

Configurar Correspondência de Certificado para Autenticação de Cliente Seguro no FTD via FDM

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configuração no FDM](#)

[Etapa 1. Configurar a interface FTD](#)

[Etapa 2. Confirmar licença do Cisco Secure Client](#)

[Etapa 3. Adicionar Pool de Endereços](#)

[Etapa 4. Criar perfil de cliente seguro](#)

[Etapa 5. Carregar Perfil de Cliente Seguro no FDM](#)

[Etapa 6. Adicionar Política de Grupo](#)

[Passo 7. Adicionar Certificado FTD](#)

[Etapa 8. Adicionar CA ao FTD](#)

[Etapa 9. Adicionar Perfil de Conexão VPN de Acesso Remoto](#)

[Etapa 10. Confirmar resumo do perfil de conexão](#)

[Confirmar na CLI do FTD](#)

[Confirmar no cliente VPN](#)

[Etapa 1. Copie o perfil do cliente seguro para o cliente VPN](#)

[Etapa 2. Confirmar certificado do cliente](#)

[Etapa 3. Confirmar CA](#)

[Verificar](#)

[Etapa 1. Iniciar conexão VPN](#)

[Etapa 2. Confirmar sessões VPN na CLI FTD](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

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

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Firepower Device Manager (FDM) Virtual
- Firewall Threat Defense (FTD) Virtual
- Fluxo de autenticação de VPN

Componentes Utilizados

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

- Cisco Secure Client 5.1.4.74
- Editor de perfis (Windows) 5.1.4.74

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

CertificateMatch é um recurso que permite aos administradores configurar critérios que o cliente deve usar para selecionar um certificado de cliente para autenticação com o servidor VPN. Essa configuração é especificada no perfil do cliente, que é um arquivo XML que pode ser gerenciado usando o Editor de perfis ou editado manualmente. O recurso CertificateMatch pode ser usado para melhorar a segurança das conexões VPN, garantindo que apenas um certificado com atributos específicos seja usado para a conexão VPN.

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.

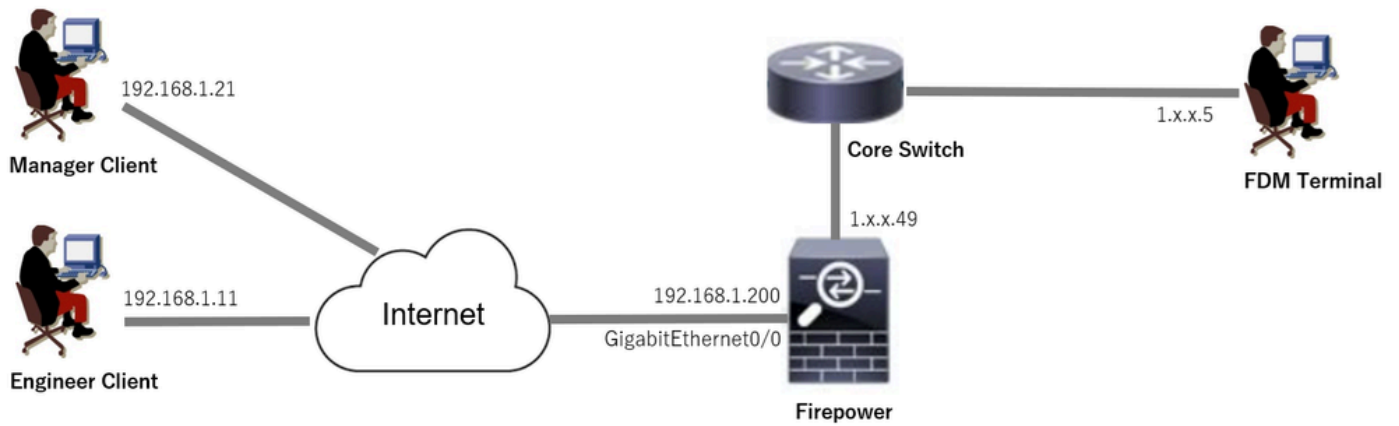


Diagrama de Rede

Configurações

Configuração no FDM

Etapa 1. Configurar a interface FTD

Navegue até Device > Interfaces > View All Interfaces, configure a interface interna e externa para FTD na guia Interfaces.

Para GigabitEthernet0/0,

- Nome: externo
- Endereço IP: 192.168.1.200/24

Device Summary
Interfaces

Cisco Firepower Threat Defense for VMware

0/0 0/1 0/2 0/3 0/4 0/5 0/6 0/7

MGMT
CONSOLE

Interfaces Virtual Tunnel Interfaces

9 Interfaces

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> ✓ GigabitEthernet0/0	outside	Enabled	Routed	192.168.1.200/24		Enabled	

Interface FTD

Etapa 2. Confirmar licença do Cisco Secure Client

Navegue até Device > Smart License > View Configuration, confirme a licença do Cisco Secure Client no item RA VPN License.

Firewall Device Manager | Monitoring | Policies | Objects | Device: firepower

admin Administrator | CISCO SECURE

SUBSCRIPTION LICENSES INCLUDED

Threat [ENABLE]
Disabled by user
This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.
Includes: Intrusion Policy

Malware [ENABLE]
Disabled by user
This license lets you perform malware defense. You must have this license to apply file policies that detect and block malware in files transmitted over your network.
Includes: File Policy

URL License [ENABLE]
Disabled by user
This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.
Includes: URL Reputation

RA VPN License Type: VPN ONLY [DISABLE]
Enabled
Please select the license type that you purchased to enable remote access VPN. Note that Secure Firewall device manager does not support any of the advanced features covered by the Apex license.
Includes: RA-VPN

Licença de cliente seguro

Etapa 3. Adicionar Pool de Endereços

Navegue até Objetos > Redes, clique no botão +.

Firewall Device Manager | Monitoring | Policies | Objects | Device: firepower

admin Administrator | CISCO SECURE

Object Types | Networks | Ports | Security Zones | Application Filters

Network Objects and Groups

7 objects

Filter [+]
Preset filters: System defined, User defined

#	NAME	TYPE	VALUE	ACTIONS
1	IPv4-Private-10.0.0.0-8	NETWORK	10.0.0.0/8	

Adicionar Pool de Endereços

Insira as informações necessárias para adicionar um novo pool de endereços IPv4. clique no botão OK.

- Nome: ftd-cert-match-pool
- Tipo: Intervalo
- Intervalo de IPs: 172.16.1.150-172.16.1.160

Add Network Object



Name

ftd-cert-match-pool

Description

Type



Network



Host



FQDN



Range

IP Range

172.16.1.150-172.16.1.160

e.g. 192.168.2.1-192.168.2.24 or 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100

