Current User > Personal > Certificates, verifique o certificado do cliente usado para autenticação.

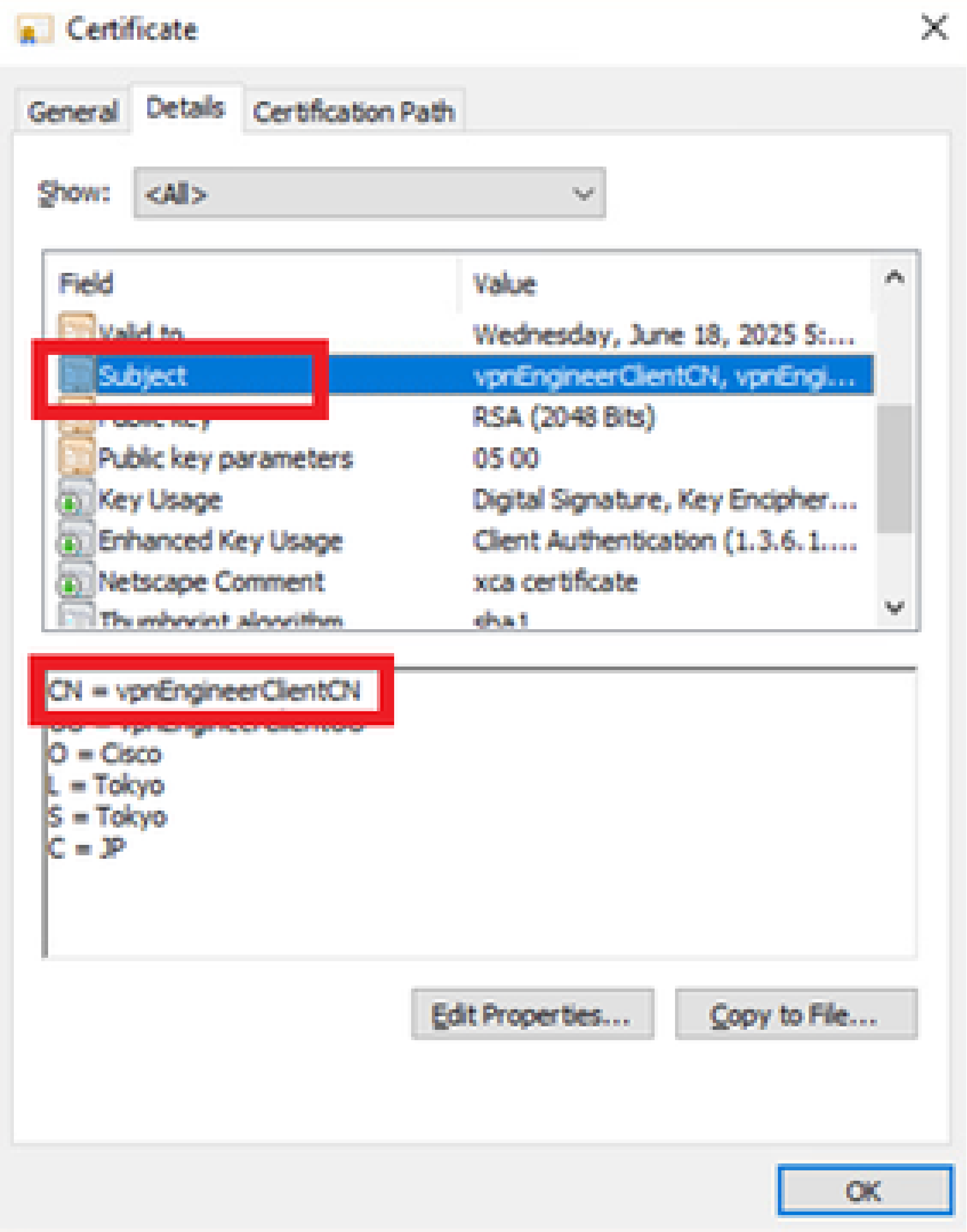

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Actions
Certificates
More ...

| Issued To | Issued By | Expiration Date | Intended Purposes | Friendly Name |
|---|---|---|---|---|
| vpnEngineerClientCN | ftd-ra-ca-common-name | 6/18/2025 | Client Authentication | vpnEngineerCli |

Confirmar certificado para cliente VPN do engenheiro

Clique duas vezes no certificado do cliente, navegue paraDetails, verifique os detalhes deSubject.

