Configurar AAA e Cert Auth para 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 Perfil de Conexão VPN de Acesso Remoto
    - Etapa 4. Adicionar Pool de Endereços para Perfil de Conexão
    - Etapa 5. Adicionar Política de Grupo para Perfil de Conexão
    - Etapa 6. Configurar Certificado de Identidade do Dispositivo e Interface Externa para Perfil de Conexão
    - Passo 7. Configurar Imagem de Cliente Seguro para Perfil de Conexão
    - Etapa 8. Confirmar resumo do perfil de conexão
    - Etapa 9. Adicionar Usuário a LocalIdentitySource
    - Etapa 10. Adicionar CA ao FTD
  - Confirmar na CLI do FTD
  - Confirmar no cliente VPN
    - Etapa 1. Confirmar certificado do cliente
    - Etapa 2. Confirmar CA
- Verificar
  - Etapa 1. Iniciar conexão VPN
  - Etapa 2. Confirmar sessão VPN na CLI FTD
  - Etapa 3. Confirmar comunicação com o servidor
- Troubleshooting
- Informações Relacionadas

Introdução

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

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

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 Firepower Device Manager (FDM) é uma interface de gerenciamento simplificada baseada na Web usada para gerenciar dispositivos do Cisco Firepower Threat Defense (FTD). O Firepower Device Manager permite que os administradores de rede configurem e gerenciem seus dispositivos de FTD sem usar o mais complexo Firepower Management Center (FMC). O FDM fornece uma interface de usuário intuitiva para operações básicas, como configurar interfaces de rede, zonas de segurança, políticas de controle de acesso e VPNs, bem como para monitorar o desempenho do dispositivo e eventos de segurança. Ele é adequado para implantações de pequeno a médio porte, onde o gerenciamento simplificado é desejado.
Este documento descreve como integrar nomes de usuário pré-preenchidos com o Cisco Secure Client no FTD gerenciado pelo FDM.
Se você estiver gerenciando o FTD com o FMC, consulte o guia Configure AAA and Cert Auth for Secure Client on FTD via FMC.

Esta é a cadeia de certificados com o nome comum de cada certificado usado no documento.