CANCEL

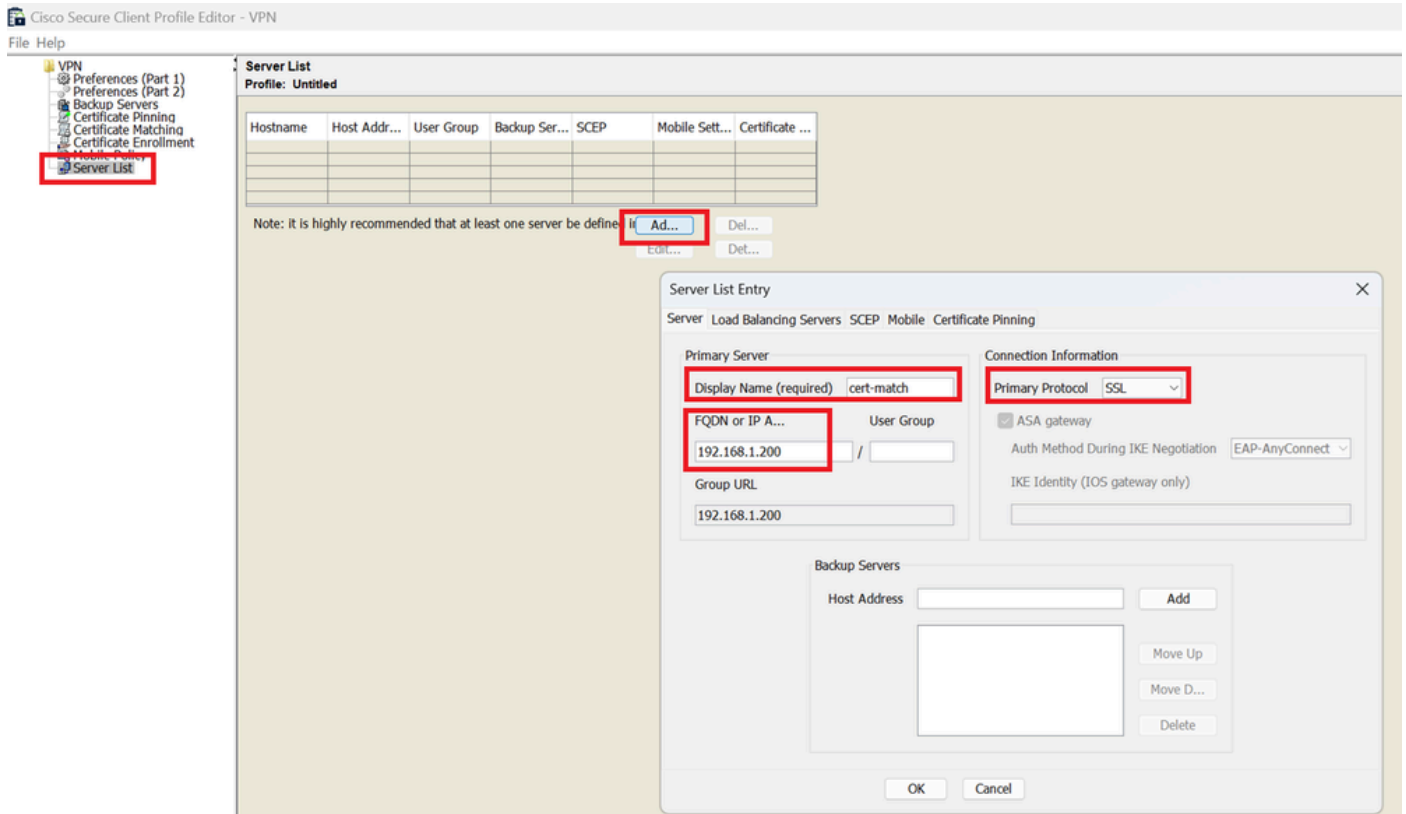
OK

Detalhes do pool de endereços IPv4

Etapa 4. Criar perfil de cliente seguro

Faça o download e instale o Secure Client Profile Editor do [site](#) do [Cisco Software](#). Navegue até Lista de servidores, clique no botão Adicionar. Insira as informações necessárias para adicionar uma Entrada da lista de servidores e clique no botão OK.

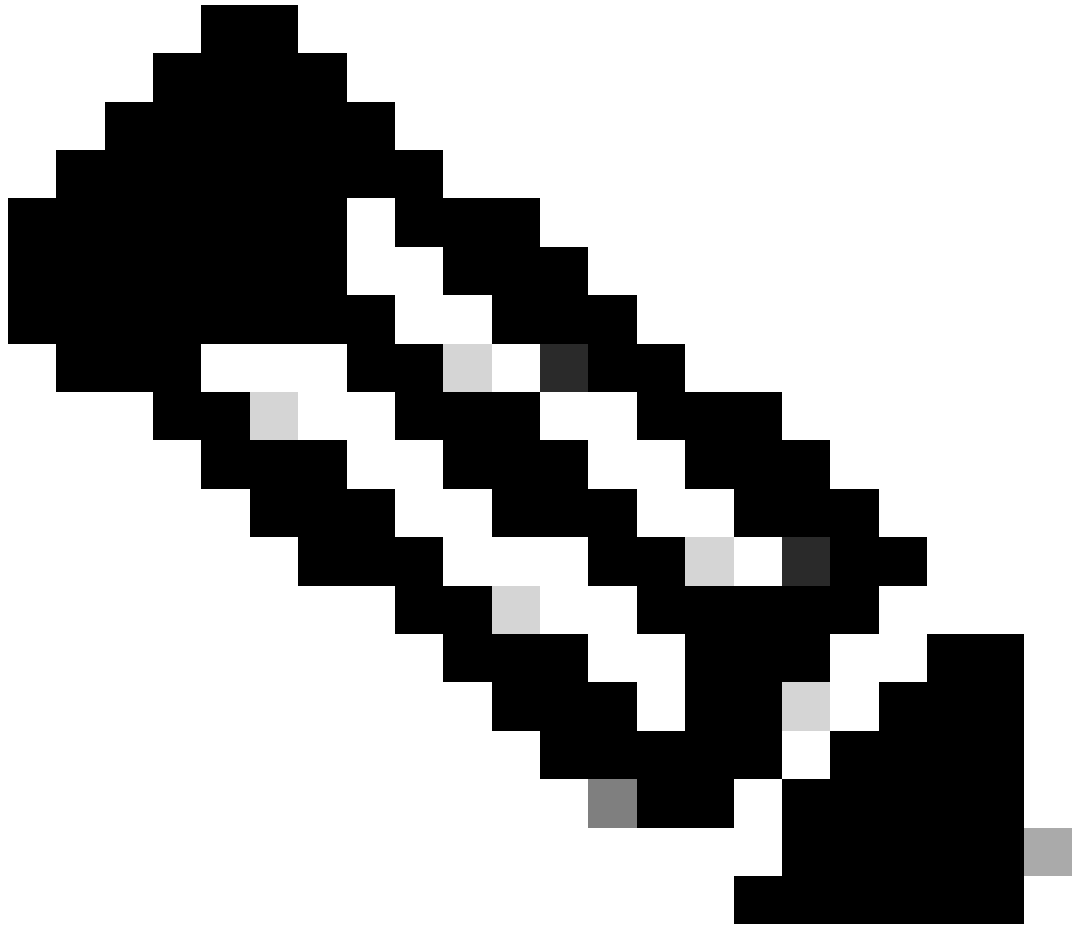
- Nome para Exibição: cert-match
- FQDN ou endereço IP: 192.168.1.200
- Protocolo principal: SSL



