Configurar AAA e Cert Auth para Secure Client no FTD via FMC

Contents

Introdução

Este documento descreve as etapas para configurar o Cisco Secure Client over SSL no FTD gerenciado pelo FMC com AAA e autenticação de certificado.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Firepower Management Center (FMC)
- Firewall Threat Defense Virtual (FTD)
- 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

À medida que as empresas adotam medidas de segurança mais rigorosas, a combinação da autenticação de dois fatores (2FA) com a autenticação baseada em certificado tornou-se uma prática comum para melhorar a segurança e proteger contra acesso não autorizado. Um dos recursos que podem melhorar significativamente a experiência e a segurança do usuário é a capacidade de preencher previamente o nome de usuário no Cisco Secure Client. Esse recurso simplifica o processo de login e melhora a eficiência geral do acesso remoto.
Este documento descreve como integrar o nome de usuário pré-preenchido com o Cisco Secure Client no FTD, garantindo que os usuários possam se conectar à rede de forma rápida e segura.

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

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

Diagrama de Rede

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

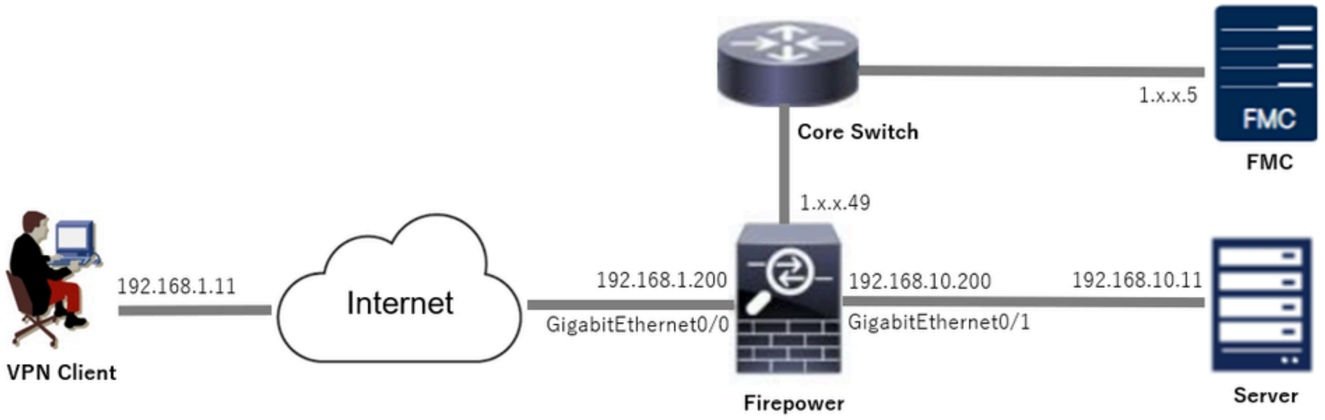


Diagrama de Rede

Configurações

Configuração no FMC

Etapa 1. Configurar a interface FTD

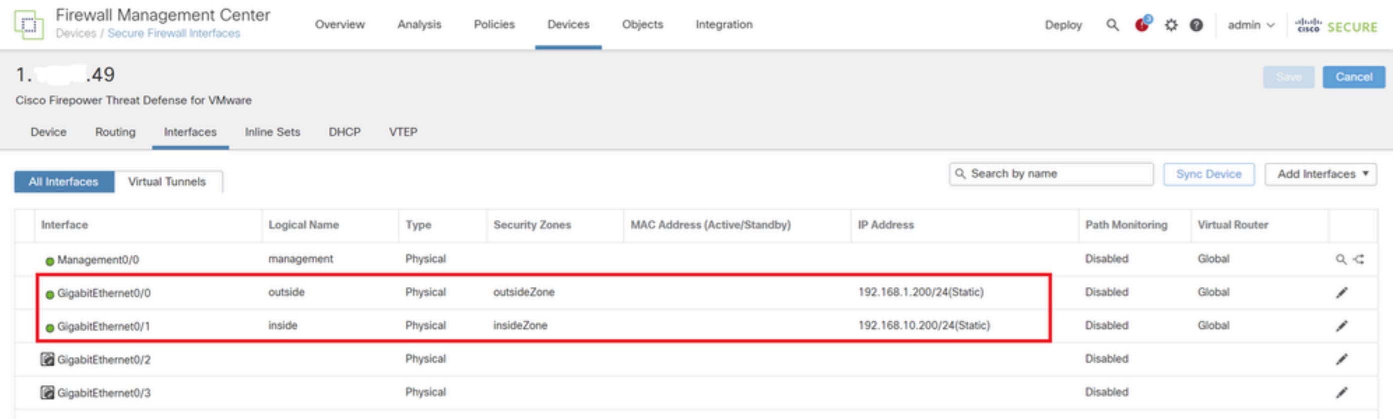
Navegue até Devices > Device Management, edite o dispositivo FTD de destino, configure a interface interna e externa para FTD na guia Interfaces.

Para GigabitEthernet0/0,

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

Para GigabitEthernet0/1,

- Nome : dentro
- Zona de segurança : insideZone
- Endereço IP: 192.168.10.200/24



1.[redacted].49

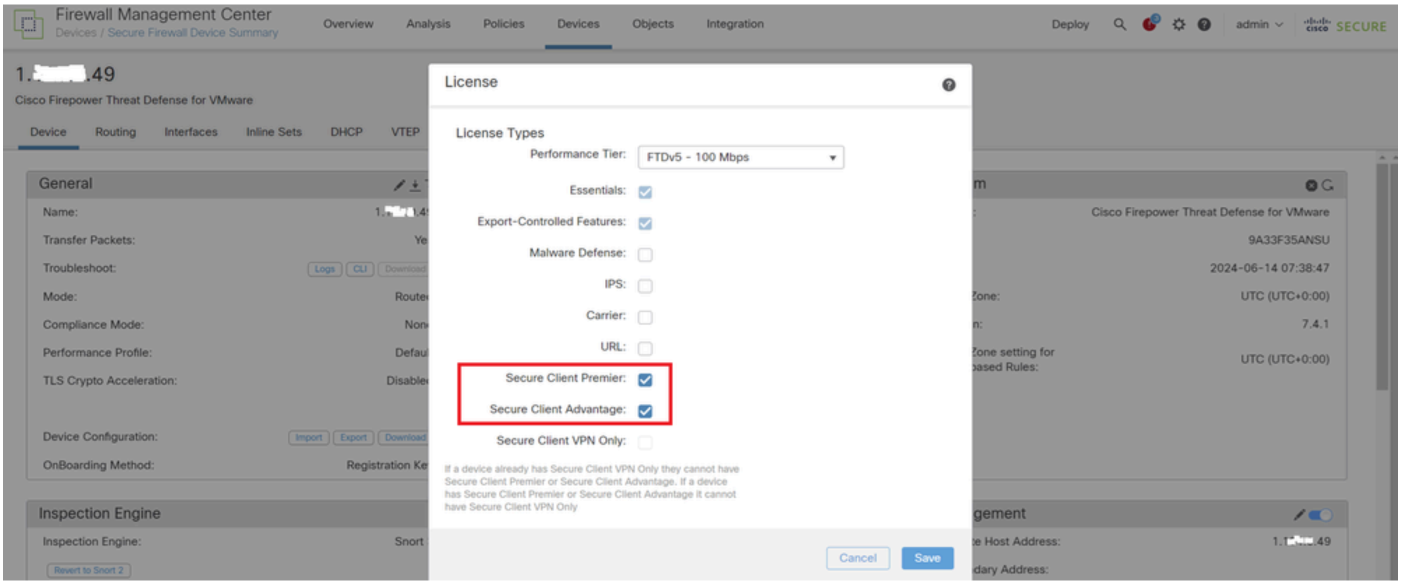
Cisco Firepower Threat Defense for VMware

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
GigabitEthernet0/1	inside	Physical	insideZone		192.168.10.200/24(Static)	Disabled	Global
GigabitEthernet0/2		Physical				Disabled	
GigabitEthernet0/3		Physical				Disabled	

Interface FTD

Etapa 2. Confirmar licença do Cisco Secure Client

Navegue até Devices > Device Management, edite o dispositivo FTD de destino, confirme a licença do Cisco Secure Client na guia Device.