- Assunto: CN = vpnEngineerClientCN

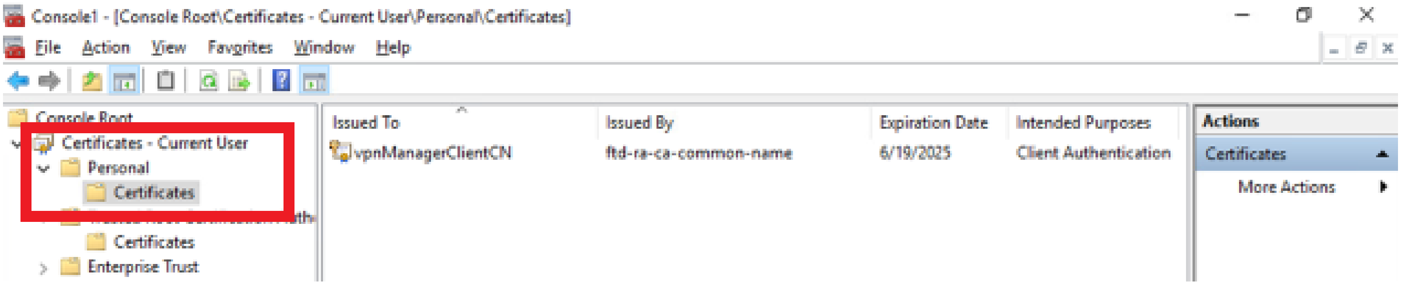


| Field | Value |
|---|---|
| Valid to | Wednesday, June 18, 2025 5:... |
| Subject | vpnEngineerClientCN, vpnEngi... |
| Public key | RSA (2048 Bits) |
| Public key parameters | 05 00 |
| Key Usage | Digital Signature, Key Encipher... |
| Enhanced Key Usage | Client Authentication (1.3.6.1.... |
| Netscape Comment | xca certificate |
| Thumbprint algorithm | sha1 |

```
CN = vpnEngineerClientCN
OU = vpnEngineerClientOU
O = Cisco
L = Tokyo
S = Tokyo
C = JP
```

Detalhes do certificado de cliente do engenheiro

No cliente VPN do gerenciador, navegue paraCertificates - Current User > Personal > Certificates, verifique o certificado do cliente usado para autenticação.