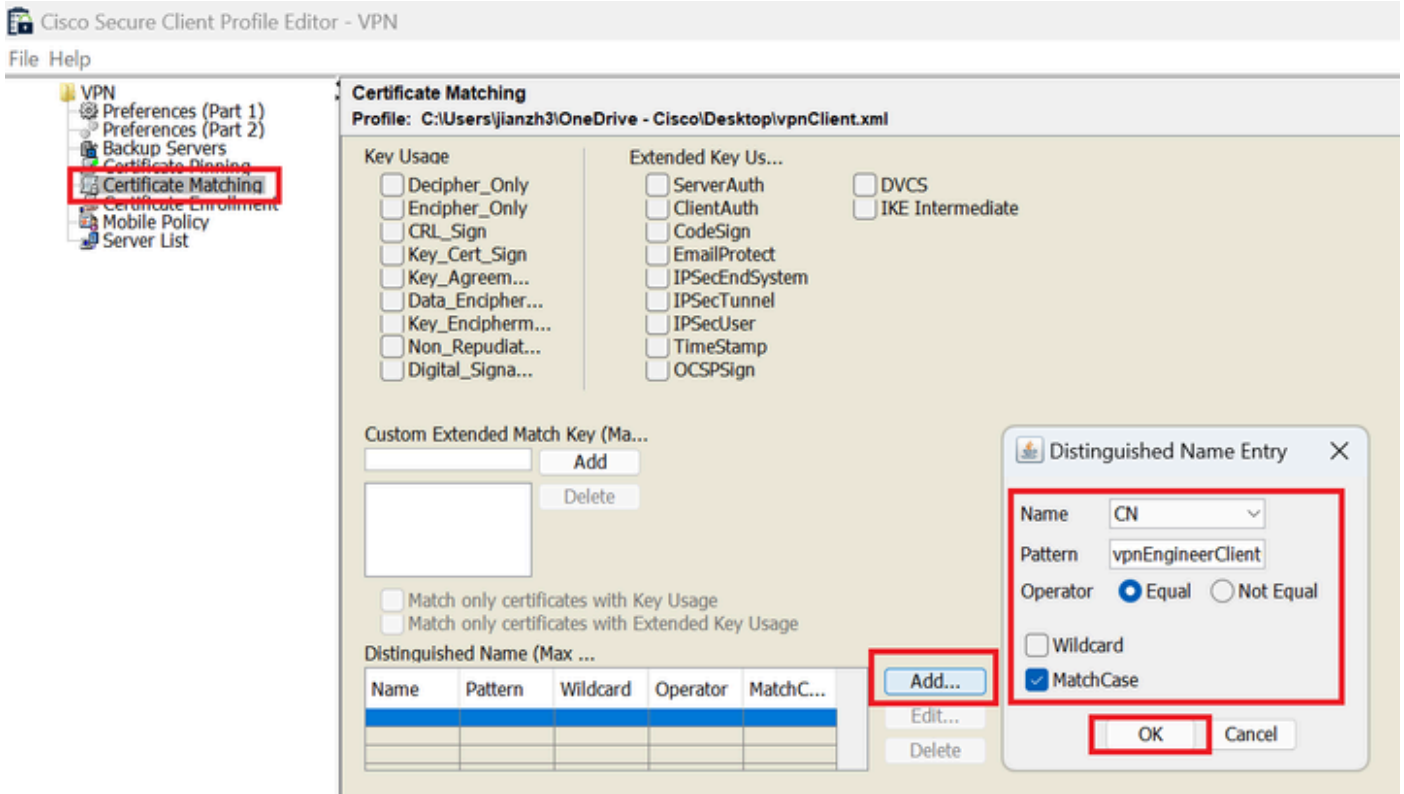
Entrada da Lista de Servidores

Navegue até Correspondência de Certificado, clique no botão Adicionar. Insira as informações necessárias para adicionar uma entrada de nome distinto e clique no botão OK.

- Nome: CN
- Padrão: vpnEngineerClientCN
- Operador: Igual



Observação: marque a opção MatchCase neste documento.



Entrada de Nome Distinto

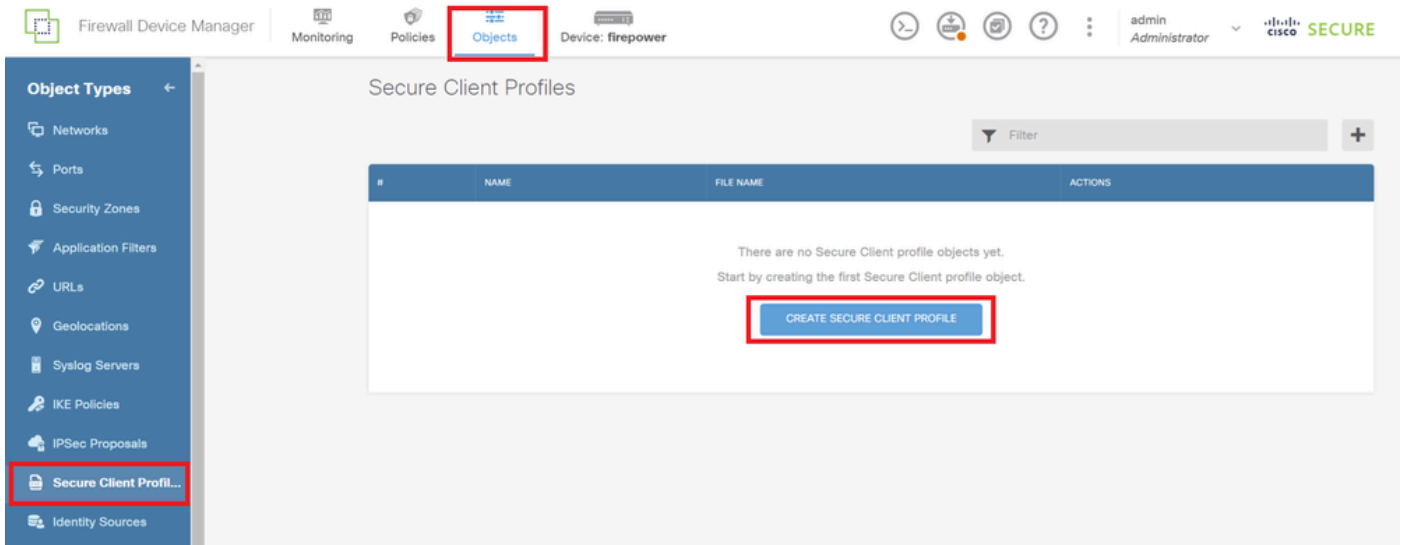
Salve o perfil de cliente seguro no computador local e confirme os detalhes do perfil.



Perfil de cliente seguro

Etapa 5. Carregar Perfil de Cliente Seguro no FDM

Navegue até Objects > Secure Client Profile, clique no botão CREATE SECURE CLIENT PROFILE.



Criar perfil de cliente seguro

Insira as informações necessárias para adicionar um perfil de cliente seguro e clique no botão OK.

- Nome: secureClientProfile
- Perfil de Cliente Seguro: secureClientProfile.xml (carregar do computador local)