Firewall Management Center
Devices / Secure Firewall Device Summary

1.[redacted].49
Cisco Firepower Threat Defense for VMware

License

License Types

Performance Tier: FTDv5 - 100 Mbps

Essentials: ☑

Export-Controlled Features: ☑

Malware Defense: □

IPS: □

Carrier: □

URL: □

Secure Client Premier: ☑

Secure Client Advantage: ☑

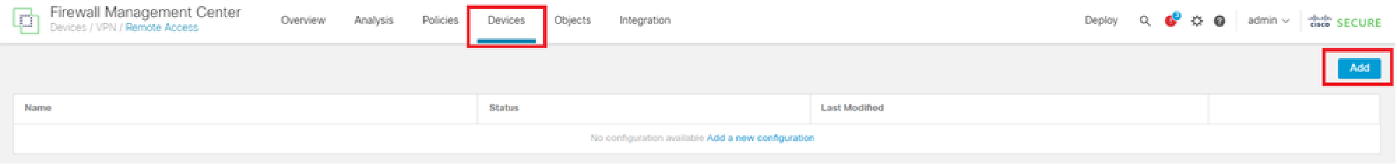
Secure Client VPN Only: □

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

Licença de cliente seguro

Etapa 3. Adicionar Atribuição de Política

Navegue até Devices > VPN > Remote Access e clique no botão Add.



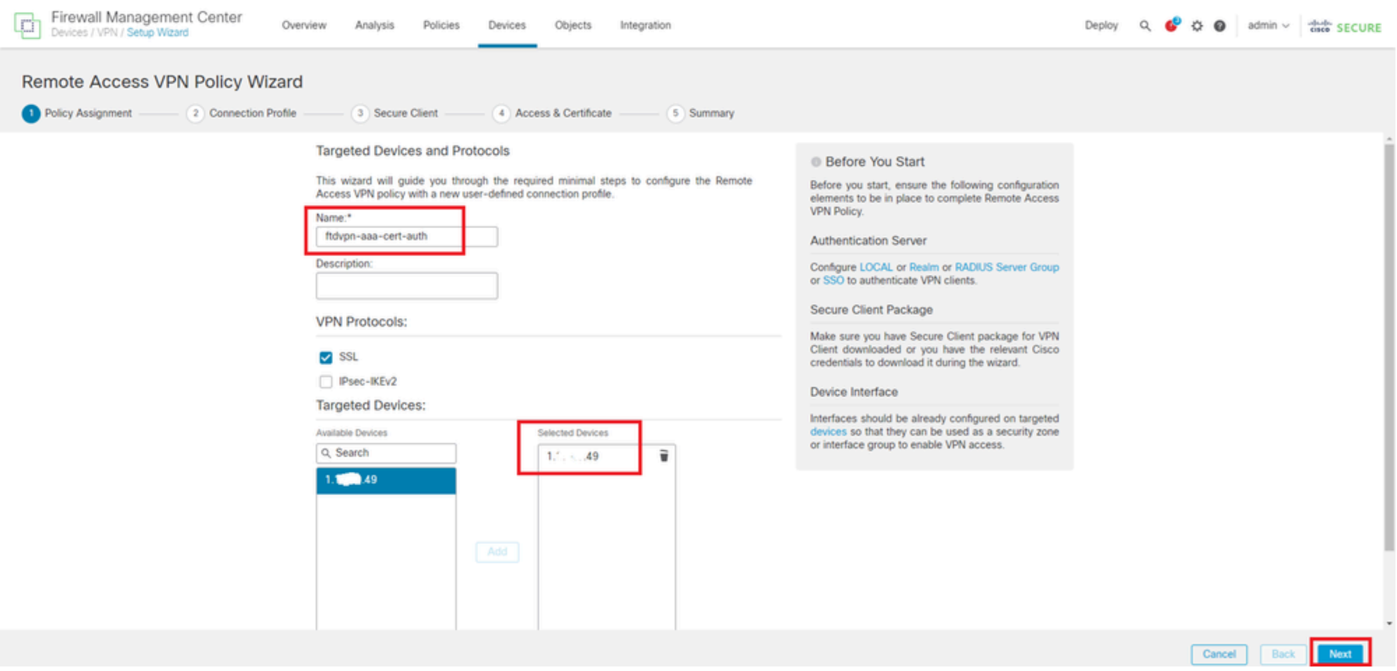
Firewall Management Center
Devices / VPN / Remote Access

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 : ftdvpn-aaa-cert-auth
- Protocolos VPN: SSL
- Dispositivos de destino: 1.x.x.49



Remote Access VPN Policy Wizard

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:* ftdvpn-aaa-cert-auth

Description:

VPN Protocols:

☑ SSL

□ IPsec-IKEv2

Targeted Devices:

Available Devices: 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

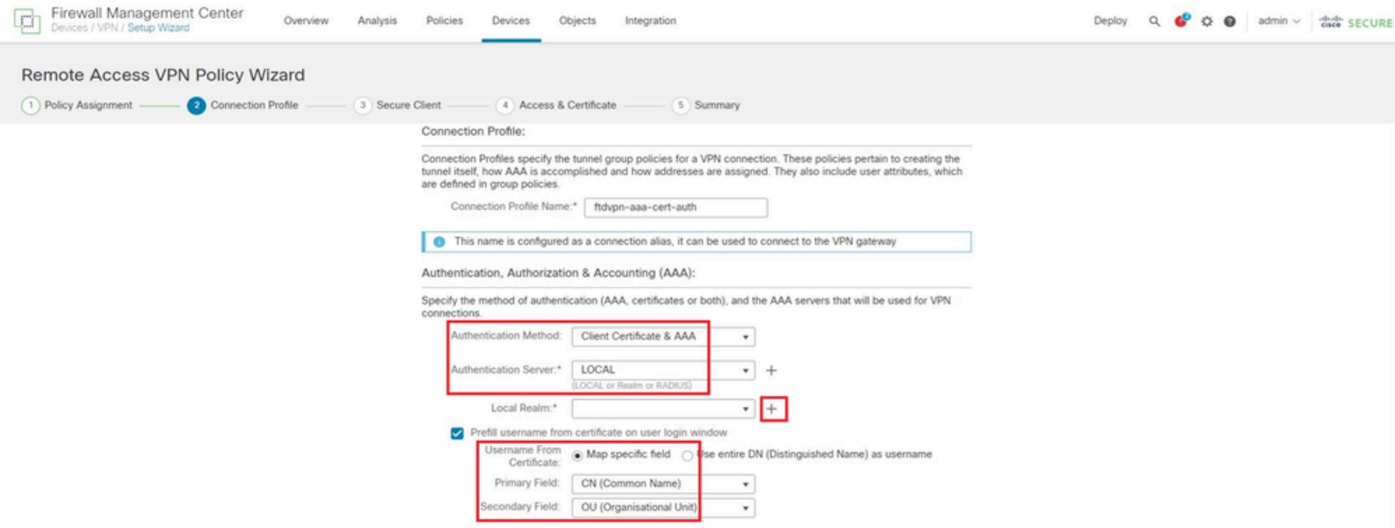
Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

Atribuição de política

Etapa 4. Detalhes da configuração do perfil de conexão

Insira as informações necessárias para o perfil de conexão e clique no botão + ao lado do item Território local.

- Método de Autenticação : Certificado do Cliente & AAA
- Servidor de autenticação : LOCAL
- Nome de Usuário do Certificado: Mapear campo específico
- Campo Primário : CN (Nome Comum)
- Campo Secundário: OU (Unidade Organizacional)



Remote Access VPN Policy Wizard

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:* ftdvpn-aaa-cert-auth

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 & AAA

Authentication Server:* LOCAL (LOCAL or Realm or RADIUS)

Local Realm:*

☑ Prefill username from certificate on user login window

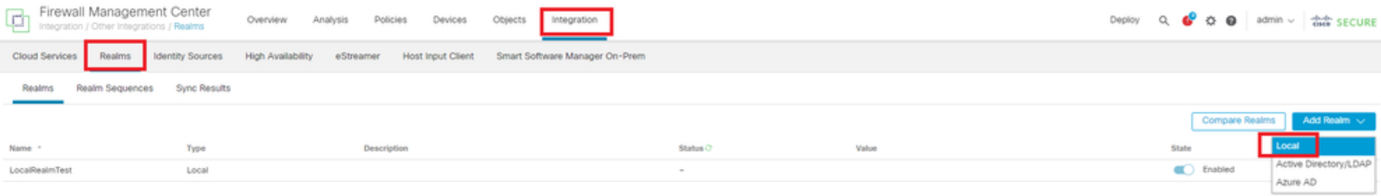
Username From Certificate: ● Map specific field ○ Use entire DN (Distinguished Name) as username

Primary Field: CN (Common Name)

Secondary Field: OU (Organisational Unit)

Detalhes do Perfil de Conexão

Clique em Local na lista suspensa Adicionar território para adicionar um novo território local.