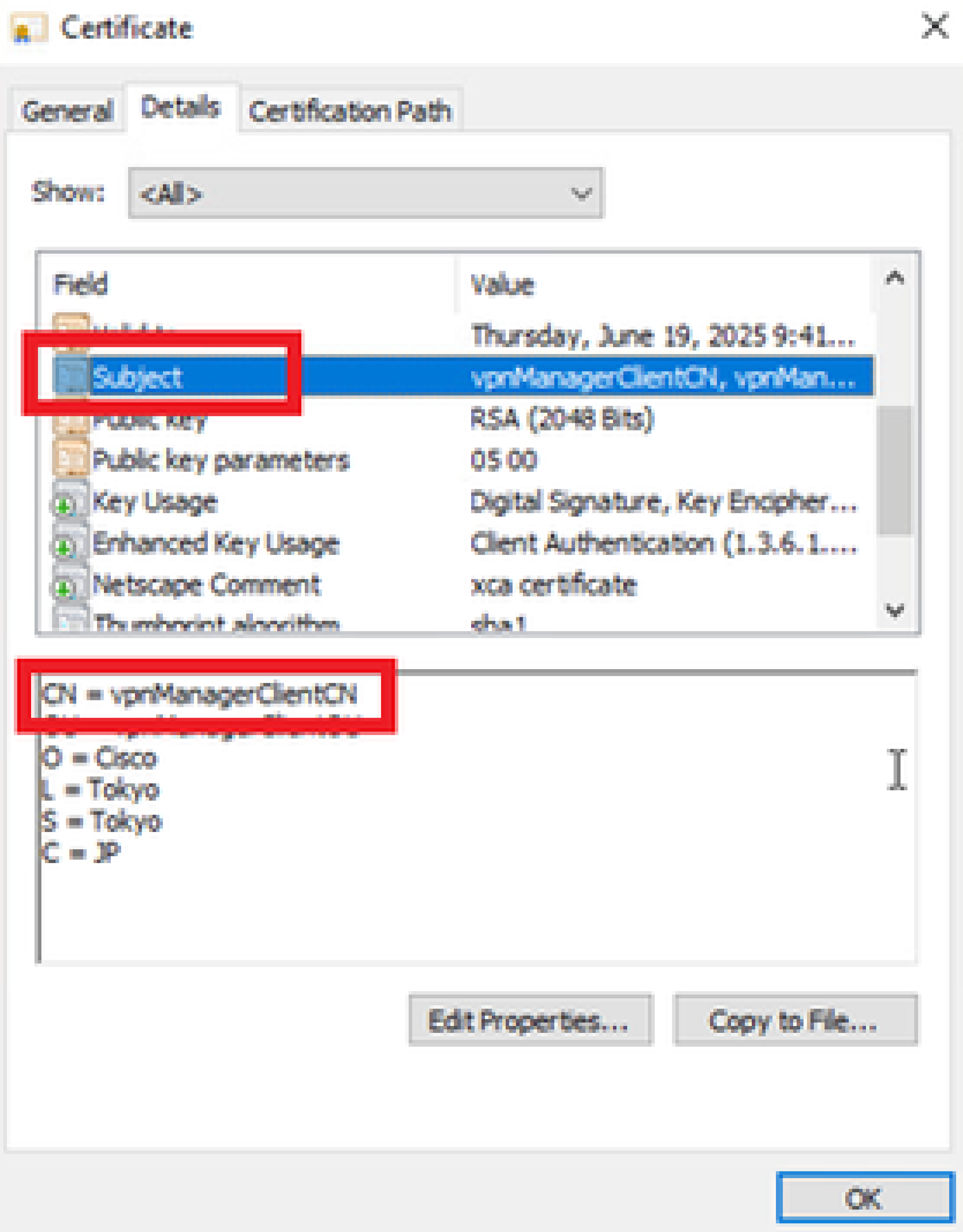


| Issued To | Issued By | Expiration Date | Intended Purposes |
|---|---|---|---|
| vpnManagerClientCN | ftd-ra-ca-common-name | 6/19/2025 | Client Authentication |

Confirmar Certificado para Cliente VPN do Manager

Clique duas vezes no certificado do cliente, navegue paraDetails, verifique os detalhes deSubject.

- Assunto: CN = vpnManagerClientCN



| Field | Value |
|---|---|
| Valid to | Thursday, June 19, 2025 9:41... |
| Subject | vpnManagerClientCN, vpnMan... |
| Public key | RSA (2048 Bits) |
| Public key parameters | 05 00 |
| Key Usage | Digital Signature, Key Encipher... |
| Enhanced Key Usage | Client Authentication (1.3.6.1.... |
| Netscape Comment | xca certificate |
| Thumbprint algorithm | sha1 |