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

Diagrama de Rede

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

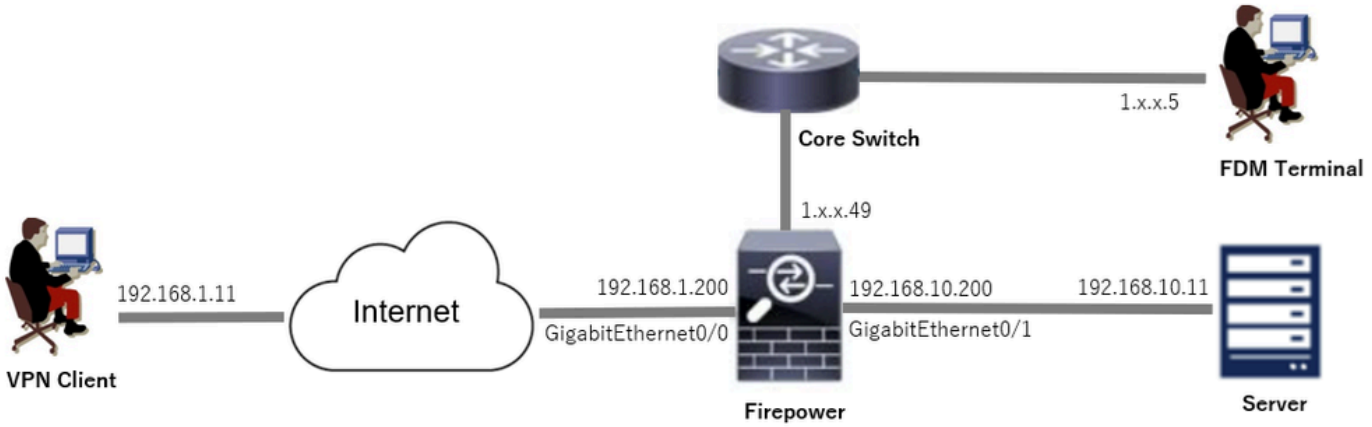


Diagrama de Rede

Configurações

Configuração no FDM

Etapa 1. Configurar a interface FTD

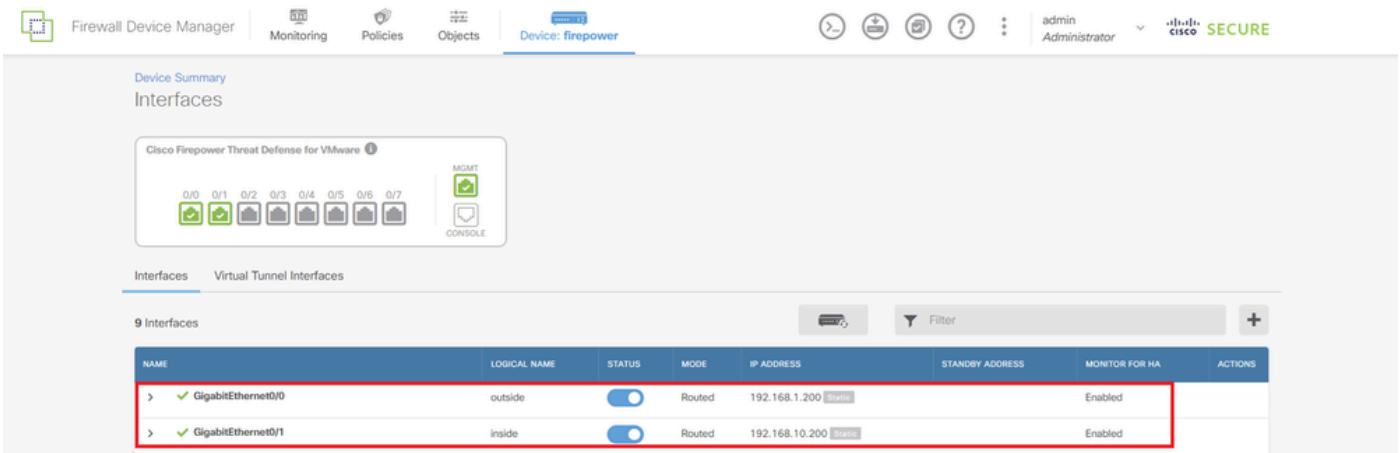
Navegue até Device > Interfaces > View All Interfaces, configure a interface interna e externa para FTD na guia Interfaces.

Para GigabitEthernet0/0,

- Nome: externo
- Endereço IP: 192.168.1.200/24

Para GigabitEthernet0/1,

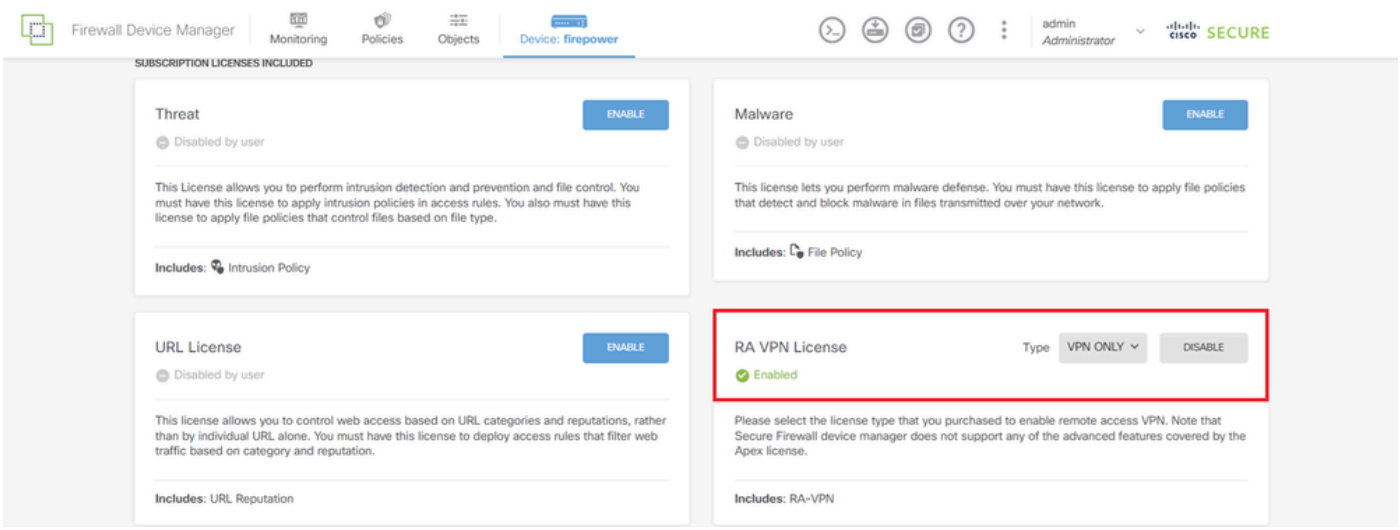
- Nome: dentro
- Endereço IP: 192.168.10.200/24