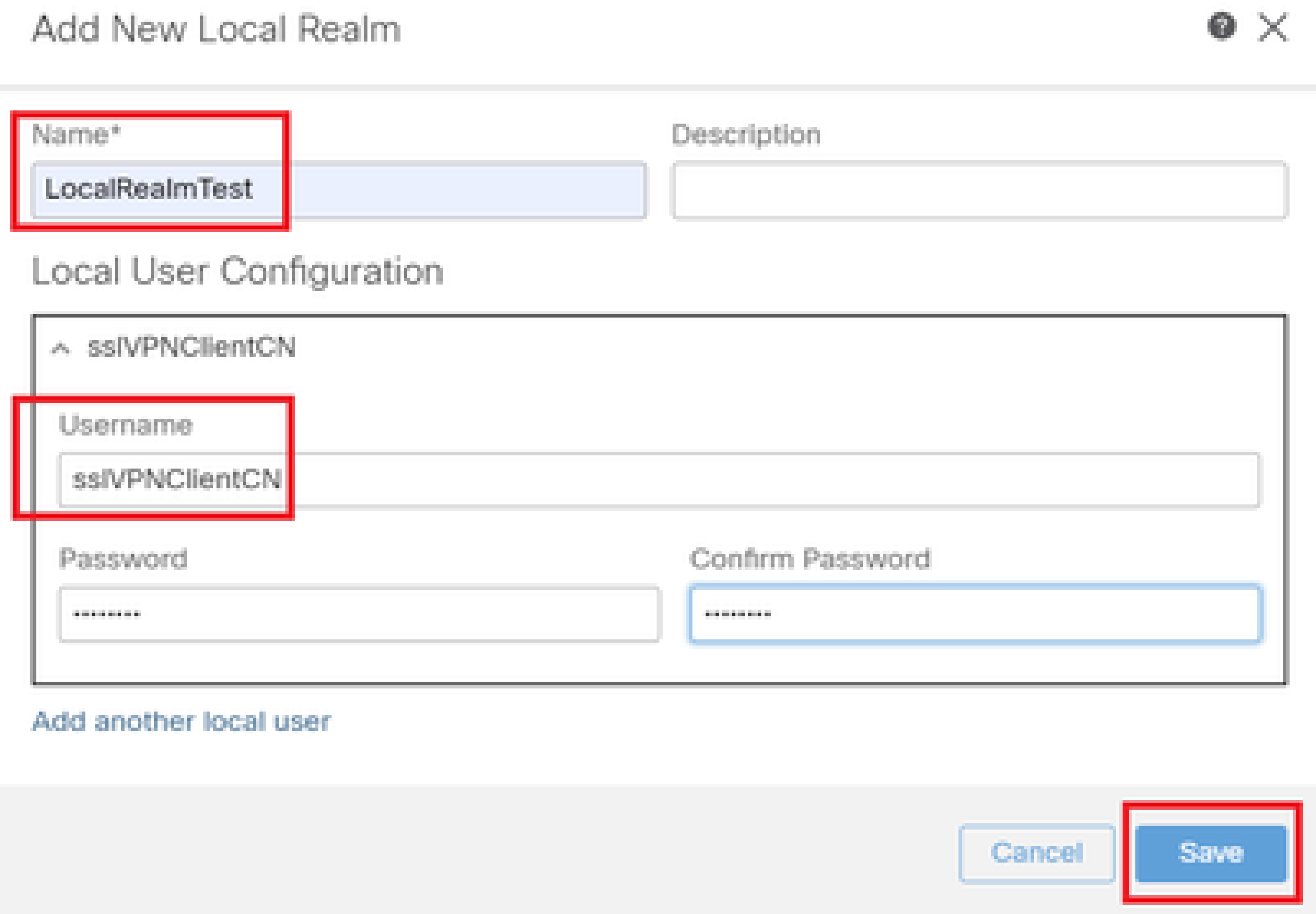
Name	Type	Description	Status	Value	State
LocalRealmTest	Local		-		Enabled

Adicionar território local

Insira as informações necessárias para o realm local e clique no botão Salvar.

- Nome : LocalRealmTest
- Nome de usuário : sslVPNClientCN

Observação: o nome de usuário é igual ao nome comum no certificado do cliente



Add New Local Realm

Name*: LocalRealmTest

Description:

Local User Configuration

sslVPNClientCN

Username: sslVPNClientCN

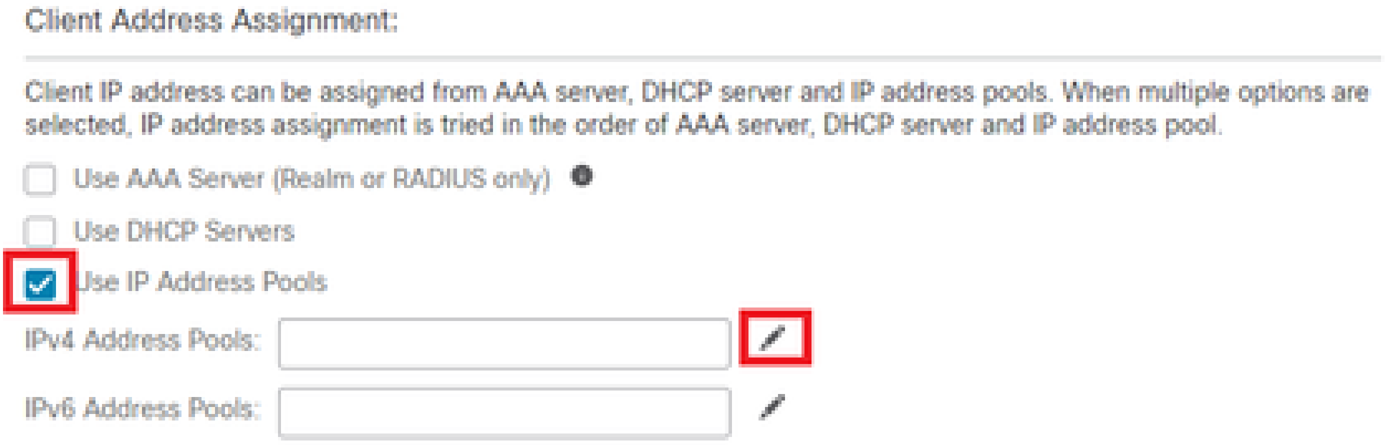
Password: ....

Confirm Password: ....

Detalhes do território local

Etapa 5. Adicionar Pool de Endereços para Perfil de Conexão

Clique no botão edit ao lado do item IPv4 Address Pools.



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:

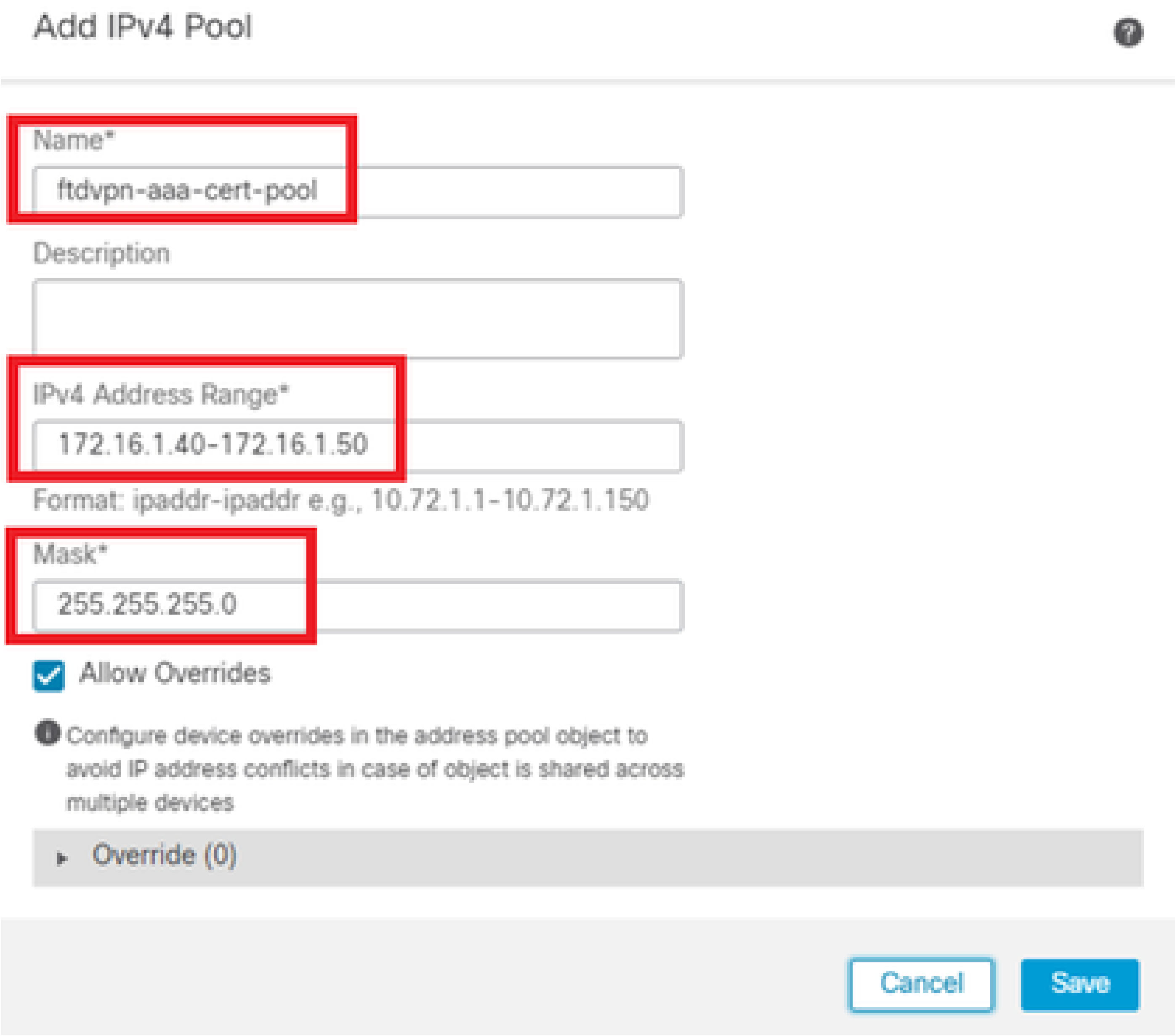
IPv6 Address Pools:

Adicionar Pool de Endereços IPv4

Insira as informações necessárias para adicionar um novo pool de endereços IPv4. Selecione o novo pool de endereços IPv4 para o perfil de conexão.

- Nome : ftdvpn-aaa-cert-pool
- Intervalo de Endereços IPv4 : 172.16.1.40-172.16.1.50

- Máscara : 255.255.255.0



Add IPv4 Pool

Name*
ftdvpn-aaa-cert-pool

Description

IPv4 Address Range*
172.16.1.40-172.16.1.50

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

Mask*
255.255.255.0

☑ Allow Overrides

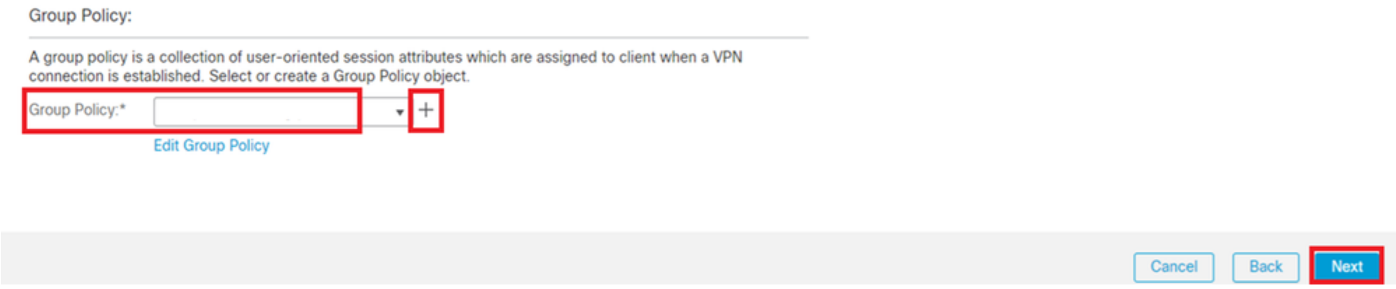
Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

▸ Override (0)

Detalhes do Pool de Endereços IPv4

Etapa 6. Adicionar Política de Grupo para Perfil de Conexão

Clique no botão + ao lado do item Diretiva de Grupo.



Group Policy:

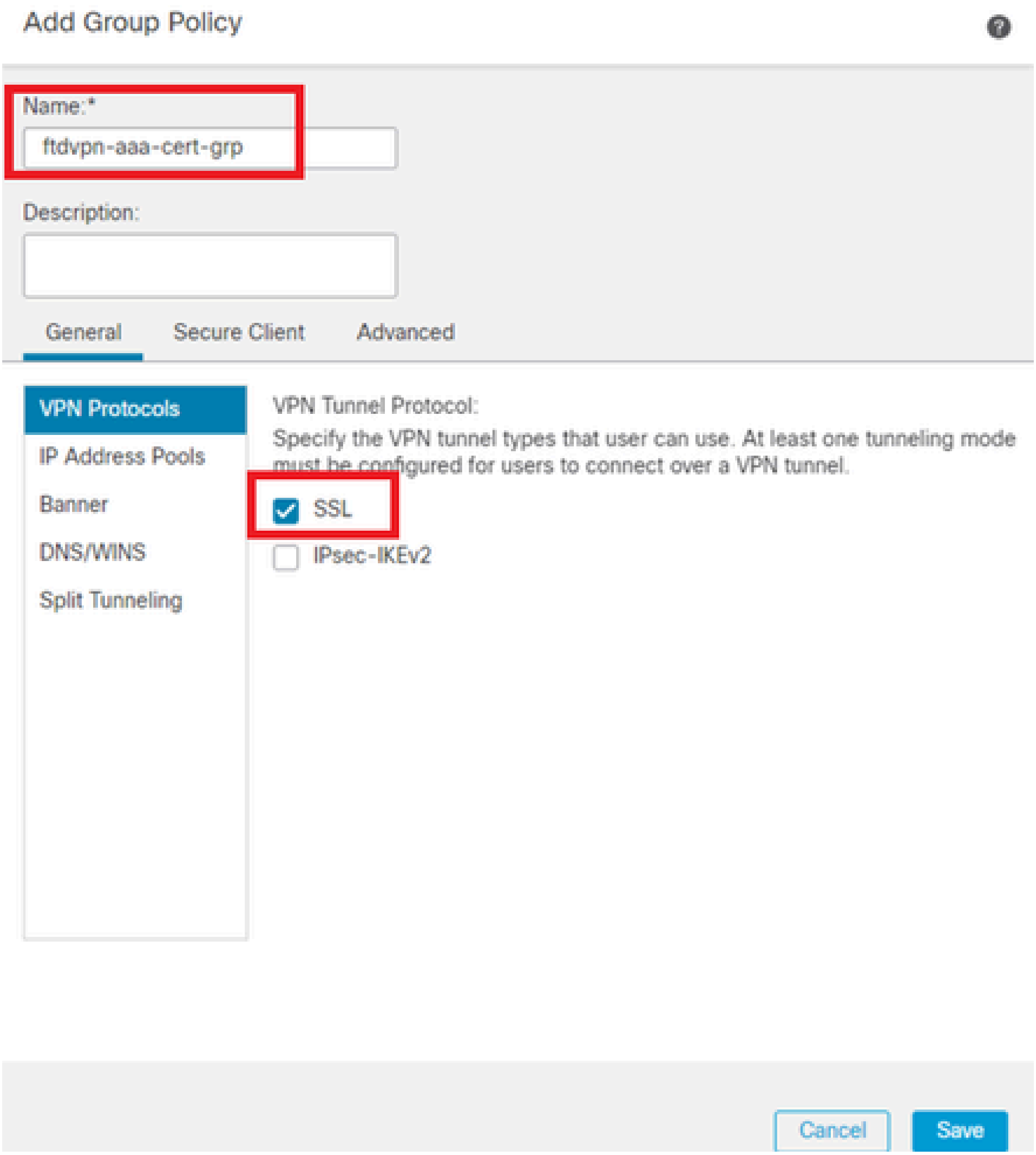
A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:*

Adicionar Política de Grupo

Insira as informações necessárias para adicionar uma nova política de grupo. Selecione a nova diretiva de grupo para o perfil de conexão.

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



Add Group Policy

Name:* ftdvpn-aaa-cert-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.