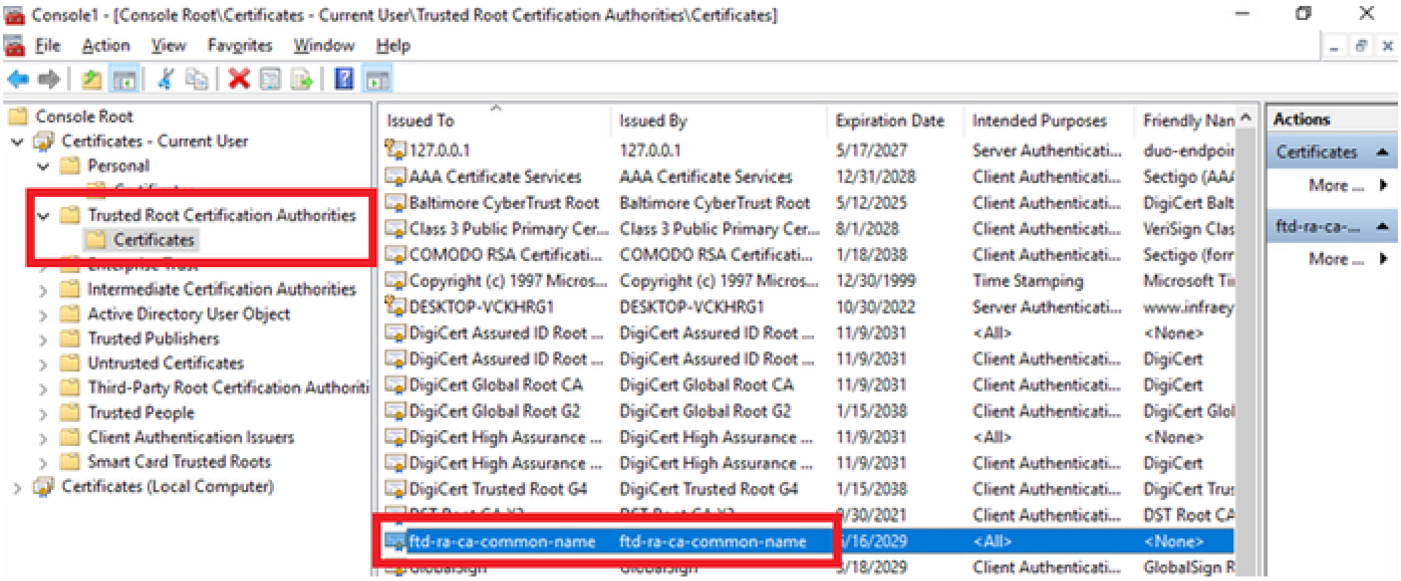
```
CN = vpnManagerClientCN
OU = vpnManagerClientOU
O = Cisco
L = Tokyo
S = Tokyo
C = JP
```

Detalhes do Certificado de Cliente do Gerenciador

Etapa 2. Confirmar CA

No cliente VPN do engenheiro e no cliente VPN do gerente, navegue paraCertificates - Current User > Trusted Root Certification Authorities > Certificates, verifique a CA usada para autenticação.

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



Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]

File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoriti
Trusted People
Client Authentication Issuers
Smart Card Trusted Roots
Certificates (Local Computer)
Actions
Certificates
More ...
ftd-ra-ca-...
More ...