Interface FTD

Etapa 2. Confirmar licença do Cisco Secure Client

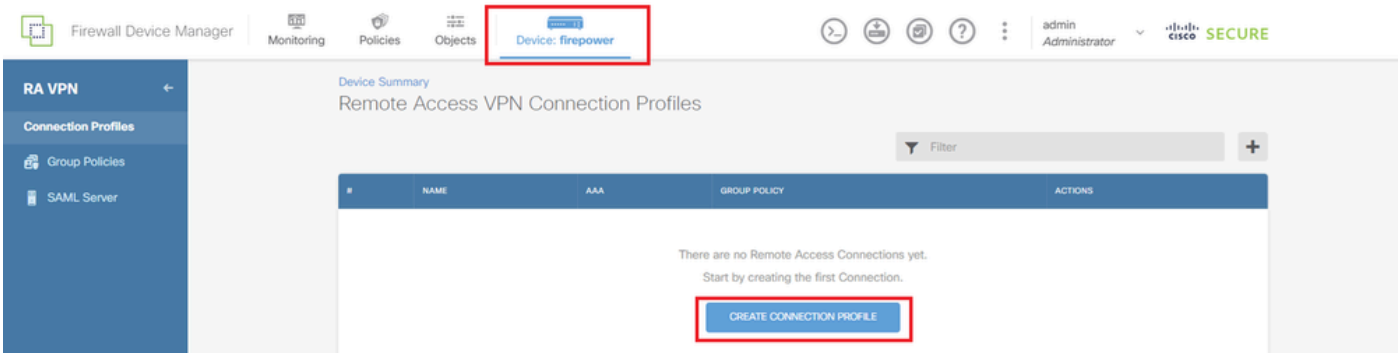
Navegue até Device > Smart License > View Configuration, confirme a licença do Cisco Secure Client em RA VPN Licenseitem.