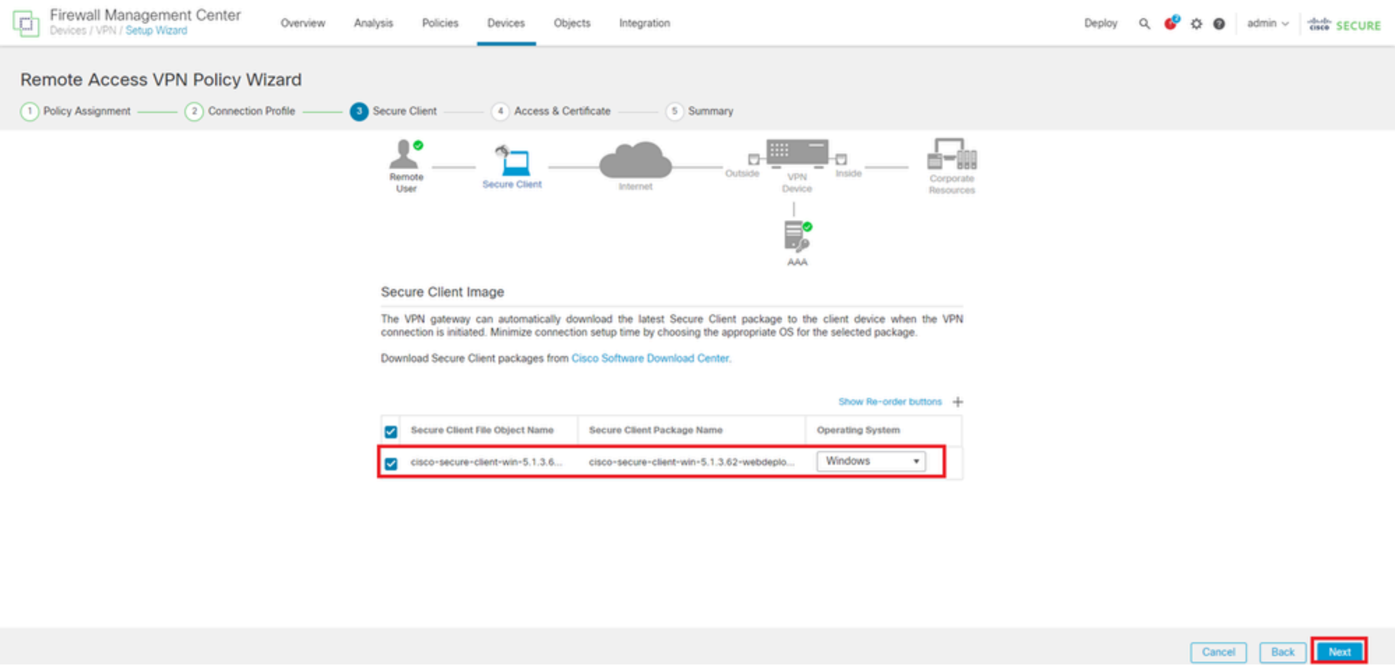
☑ SSL

□ IPsec-IKEv2

Detalhes da Política de Grupo

Passo 7. Config Secure Client Image para o perfil de conexão

Selecione o arquivo de imagem de cliente seguro e clique no botão Avançar.



Remote Access VPN Policy Wizard

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.

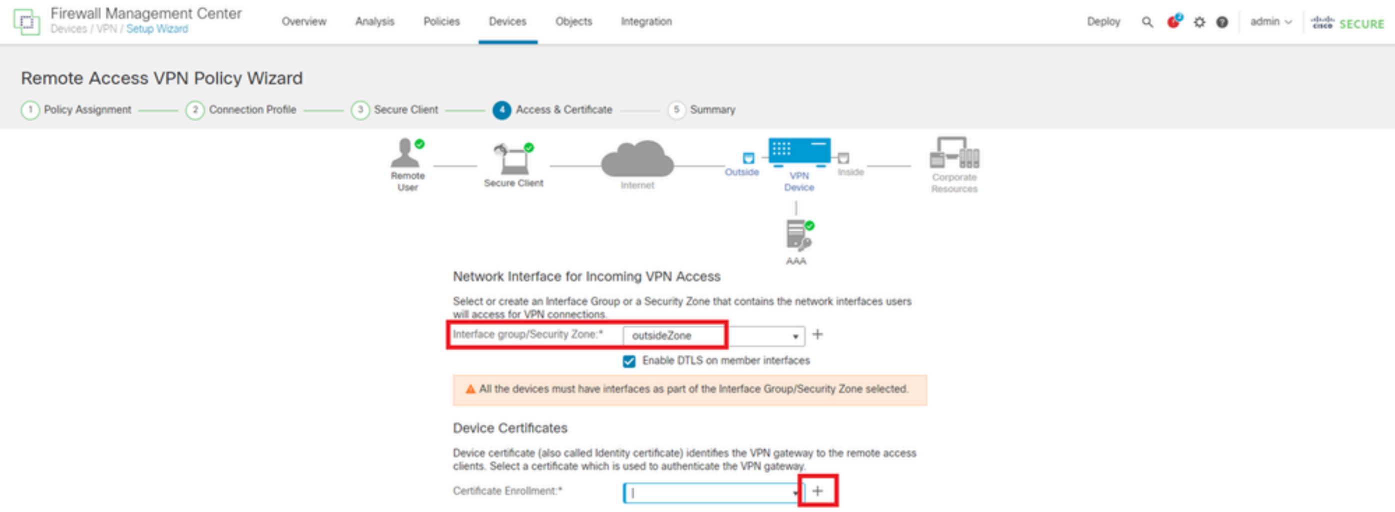
☑	Secure Client File Object Name	Secure Client Package Name	Operating System
☑	cisco-secure-client-win-5.1.3.6...	cisco-secure-client-win-5.1.3.62-webdeplo...	Windows ▾

Selecionar Imagem de Cliente Segura

Etapa 8. Acesso à configuração e certificado para o perfil de conexão

Selecione Security Zone para conexão VPN e clique no botão + ao lado do item Certificate Enrollment.

- Grupo de interface/Zona de segurança : outsideZone



Remote Access VPN Policy Wizard

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

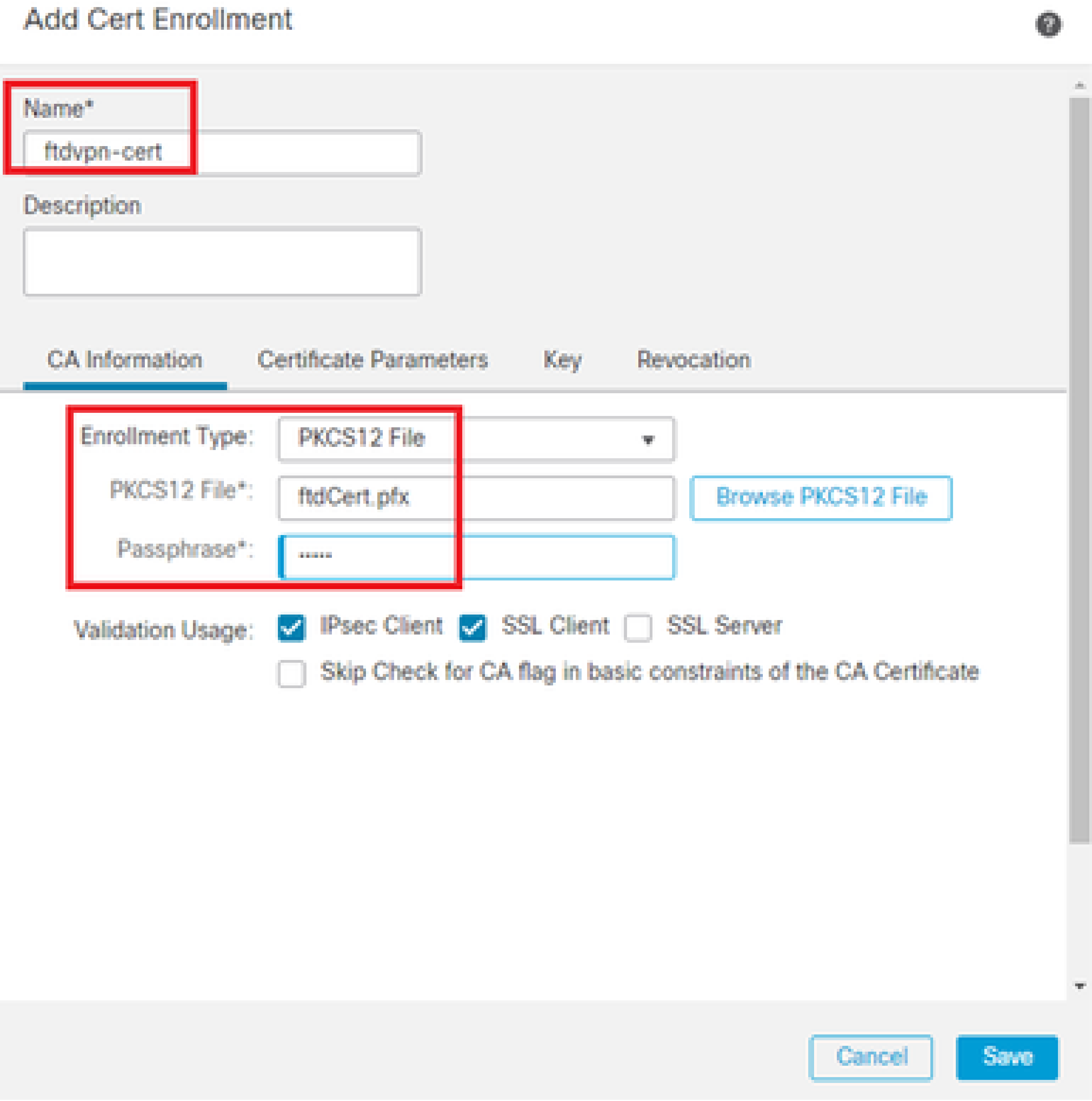
Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:*

Selecionar Zona de Segurança

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

- Nome : ftdvpn-cert
- Tipo de registro: arquivo PKCS12



Add Cert Enrollment

Name*

ftdvpn-cert

Description

Enrollment Type: PKCS12 File

PKCS12 File*: ftdCert.pfx

Passphrase*: ......