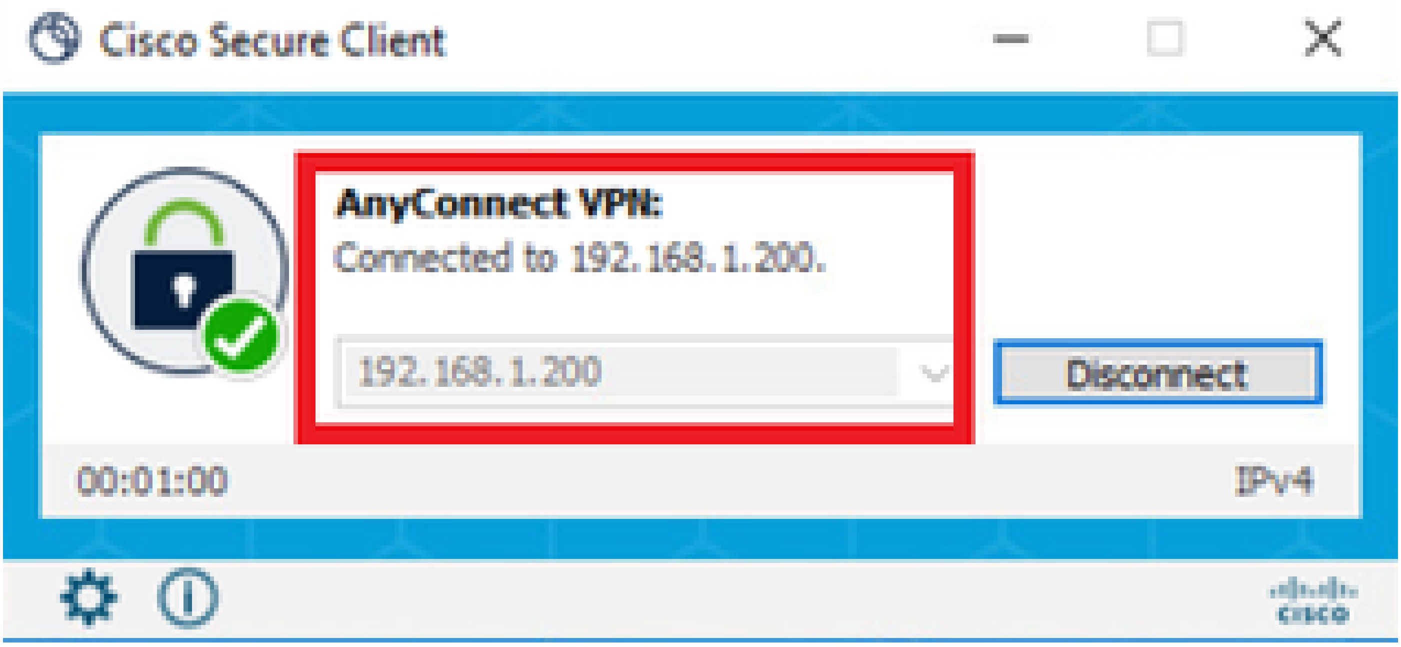
| Issued To | Issued By | Expiration Date | Intended Purposes | Friendly Nan |
|---|---|---|---|---|
| 127.0.0.1 | 127.0.0.1 | 5/17/2027 | Server Authenticati... | duo-endpoi |
| AAA Certificate Services | AAA Certificate Services | 12/31/2028 | Client Authenticati... | Sectigo (AA |
| Baltimore CyberTrust Root | Baltimore CyberTrust Root | 5/12/2025 | Client Authenticati... | DigiCert Balt |
| Class 3 Public Primary Cer... | Class 3 Public Primary Cer... | 8/1/2028 | Client Authenticati... | VeriSign Clas |
| COMODO RSA Certificati... | COMODO RSA Certificati... | 1/18/2038 | Client Authenticati... | Sectigo (forr |
| Copyright (c) 1997 Micros... | Copyright (c) 1997 Micros... | 12/30/1999 | Time Stamping | Microsoft Ti |
| DESKTOP-VCKHRG1 | DESKTOP-VCKHRG1 | 10/30/2022 | Server Authenticati... | www.infraey |
| DigiCert Assured ID Root ... | DigiCert Assured ID Root ... | 11/9/2031 | <All> | <None> |
| DigiCert Assured ID Root ... | DigiCert Assured ID Root ... | 11/9/2031 | Client Authenticati... | DigiCert |
| DigiCert Global Root CA | DigiCert Global Root CA | 11/9/2031 | Client Authenticati... | DigiCert |
| DigiCert Global Root G2 | DigiCert Global Root G2 | 1/15/2038 | Client Authenticati... | DigiCert Glol |
| DigiCert High Assurance ... | DigiCert High Assurance ... | 11/9/2031 | <All> | <None> |
| DigiCert High Assurance ... | DigiCert High Assurance ... | 11/9/2031 | Client Authenticati... | DigiCert |
| DigiCert Trusted Root G4 | DigiCert Trusted Root G4 | 1/15/2038 | Client Authenticati... | DigiCert Trus |
| DST Root CA X3 | DST Root CA X3 | 9/30/2021 | Client Authenticati... | DST Root CA |
| ftd-ra-ca-common-name | ftd-ra-ca-common-name | 6/16/2029 | <All> | <None> |
| GlobalSign | GlobalSign | 3/18/2029 | Client Authenticati... | GlobalSign R |

Confirmar CA

# Verificar

Etapa 1. Iniciar conexão VPN

No cliente VPN do engenheiro, inicie a conexão do Cisco Secure Client. Não há necessidade de inserir o nome de usuário e a senha, a VPN se conectou com êxito.