Licença de cliente seguro

Etapa 3. Adicionar Perfil de Conexão VPN de Acesso Remoto

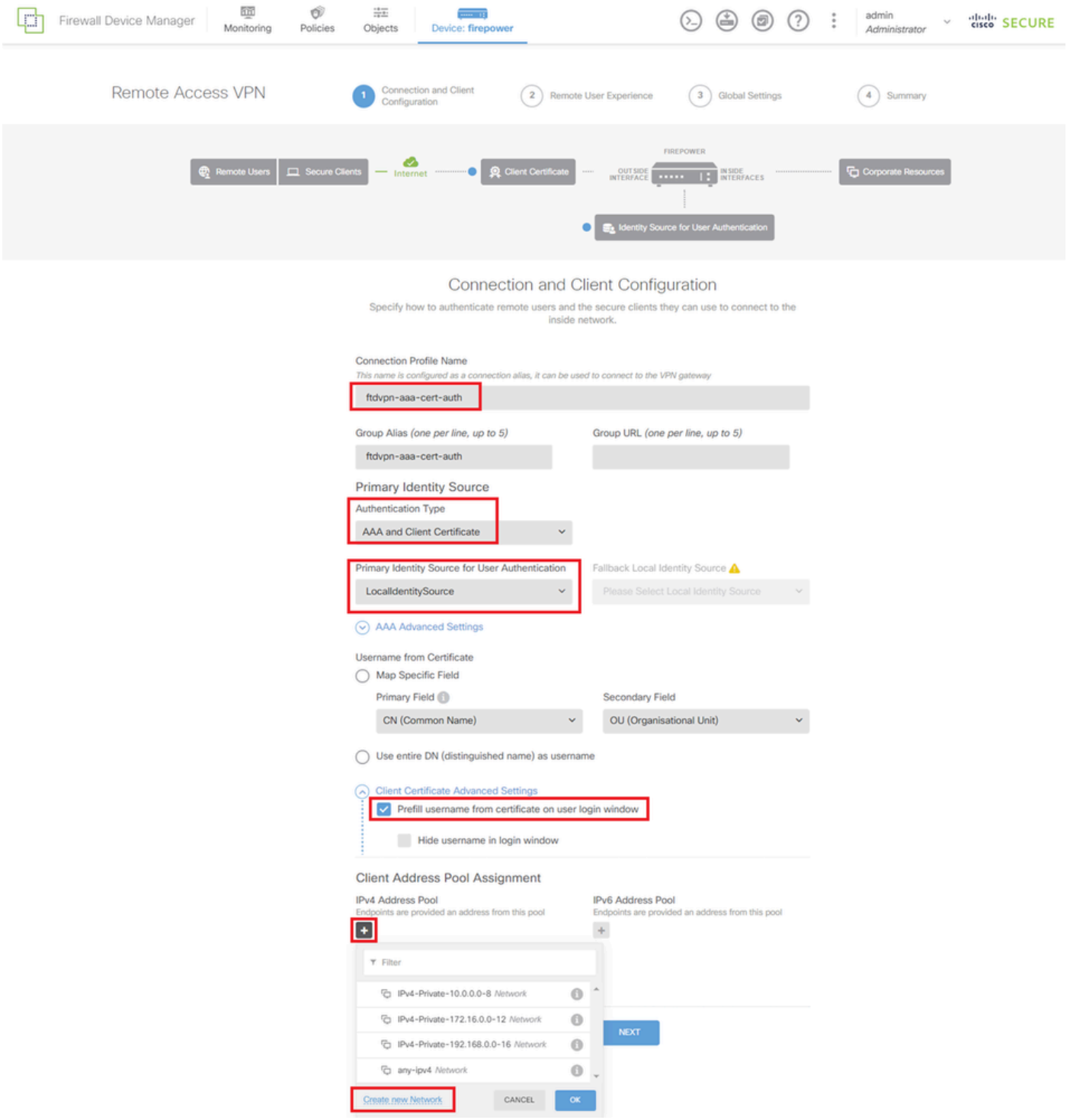
Navegue até Device > Remote Access VPN > View Configuration, clique no botão CREATE CONNECTION PROFILE.



Adicionar Perfil de Conexão VPN de Acesso Remoto

Insira as informações necessárias para o perfil de conexão e clique no botão Create new Network no item IPv4 Address Pool.