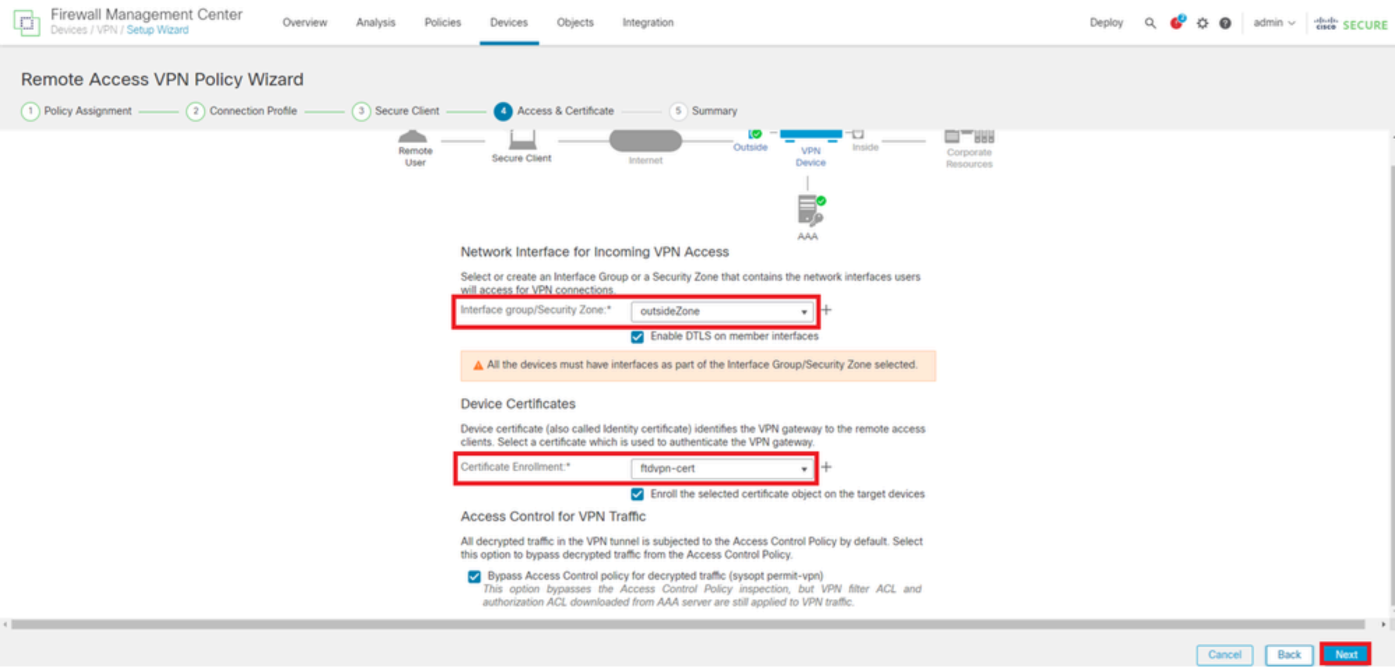
Validation Usage: ☑ IPsec Client ☑ SSL Client □ SSL Server

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

Adicionar Certificado FTD

Confirme as informações inseridas no assistente Access & Certificate e clique no botão Next.

Observação: habilite a política Bypass Access Control para tráfego descriptografado (sysopt permit-vpn), para que o tráfego VPN descriptografado não seja submetido à inspeção de política de controle de acesso.



Remote Access VPN Policy Wizard

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

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:* ftdvpn-cert

☑ Enroll the selected certificate object on the target devices

Access Control for VPN Traffic

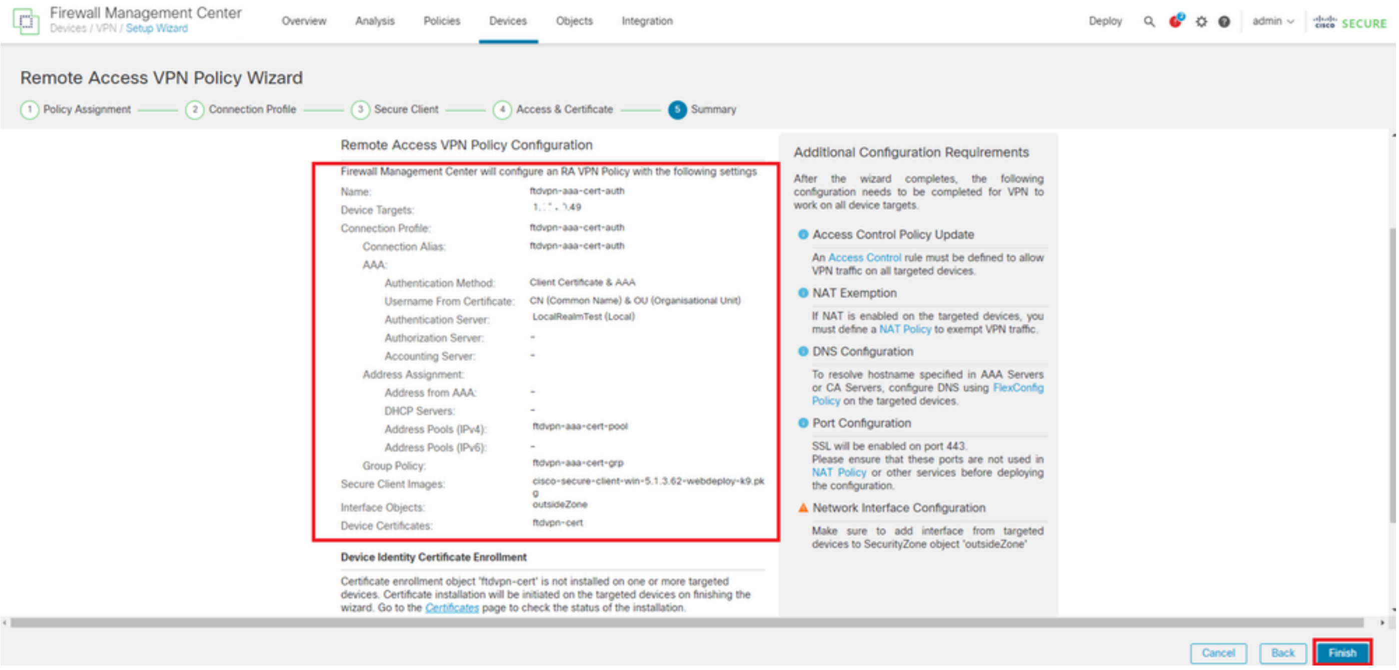
All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

☑ Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Confirmar configurações em Acesso e Certificado

Etapa 9. Confirmar resumo do perfil de conexão

Confirme as informações inseridas para a conexão VPN e clique no botão Finish.



Remote Access VPN Policy Wizard

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

Remote Access VPN Policy Configuration

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

```
Name:                              ftdvpn-aaa-cert-auth
Device Targets:                    1.[redacted].49
Connection Profile:                ftdvpn-aaa-cert-auth
    Connection Alias:              ftdvpn-aaa-cert-auth
    AAA:
        Authentication Method:     Client Certificate & AAA
        Username From Certificate: CN (Common Name) & OU (Organisational Unit)
        Authentication Server:     LocalRealmTest (Local)
        Authorization Server:      -
        Accounting Server:         -
    Address Assignment:
        Address from AAA:          -
        DHCP Servers:              -
        Address Pools (IPv4):      ftdvpn-aaa-cert-pool
        Address Pools (IPv6):      -
    Group Policy:                  ftdvpn-aaa-cert-grp
Secure Client Images:              cisco-secure-client-win-5.1.3.62-webdeploy-k9.pk
                                   g
Interface Objects:                 outsideZone
Device Certificates:               ftdvpn-cert
```

Device Identity Certificate Enrollment

Certificate enrollment object 'ftdvpn-cert' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the Certificates page to check the status of the installation.