Add Secure Client Profile

Name

secureClientProfile

Description

Secure Client Profile

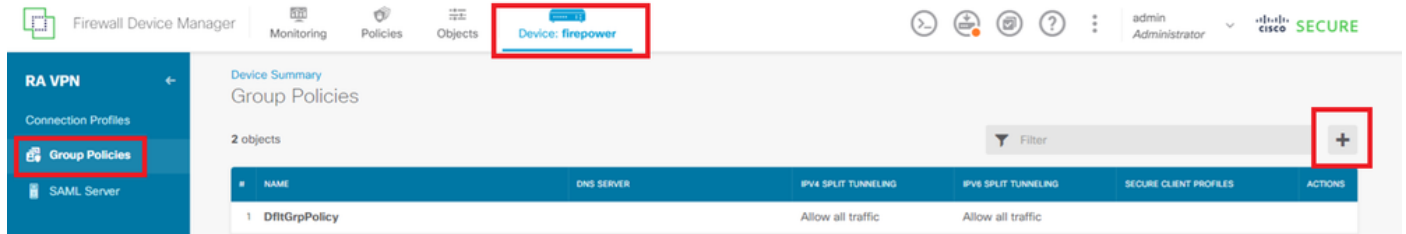
UPLOAD secureClientProfile.xml

CANCEL OK

Adicionar perfil de cliente seguro

Etapa 6. Adicionar Política de Grupo

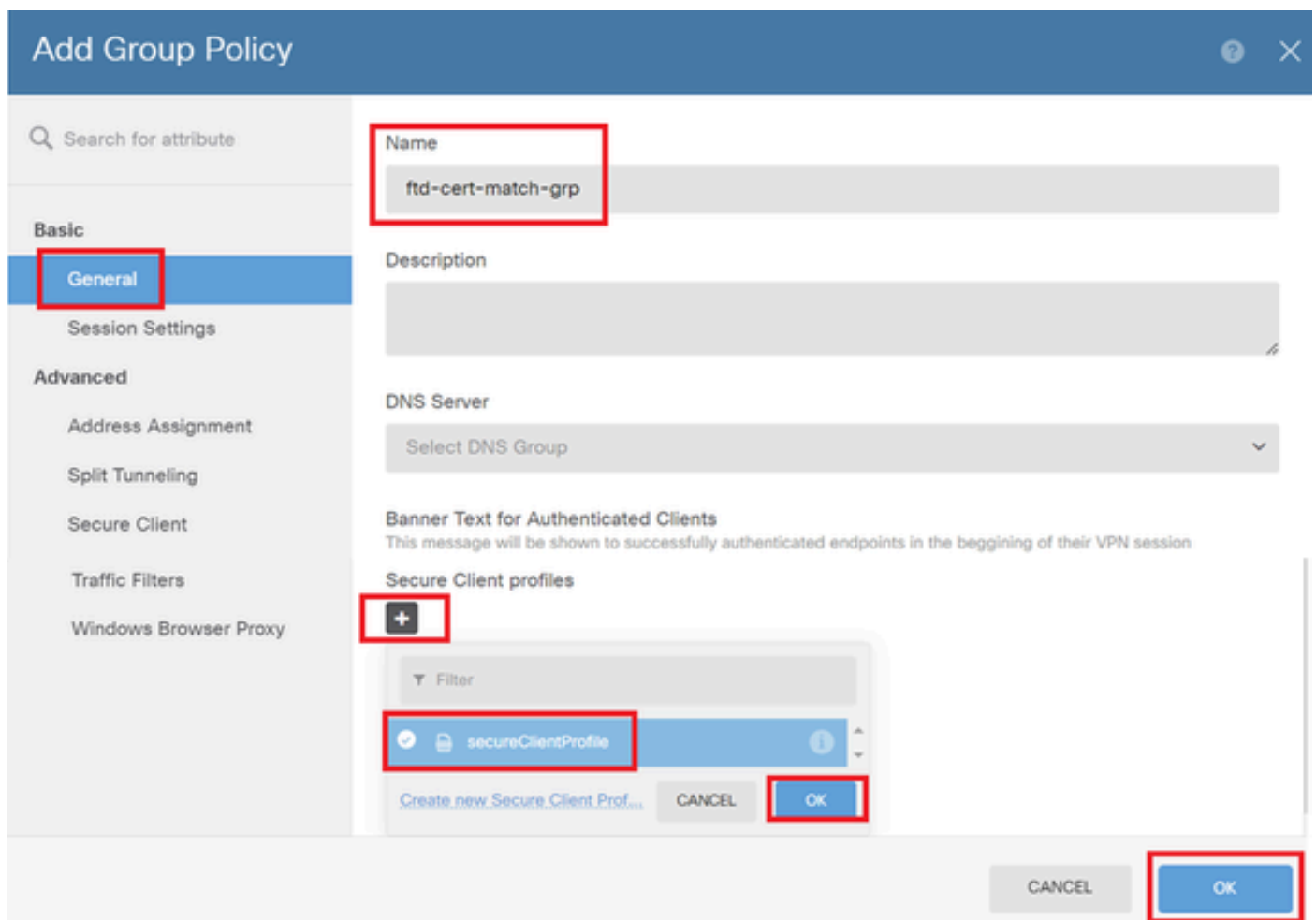
Navegue até Device > Remote Access VPN > View Configuration > Group Policies e clique no botão +.



Adicionar Política de Grupo

Insira as informações necessárias para adicionar uma política de grupo e clique no botão OK.

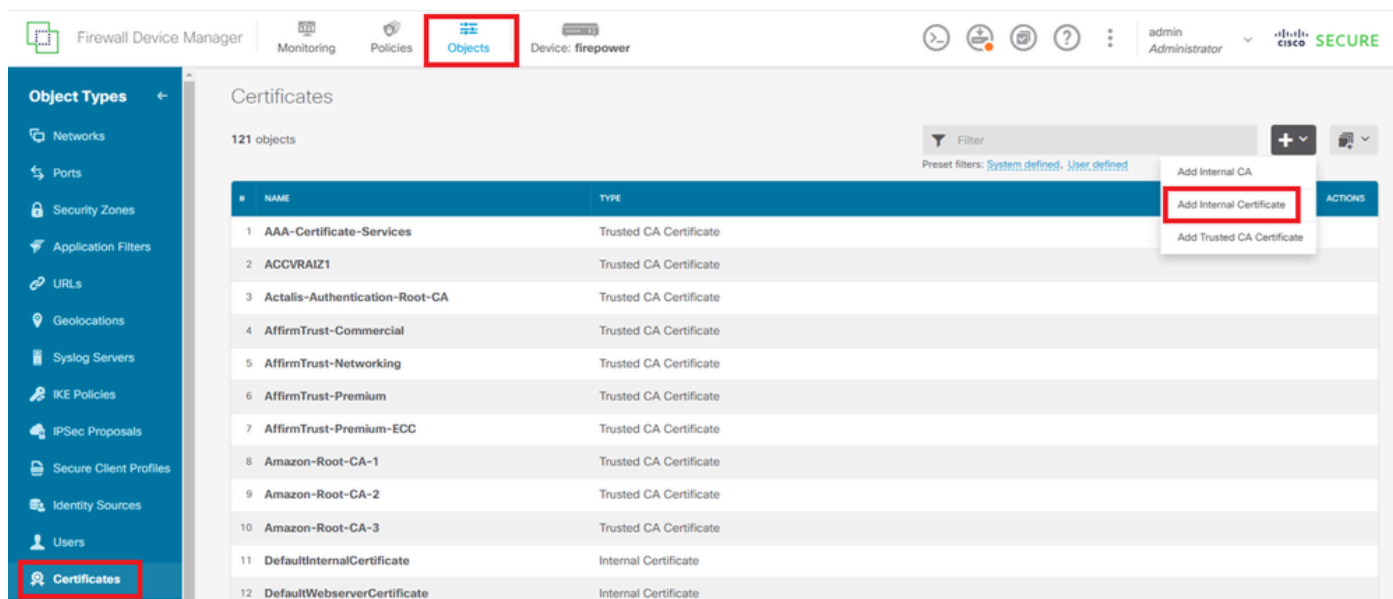
- Nome: ftd-cert-match-grp
- Perfis de cliente seguro: secureClientProfile



Detalhes da Política de Grupo

Passo 7. Adicionar Certificado FTD

Navegue até Objetos > Certificados, clique em Adicionar certificado interno do item +.



Firewall Device Manager | Monitoring | Policies | **Objects** | Device: firepower | admin Administrator | cisco SECURE

Object Types | Certificates

121 objects

#	NAME	TYPE	ACTIONS
1	AAA-Certificate-Services	Trusted CA Certificate	
2	ACCVRAIZ1	Trusted CA Certificate	
3	Actalis-Authentication-Root-CA	Trusted CA Certificate	
4	AffirmTrust-Commercial	Trusted CA Certificate	
5	AffirmTrust-Networking	Trusted CA Certificate	
6	AffirmTrust-Premium	Trusted CA Certificate	
7	AffirmTrust-Premium-ECC	Trusted CA Certificate	
8	Amazon-Root-CA-1	Trusted CA Certificate	
9	Amazon-Root-CA-2	Trusted CA Certificate	
10	Amazon-Root-CA-3	Trusted CA Certificate	
11	DefaultInternalCertificate	Internal Certificate	
12	DefaultWebserverCertificate	Internal Certificate	