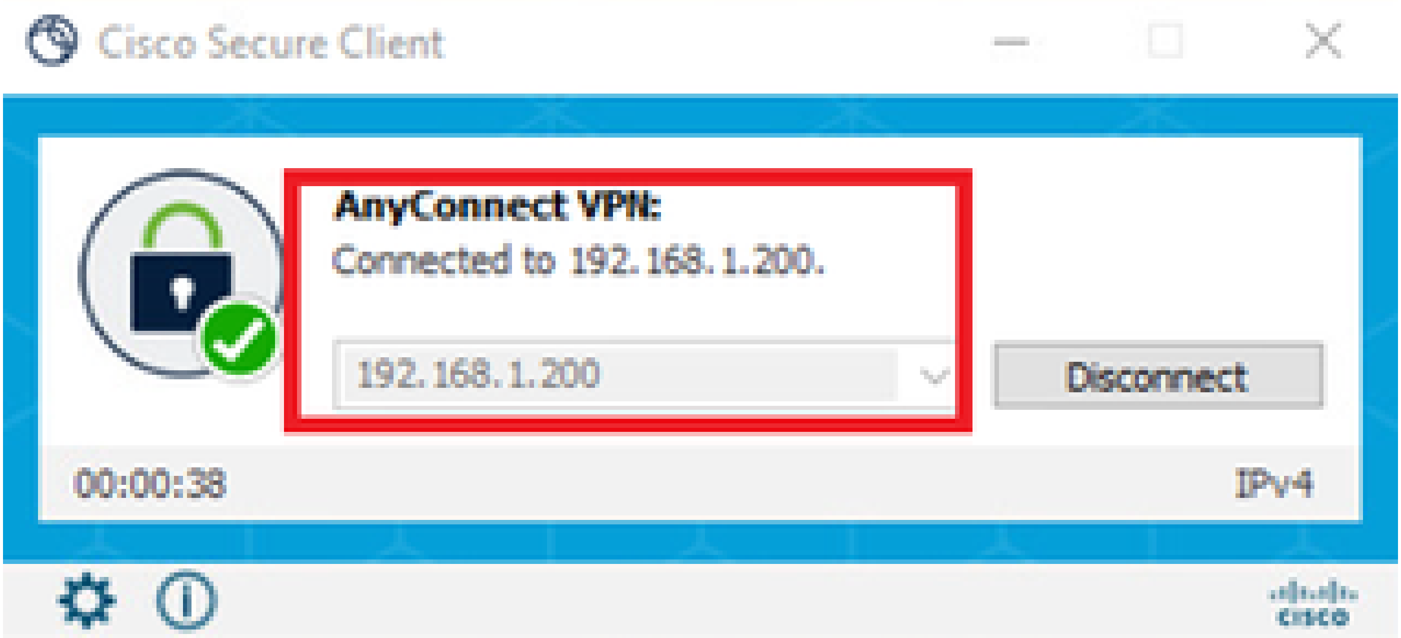


AnyConnect VPN:
Connected to 192.168.1.200.

192.168.1.200

Iniciar conexão VPN do cliente do engenheiro

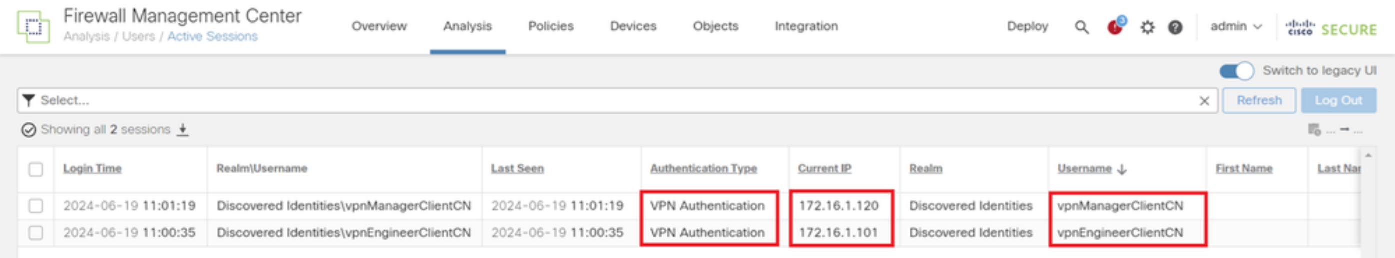
No cliente VPN do gerenciador, inicie a conexão do Cisco Secure Client. Não há necessidade de inserir o nome de usuário e a senha, a VPN se conectou com êxito.



Iniciar conexão VPN a partir do cliente gerenciador

## Etapa 2. Confirmar sessões ativas no FMC

Navegue até Analysis > Users > Ative Sessions, verifique a sessão ativa quanto à autenticação de VPN.