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

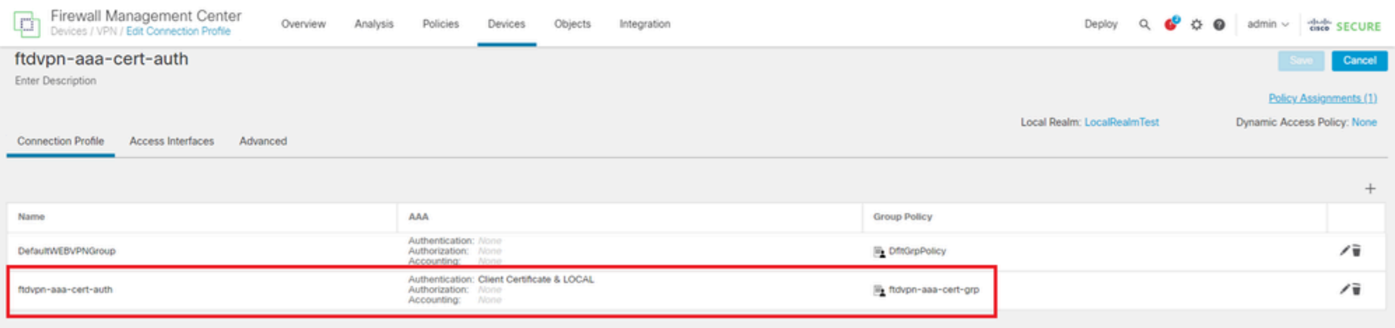
SSL will be enabled on port 443.
Please ensure that these ports are not used in NAT Policy or other services before deploying the configuration.

⚠ Network Interface Configuration

Make sure to add interface from targeted devices to SecurityZone object 'outsideZone'

Confirmar configurações para conexão VPN

Confirme o resumo da política de VPN de acesso remoto e implante as configurações no FTD.



ftdvpn-aaa-cert-auth

Enter Description

Local Realm: LocalRealmTest

Dynamic Access Policy: None

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
ftdvpn-aaa-cert-auth	Authentication: Client Certificate & LOCAL Authorization: None Accounting: None	ftdvpn-aaa-cert-grp

Resumo da Política de VPN de Acesso Remoto

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
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
```

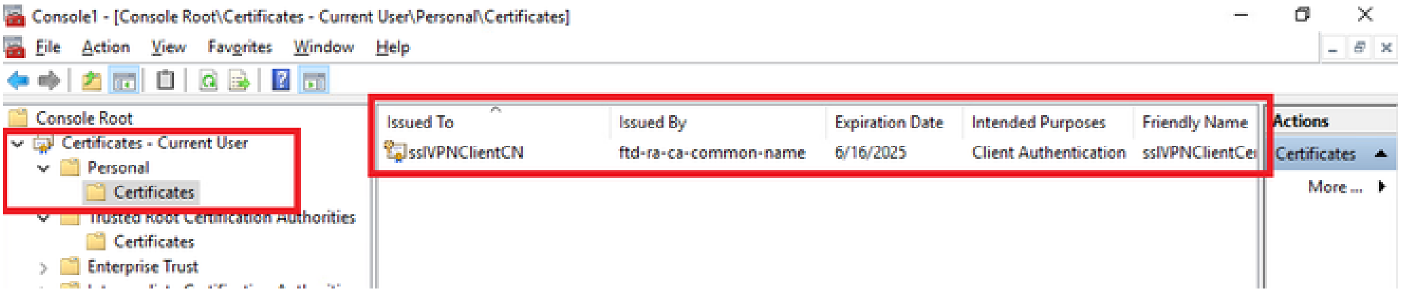
```
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// 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 no cliente VPN

Etapa 1. Confirmar certificado do cliente

Navegue até Certificates - Current User > Personal > Certificates, verifique o certificado do cliente usado para autenticação.

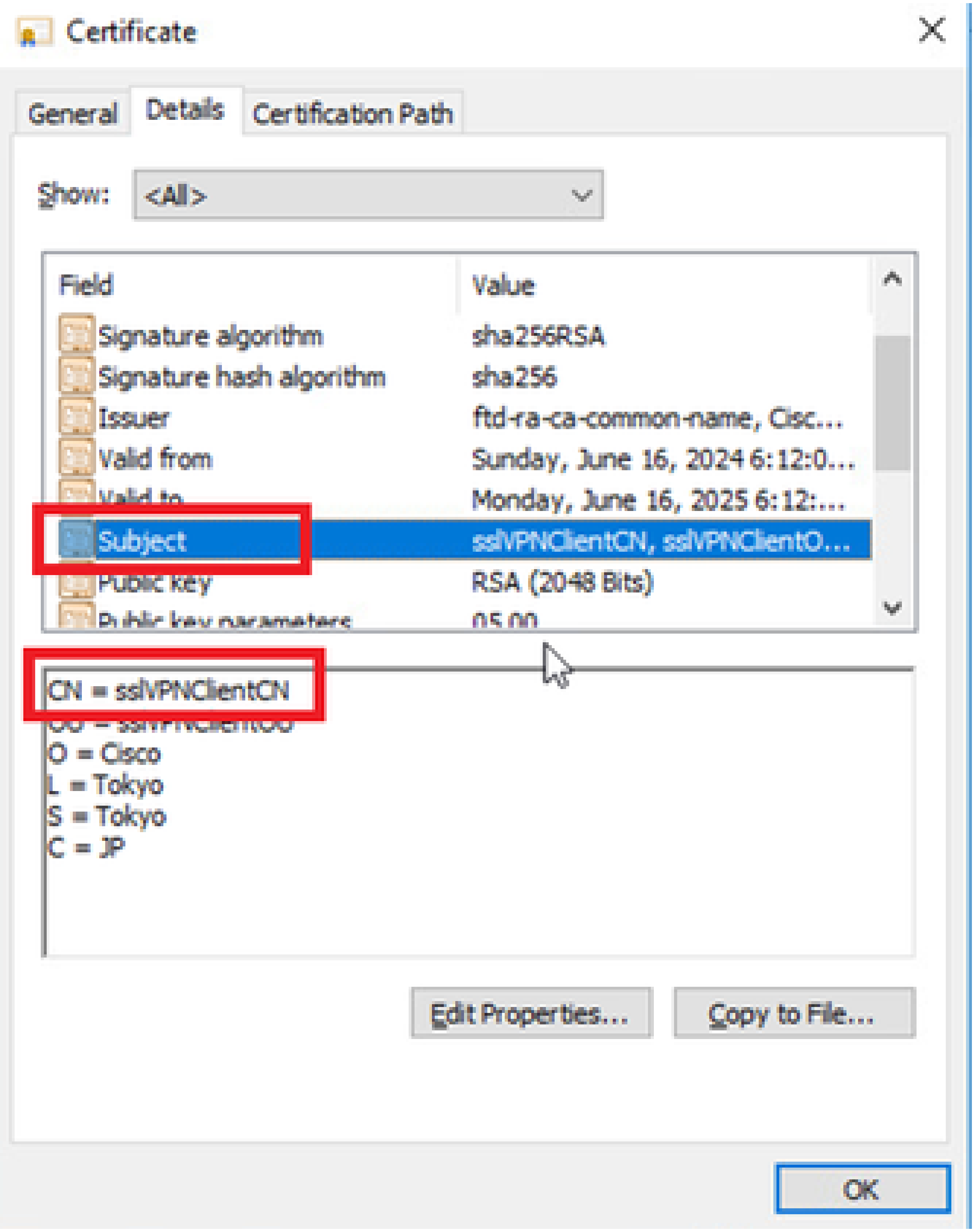

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Actions
Certificates
More ...

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
sslVPNClientCN	ftd-ra-ca-common-name	6/16/2025	Client Authentication	sslVPNClientCe

Confirmar certificado do cliente

Clique duas vezes no certificado do cliente, navegue para Detalhes, verifique os detalhes de Assunto.

- Assunto : CN = sslVPNClientCN



Show: <All>

Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ftd-ra-ca-common-name, Cisc...
Valid from	Sunday, June 16, 2024 6:12:0...
Valid to	Monday, June 16, 2025 6:12:...
Subject	sslVPNClientCN, sslVPNClientO...
Public key	RSA (2048 Bits)
Public key parameters	05 00

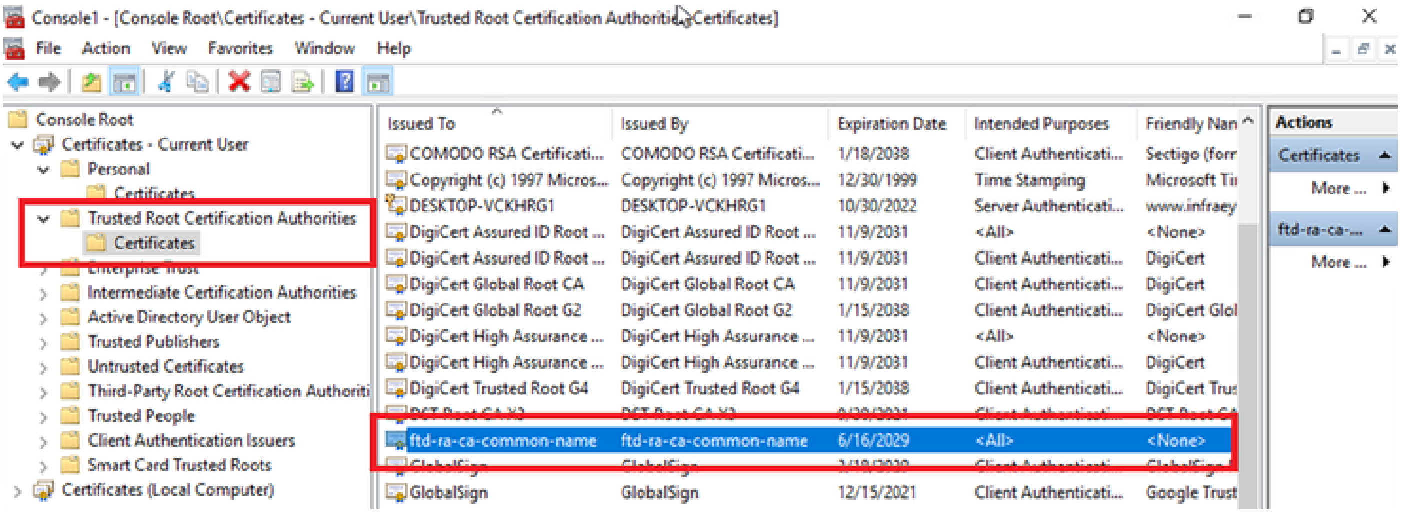
CN = sslVPNClientCN
OU = sslVPNClientOU
O = Cisco
L = Tokyo
S = Tokyo
C = JP