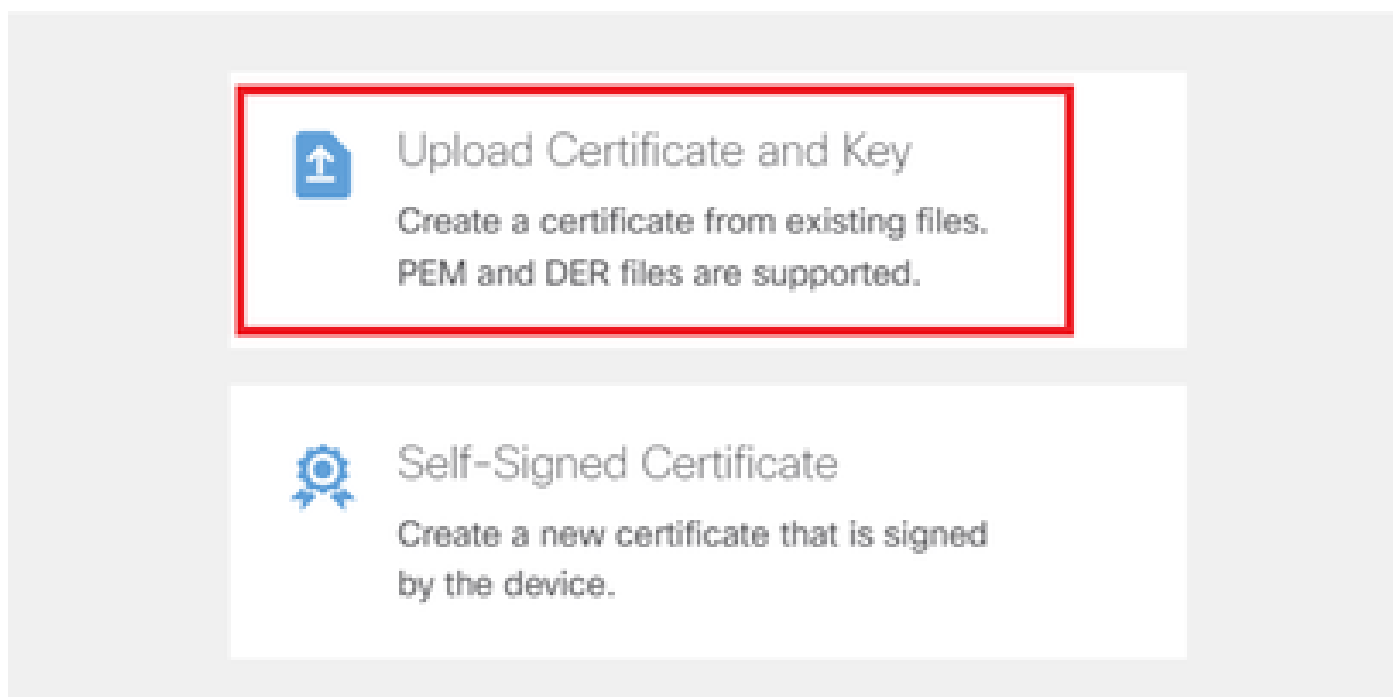
Filter | Preset filters: System defined, User defined

Actions: Add Internal CA, **Add Internal Certificate**, Add Trusted CA Certificate

Adicionar certificado interno

Clique em Carregar certificado e chave.

Choose the type of internal certificate you want to create



Upload Certificate and Key
Create a certificate from existing files.
PEM and DER files are supported.

Self-Signed Certificate
Create a new certificate that is signed by the device.

Carregar certificado e chave

Insira as informações necessárias para o certificado FTD, importe um certificado e uma chave de certificado do computador local e clique no botão OK.

- Nome: ftd-vpn-cert
- Uso da validação para serviços especiais: servidor SSL

Add Internal Certificate

Name

ftd-vpn-cert

Certificate

Paste certificate, or choose a file (DER, PEM, CRT, CER)

[Upload Certificate](#)

```
-----BEGIN CERTIFICATE-----
MIIDfDCCAmSgAwIBAgIIIkE99YS2cmwDQYJKoZIhvcNAQELBQAwTELMAkGA1UE
BhMCS1AxOjAjAMBgNVBAGTBVRva31vMQ4wDAYDVQQHEwVUB2t5bzEOMAwGA1UE
ChMF
O31-V38-w04AMP-4BDA-TB18k-z78k-MQ4-UAYV8Q9CE-ufA-dC9t-zwE+V3E+V30+KLD...
```

Certificate Key

Paste certificate key, or choose a file (KEY, PEM)

[Upload Certificate Key](#)