Showing all 2 sessions

| | Login Time | Realm\Username | Last Seen | Authentication Type | Current IP | Realm | Username ↓ | First Name | Last Nar |
|---|---|---|---|---|---|---|---|---|---|
| □ | 2024-06-19 11:01:19 | Discovered Identities\vpnManagerClientCN | 2024-06-19 11:01:19 | VPN Authentication | 172.16.1.120 | Discovered Identities | vpnManagerClientCN | | |
| □ | 2024-06-19 11:00:35 | Discovered Identities\vpnEngineerClientCN | 2024-06-19 11:00:35 | VPN Authentication | 172.16.1.101 | Discovered Identities | vpnEngineerClientCN | | |

Confirmar sessão ativa

## Etapa 3. Confirmar sessões VPN na CLI FTD

Executeshow vpn-sessiondb detail anyconnect o comando na CLI do FTD (Lina) para confirmar as sessões de VPN do engenheiro e do gerente.

```
ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 13
Assigned IP : 172.16.1.101 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 : 14782 Bytes Rx : 12714
Pkts Tx : 2 Pkts Rx : 32
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-vpn-engineer-grp Tunnel Group : ftd-vpn-engineer
Login Time : 02:00:35 UTC Wed Jun 19 2024
Duration : 0h:00m:55s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000d00066723bc3
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 13.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50225 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 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 : 7391 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 13.2
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 50232
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 1775
Pkts Tx : 1 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 13.3
Assigned IP : 172.16.1.101 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 50825
UDP Dst Port : 443 Auth Mode : Certificate
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 : 10939
Pkts Tx : 0 Pkts Rx : 30
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

```
Username : vpnManagerClientCN Index : 14
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
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 : 14782 Bytes Rx : 13521
Pkts Tx : 2 Pkts Rx : 57
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-vpn-manager-grp Tunnel Group : ftd-vpn-manager
Login Time : 02:01:19 UTC Wed Jun 19 2024
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000e00066723bef
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 14.1
Public IP : 192.168.1.21
Encryption : none Hashing : none
TCP Src Port : 49809 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 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 : 7391 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 14.2
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 49816
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7391 Bytes Rx : 3848
Pkts Tx : 1 Pkts Rx : 25
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 14.3
Assigned IP : 172.16.1.120 Public IP : 192.168.1.21
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 65501
UDP Dst Port : 443 Auth Mode : Certificate
```

```
Idle Time Out: 30 Minutes Idle TO Left : 30 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 : 9673
Pkts Tx : 0 Pkts Rx : 32
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

## Troubleshooting

Você pode esperar encontrar informações sobre a autenticação VPN no syslog de depuração do mecanismo Lina e no arquivo DART no PC com Windows.

Este é um exemplo de logs de depuração no mecanismo Lina durante a conexão VPN do cliente do engenheiro.

<#root>

```
Jun 19 2024 02:00:35: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpn
Jun 19 2024 02:00:35: %FTD-6-717022:

Certificate was successfully validated

. serial number: 7AF1C78ADCC8F941, subject name:

CN=vpnEngineerClientCN

,OU=vpnEngineerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.
Jun 19 2024 02:00:35: %FTD-7-717038: Tunnel group match found.

Tunnel Group: ftd-vpn-engineer

, Peer certificate: serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN,OU=vpnEnginee
Jun 19 2024 02:00:35: %FTD-6-113009: AAA retrieved default group policy (ftd-vpn-engineer-grp) for user
Jun 19 2024 02:00:46: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50
```

Este é um exemplo de logs de depuração no mecanismo Lina durante a conexão VPN do cliente gerenciador.

<#root>

```
Jun 19 2024 02:01:19: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 1AD1B5EAE28C6D3C, subject name: CN=vp
Jun 19 2024 02:01:19: %FTD-6-717022:

Certificate was successfully validated

. serial number: 1AD1B5EAE28C6D3C, subject name:

 CN=vpnManagerClientCN

,OU=vpnManagerClientOU,O=Cisco,L=Tokyo,ST=Tokyo,C=JP.
Jun 19 2024 02:01:19: %FTD-7-717038: Tunnel group match found.

Tunnel Group: ftd-vpn-manager

, Peer certificate: serial number: 1AD1B5EAE28C6D3C, subject name: CN=vpnManagerClientCN,OU=vpnManagerC
Jun 19 2024 02:01:19: %FTD-6-113009: AAA retrieved default group policy (ftd-vpn-manager-grp) for user =
Jun 19 2024 02:01:25: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.21/65
```

Informações Relacionadas

[Configurar Autenticação Baseada em Certificado do Anyconnect para Acesso Móvel]()