Detalhes do Certificado do Cliente

Etapa 2. Confirmar CA

Navegue até Certificates - 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
Certificates
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
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
GlobalSign	GlobalSign	12/15/2021	Client Authenticati...	Google Trust

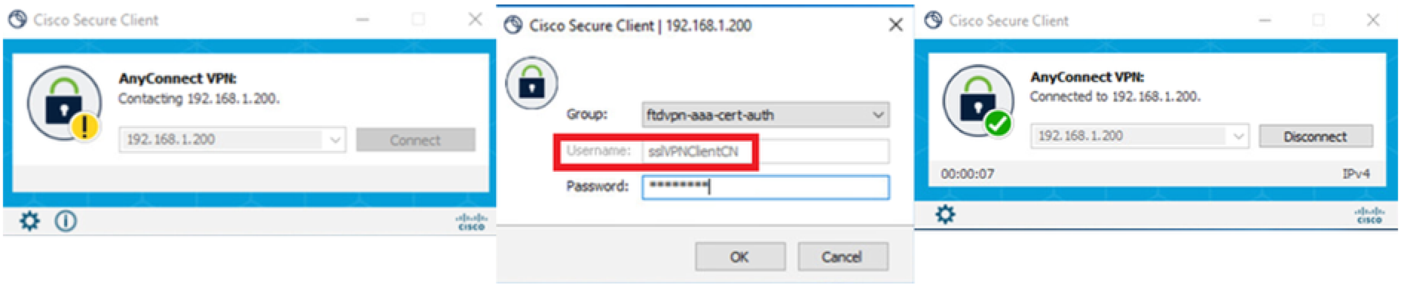
Confirmar CA

Verificar

Etapa 1. Iniciar conexão VPN

No endpoint, inicie a conexão do Cisco Secure Client. O nome de usuário é extraído do certificado do cliente, você precisa inserir a senha para autenticação VPN.

Observação: o nome de usuário é extraído do campo CN (Common Name) do certificado de cliente neste documento.



AnyConnect VPN: Contacting 192.168.1.200.

192.168.1.200

Group: ftdvpn-aaa-cert-auth

Username: sslVPNClientCN

Password: ********

AnyConnect VPN: Connected to 192.168.1.200.

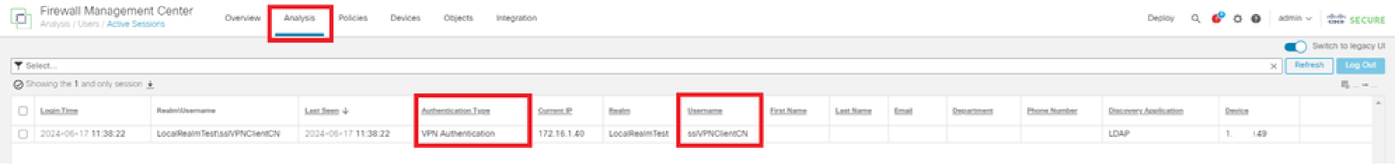
192.168.1.200

00:00:07 IPv4

Iniciar conexão VPN

Etapa 2. Confirmar sessões ativas no FMC

Navegue para Analysis > Users > Ative Sessions, verifique a sessão ativa para autenticação de VPN.



	Login Time	Realm\Username	Last Seen ↓	Authentication Type	Current IP	Realm	Username	First Name	Last Name	Email	Department	Phone Number	Discovery Application	Device
□	2024-06-17 11:38:22	LocalRealmTest\sslVPNClientCN	2024-06-17 11:38:22	VPN Authentication	172.16.1.40	LocalRealmTest	sslVPNClientCN						LDAP	1. .49

Confirmar sessão ativa

Etapa 3. Confirmar sessão VPN na CLI FTD

Executeshow vpn-sessiondb detail anyconnect o comando na CLI FTD (Lina) para confirmar a sessão VPN.

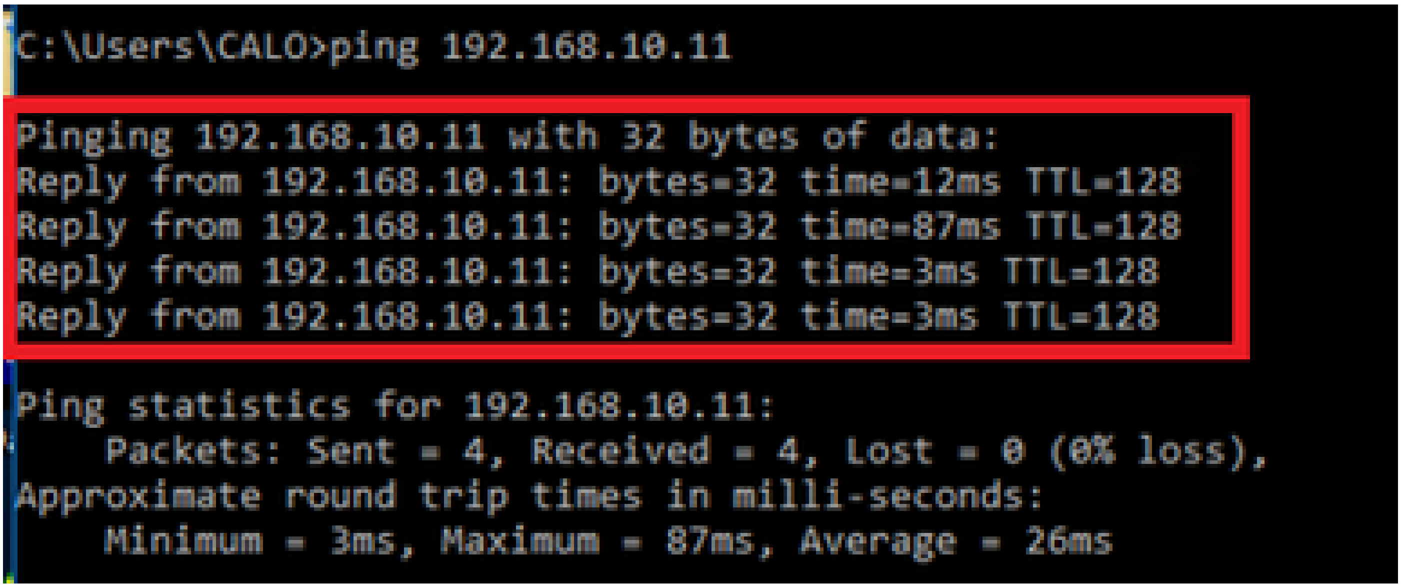
```
ftd702# show vpn-sessiondb detail anyconnect

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 : cb0071820000700066 6fa19e
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

Etapa 4. Confirmar comunicação com o servidor

Inicie o ping do cliente VPN para o servidor, confirme se a comunicação entre o cliente VPN e o servidor foi bem-sucedida.



```
C:\Users\CALO>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time=12ms TTL=128
Reply from 192.168.10.11: bytes=32 time=87ms TTL=128
Reply from 192.168.10.11: bytes=32 time=3ms TTL=128
Reply from 192.168.10.11: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 87ms, Average = 26ms
```

Ping bem-sucedido

Execute capture in interface inside real-time o comando na CLI do FTD (Lina) para confirmar a captura de pacotes.

<#root>

```
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
```

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.

```
// 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=sslVPNClientC

// 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
```

Essas depurações podem ser executadas a partir da CLI de diagnóstico do FTD, que fornece informações que você pode usar para solucionar problemas de configuração.

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

Referência

Configurar o AnyConnect Remote Access VPN no FTD

Configurar Autenticação Baseada em Certificado do Anyconnect para Acesso Móvel

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.