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAxdn5eTUngo5+GUG2Ng2FjI/+xHRkR-rf6o2OccGdzLYK1tzwB
98WPu1YP0T/qwCfFKXuMQ9DEVGMIjLRX9nvXdBNoakUbZVzc03qM3AjE87p0h0t0
+42b188PT-0u41-1-1-003-uf-+V6E0+1u4140-73E-7hK0-0M/7h0-774-0+V6-0F
```

Validation Usage for Special Services

SSL Server

CANCEL OK

Detalhes do certificado interno

Etapa 8. Adicionar CA ao FTD

Navegue até Objetos > Certificados, clique em Adicionar certificado CA confiável do item +.

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: firepower | admin Administrator | CISCO SECURE

Application Filters | URLs | Geolocations | Syslog Servers | IKE Policies | IPsec Proposals | Secure Client Profiles | Identity Sources | Users | **Certificates** | Secret Keys

Certificates

120 objects

#	NAME	TYPE	ACTIONS
1	NGFW-Default-InternalCA	Internal CA	Add Internal CA Add Internal Certificate Add Trusted CA Certificate
2	AAA-Certificate-Services	Trusted CA Certificate	
3	ACCVRAIZ1	Trusted CA Certificate	
4	Actalis-Authentication-Root-CA	Trusted CA Certificate	
5	AffirmTrust-Commercial	Trusted CA Certificate	
6	AffirmTrust-Networking	Trusted CA Certificate	
7	AffirmTrust-Premium	Trusted CA Certificate	

Adicionar Certificado CA Confiável

Insira as informações necessárias para a CA e importe um certificado do computador local.

- Nome: ftdvpn-ca-cert
- Uso de Validação para Serviços Especiais: Cliente SSL

Add Trusted CA Certificate

Name:

Certificate: [Upload Certificate](#)

Paste certificate, or choose a file (DER, PEM, CRT, CER)

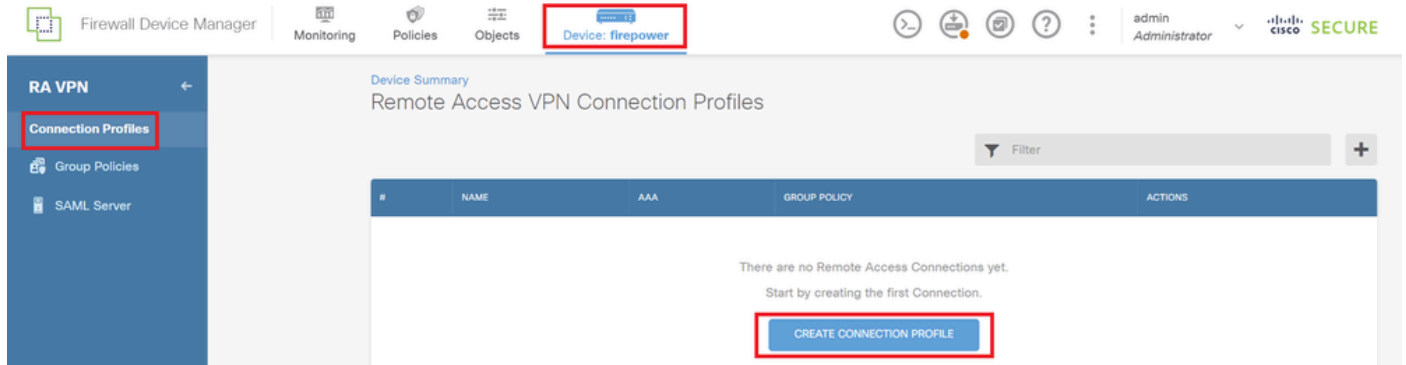
```
-----BEGIN CERTIFICATE-----
MIIDbDCCA1SgAwIBAgIIUkKgLG229/0wDQYJKoZIhvcNAQELBQAwbTELMAkGA1UE
BHMCS1AxDjAMBgNVBAgTBVRva31vMQ4wDAYDQgQEwVUub2t5bzEOMAwGA1UEChMF
O31-V38-wD4AMBgNVBAgTBVRva31vMQ4wDAYDQgQEwVUub2t5bzEOMAwGA1UEChMF
-----
```

Skip CA Certificate Check ⓘ

Validation Usage for Special Services:

Etapa 9. Adicionar Perfil de Conexão VPN de Acesso Remoto

Navegue até Device > Remote Access VPN > View Configuration > Connection Profiles, clique no botão CREATE CONNECTION PROFILE.



Adicionar Perfil de Conexão VPN de Acesso Remoto

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

- Nome do perfil de conexão: ftd-cert-match-vpn
- Tipo 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-cert-match-pool

Remote Access VPN | 1 Connection and Client Configuration | 2 Remote User Experience | 3 Global Settings | 4 Summary



Connection and Client Configuration

Specify how to authenticate remote users and the secure clients they can use to connect to the inside network.

Connection Profile Name

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

ftd-cert-match-vpn

Group Alias (one per line, up to 5)

ftd-cert-match-vpn

Group URL (one per line, up to 5)

Primary Identity Source

Authentication Type

Client Certificate Only

Username from Certificate

Map Specific Field

Primary Field: CN (Common Name) | Secondary Field: OU (Organisational Unit)

Use entire DN (distinguished name) as username

Advanced

Authorization Server

Please select

Accounting Server

Please select

Client Address Pool Assignment

IPv4 Address Pool

Endpoints are provided an address from this pool

ftd-cert-match-pool

IPv6 Address Pool

Endpoints are provided an address from this pool

+

DHCP Servers

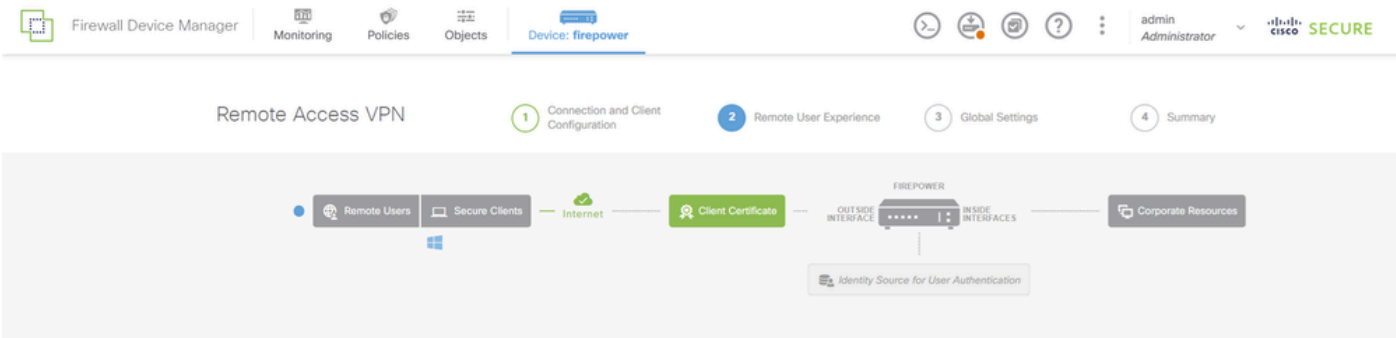
+

CANCEL | NEXT

Detalhes do perfil de conexão VPN

Insira as informações necessárias para a diretiva de grupo e clique no botão Avançar.

- Exibir Política de Grupo: ftd-cert-match-grp



Remote User Experience

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.

View Group Policy

ftd-cert-match-grp

Policy Group Brief Details

DNS + BANNER Edit

DNS Server None

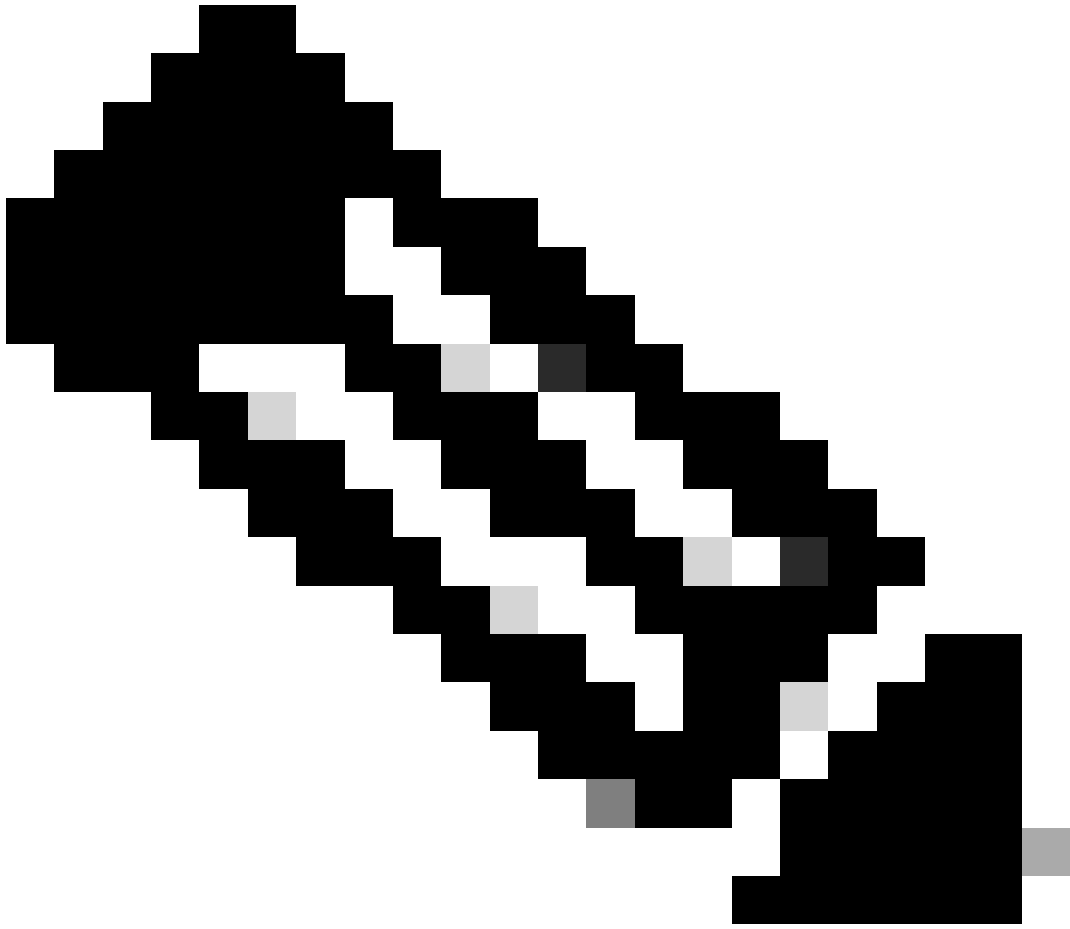
Banner Text for Authentication

BACK NEXT

Selecionar Diretiva de Grupo

Selecione Certificate of Device Identity, Outside Interface, Secure Client Package para conexão VPN.

- Certificado de identidade do dispositivo: ftd-vpn-cert
- Interface externa: externa (GigabitEthernet0/0)
- Pacote de cliente seguro: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg



Observação: o recurso NAT Exempt foi desativado neste documento.



Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

Certificate of Device Identity
ftd-vpn-cert (Validation Usage: SSL Se...)

Outside Interface
outside (GigabitEthernet0/0)

Fully-qualified Domain Name for the Outside Interface
Port
e.g. ravn.example.com 443
e.g. 8080

Access Control for VPN Traffic
Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic.
 Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

NAT Exempt

Secure Client Package
If a user does not already have the right secure client package installed, the system will launch the secure client installer when the client authenticates for the first time. The user can then install the package from the system.
You can download secure client packages from software.cisco.com.
You must have the necessary secure client software license.

Packages
UPLOAD PACKAGE
Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

BACK NEXT

Detalhes das configurações globais

Etapa 10. Confirmar resumo do perfil de conexão

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

^ Summary

Review the summary of the Remote Access VPN configuration.

Ftd-Cert-Match-Vpn

STEP 1: CONNECTION AND CLIENT CONFIGURATION

Primary Identity Source

Authentication Type: Client Certificate Only

Primary Identity Source: -

Fallback Local Identity Source: -

Username from Certificate: Map Specific Field

Primary Field: CN (Common Name)

Secondary Field: OU (Organisational Unit)

Advanced

Authorization Server

Accounting Server

Client Address Pool Assignment

IPv4 Address Pool: ftd-cert-match-pool

IPv6 Address Pool: -

DHCP Servers: -

STEP 2: GROUP POLICY

Group Policy Name: ftd-cert-match-grp

Banner + DNS Server

DNS Server: -

Banner text for authenticated clients: -

Session Settings

Maximum Connection Time / Alert Interval: Unlimited / 1 minutes

Idle Timeout / Alert Interval: 30 / 1 minutes

Simultaneous Login per User: 3

Split Tunneling

IPv4 Split Tunneling: Allow all traffic over tunnel

IPv6 Split Tunneling: Allow all traffic over tunnel

Secure Client

Secure Client Profiles: secureClientProfile

STEP 3: GLOBAL SETTINGS

Certificate of Device Identity: ftd-vpn-cert

Outside Interface: GigabitEthernet0/0 (outside)

Fully-qualified Domain Name for the Outside Interface: -

Port: 443

Access Control for VPN Traffic: No

NAT Exempt

NAT Exempt: No

Inside Interfaces: -

Inside Networks: -

Secure Client Package

Packages: Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

BACK FINISH

Confirmar resumo do perfil de conexão

Confirmar na CLI do FTD

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

```
// Defines IP of interface
interface GigabitEthernet0/0
speed auto
nameif outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.1.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftd-cert-match-pool 172.16.1.150-172.16.1.160

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

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

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

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

// Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/anyconnpkgs/cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg 2
anyconnect profiles secureClientProfile disk0:/anyconncprofs/secureClientProfile.xml
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Configures the group-policy to allow SSL connections
```

```
group-policy ftd-cert-match-grp internal
group-policy ftd-cert-match-grp attributes
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
webvpn
anyconnect ssl dtls none
anyconnect mtu 1406
anyconnect ssl keepalive none
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client none
anyconnect dpd-interval gateway none
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules none
anyconnect profiles value secureClientProfile type user
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting

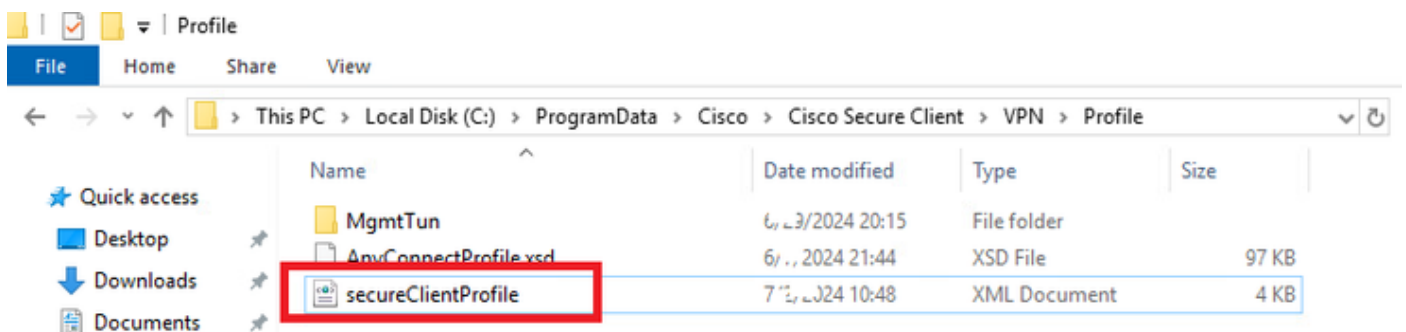
// Configures the tunnel-group to use the certificate authentication
tunnel-group ftd-cert-match-vpn type remote-access
tunnel-group ftd-cert-match-vpn general-attributes
address-pool ftd-cert-match-pool
default-group-policy ftd-cert-match-grp
tunnel-group ftd-cert-match-vpn webvpn-attributes
authentication certificate
group-alias ftd-cert-match-vpn enable
```

Confirmar no cliente VPN

Etapa 1. Copie o perfil do cliente seguro para o cliente VPN

Copie o perfil de cliente seguro para o cliente VPN do engenheiro e o cliente VPN do gerente.

Observação: o diretório do perfil de cliente seguro no computador Windows:
C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile



Copie o perfil do cliente seguro para o cliente VPN

Etapa 2. Confirmar certificado do cliente

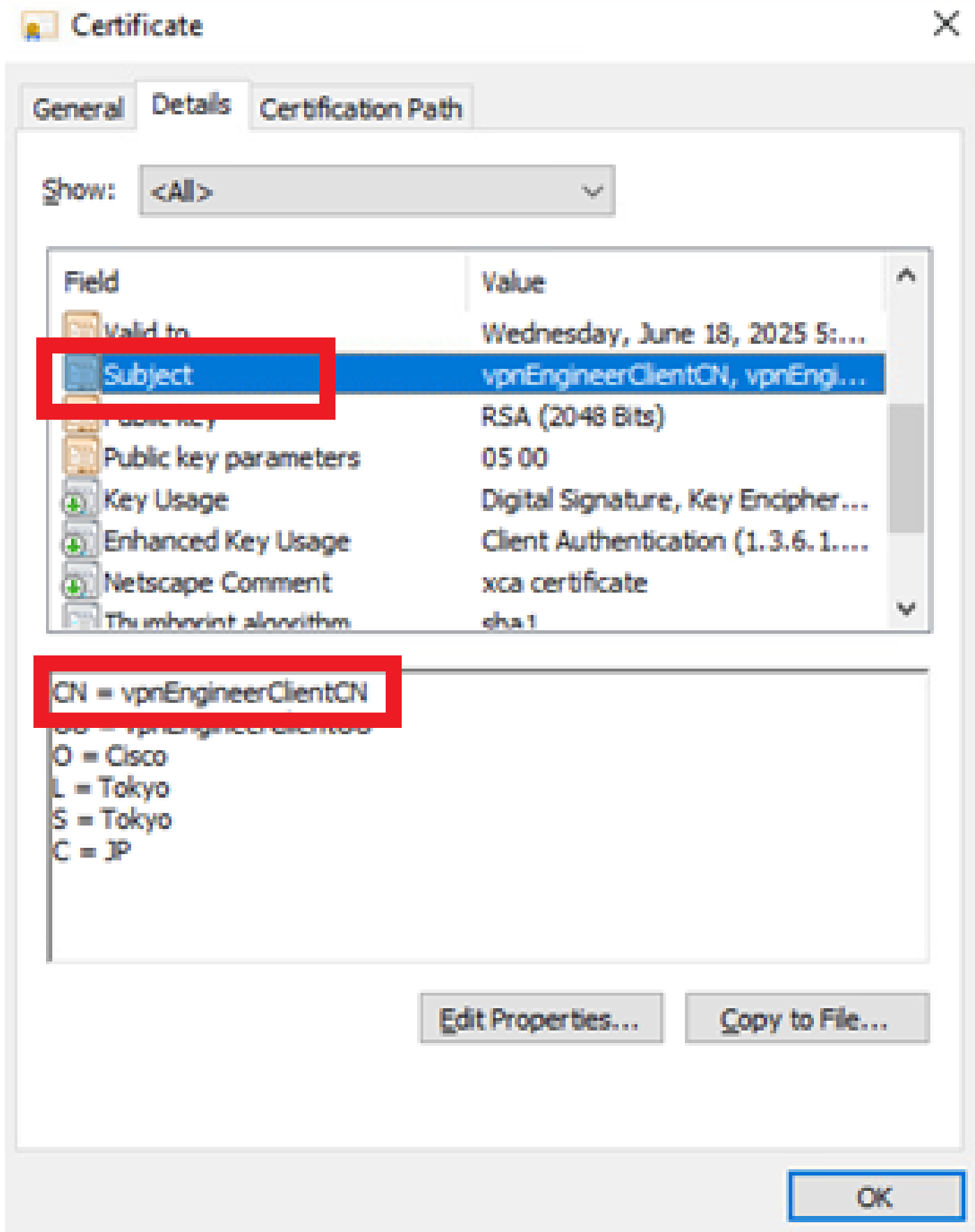
No cliente VPN do engenheiro, navegue para Certificates - Current User > Personal > Certificates, verifique o certificado do cliente usado para autenticação.



Confirmar certificado para cliente VPN do engenheiro

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

- Assunto: CN = vpnEngineerClientCN



Detalhes do certificado de cliente do engenheiro

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



Confirmar Certificado para Cliente VPN do Manager

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

- Assunto: CN = vpnManagerClientCN

Certificate



General Details Certification Path

Show: <All>

Field	Value
Issued	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
O = Cisco
L = Tokyo
S = Tokyo
C = JP

Edit Properties... Copy to File...

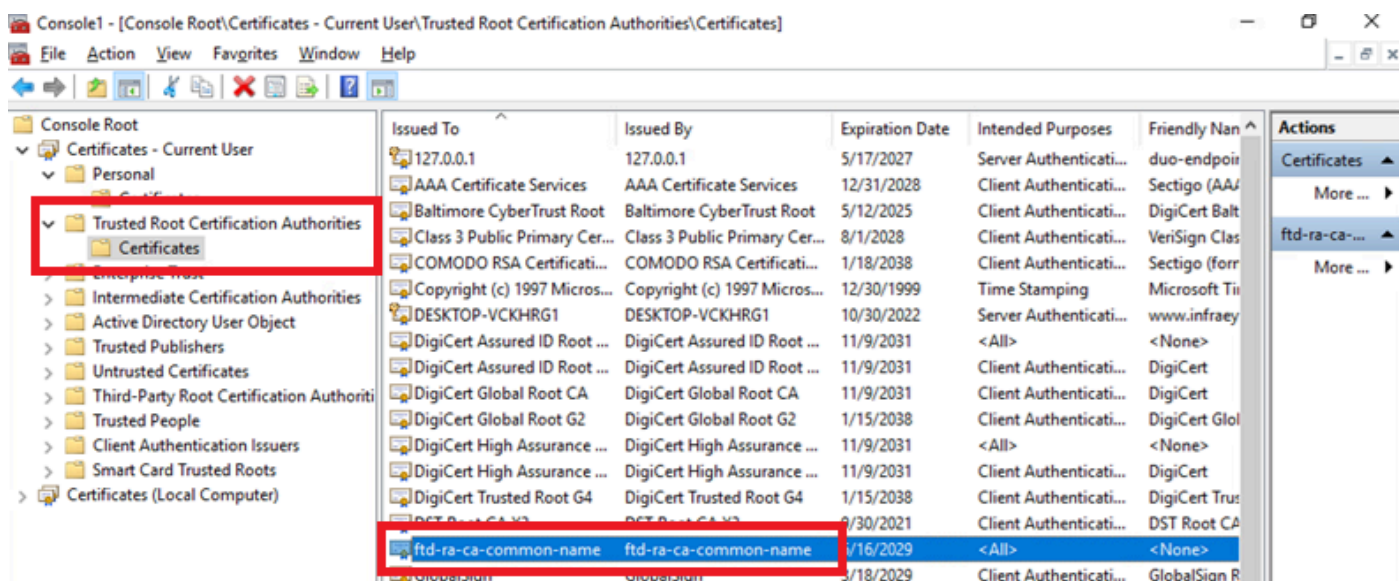
OK

Detalhes do Certificado de Cliente do Gerenciador

Etapa 3. Confirmar CA

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

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



Confirmar CA

Verificar

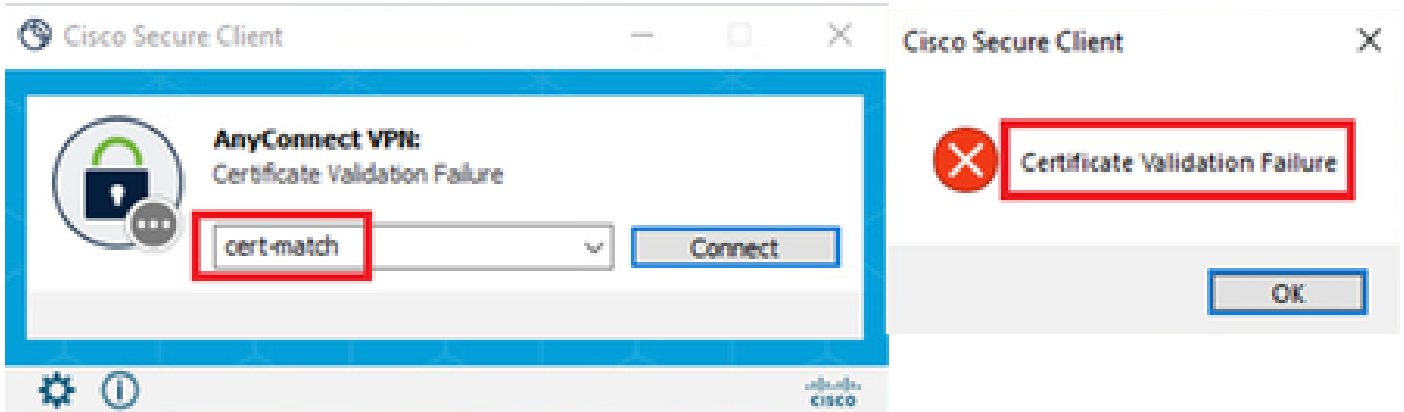
Etapa 1. Iniciar conexão VPN

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.



Conexão VPN bem-sucedida para o VPN Client do Engenheiro

No cliente VPN do gerenciador, inicie a conexão do Cisco Secure Client. A conexão VPN falhou devido a uma falha na validação do certificado.



Falha na conexão VPN para o cliente VPN do gerenciador

Etapa 2. Confirmar sessões VPN na CLI FTD

Execute `show vpn-sessiondb detail anyconnect` o comando na CLI do FTD (Lina) para confirmar as sessões de VPN do engenheiro.

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

Session Type: AnyConnect Detailed

```
Username : vpnEngineerClientCN Index : 32
Assigned IP : 172.16.1.150 Public IP : 192.168.1.11
Protocol : AnyConnect-Parent SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384
Bytes Tx : 14718 Bytes Rx : 12919
Pkts Tx : 2 Pkts Rx : 51
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-cert-match-grp Tunnel Group : ftd-cert-match-vpn
Login Time : 05:42:03 UTC Tue Jul 2 2024
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 00000000000200006683932b
Security Grp : none Tunnel Zone : 0
```

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

AnyConnect-Parent:

```
Tunnel ID : 32.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50170 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.17763
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 7359 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
```

Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 32.2

Assigned IP : 172.16.1.150 Public IP : 192.168.1.11

Encryption : AES-GCM-256 Hashing : SHA384

Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384

Encapsulation: TLSv1.2 TCP Src Port : 50177

TCP Dst Port : 443 Auth Mode : Certificate

Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes

Client OS : Windows

Client Type : SSL VPN Client

Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74

Bytes Tx : 7359 Bytes Rx : 12919

Pkts Tx : 1 Pkts Rx : 51

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 computador Windows.

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

Jul 02 2024 04:16:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpn

Jul 02 2024 04:16:03: %FTD-6-717022: Certificate was successfully validated. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClic

Jul 02 2024 04:16:04: %FTD-6-113009: AAA retrieved default group policy (ftd-cert-match-grp) for user = vpnEngineerClientCN

Jul 02 2024 04:16:09: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50158 to 192.168.1.200/443 for TLSv1.2 sessi

Informações Relacionadas

[Configurar o Serviço de Gerenciamento em Caixa do FDM para Firepower 2100](#)

[Configurar a VPN de Acesso Remoto no FTD Gerenciado pelo FDM](#)

[Configurar e verificar o Syslog no Gerenciador de dispositivos do Firepower](#)

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.