- Nome do perfil de conexão: ftdvpn-aaa-cert-auth
- Tipo de autenticação: AAA e certificado do cliente
- Origem de Identidade Primária para Autenticação de Usuário: LocalIdentitySource
- Configurações Avançadas de Certificado de Cliente: Preencha previamente o nome de usuário a partir do certificado na janela de logon do usuário

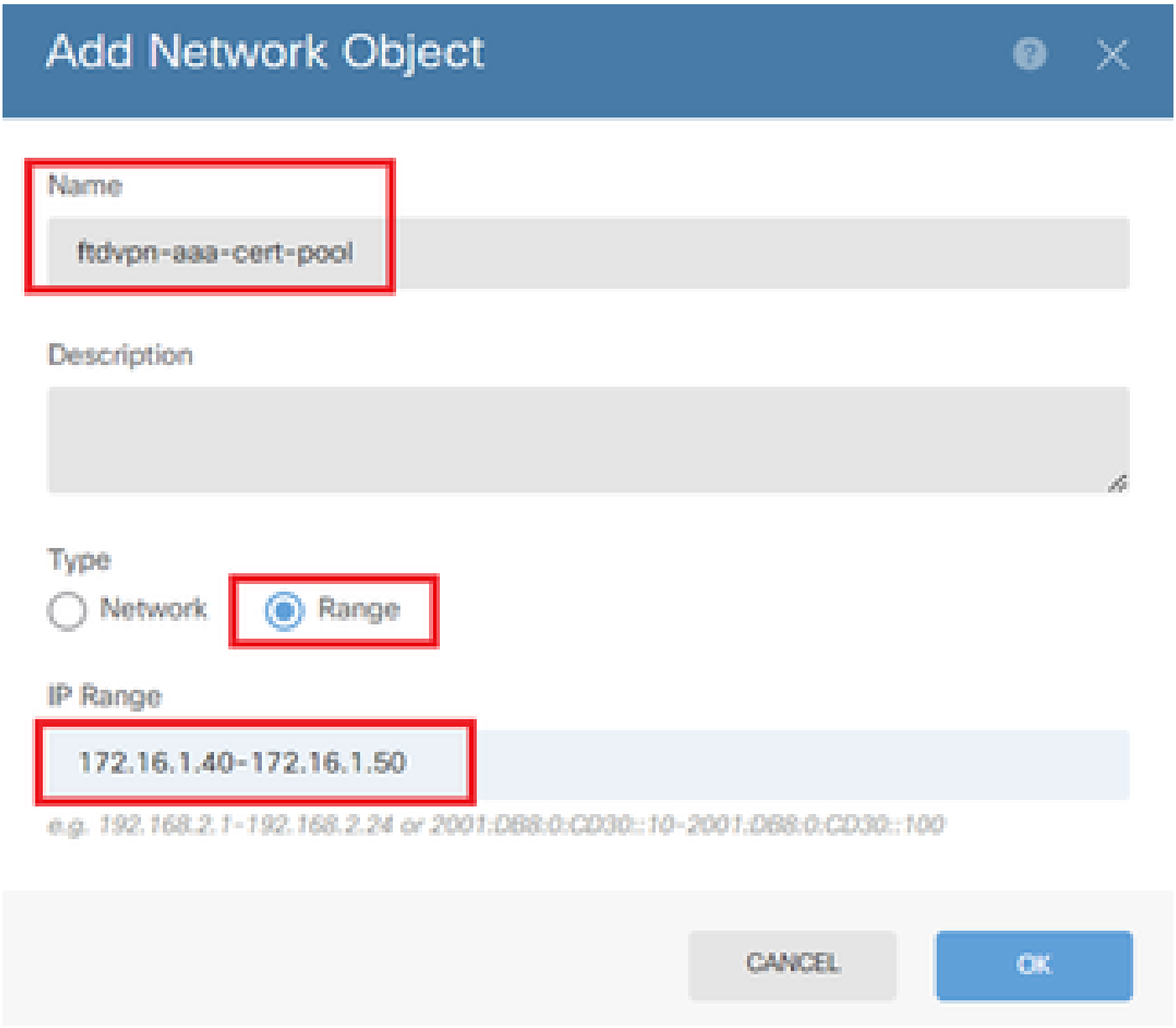


Detalhes do perfil de conexão VPN

Etapa 4. Adicionar Pool de Endereços para Perfil de Conexão

Insira as informações necessárias para adicionar um novo pool de endereços IPv4. Selecione o novo pool de endereços IPv4 adicionado para o perfil de conexão e clique no botão Avançar.

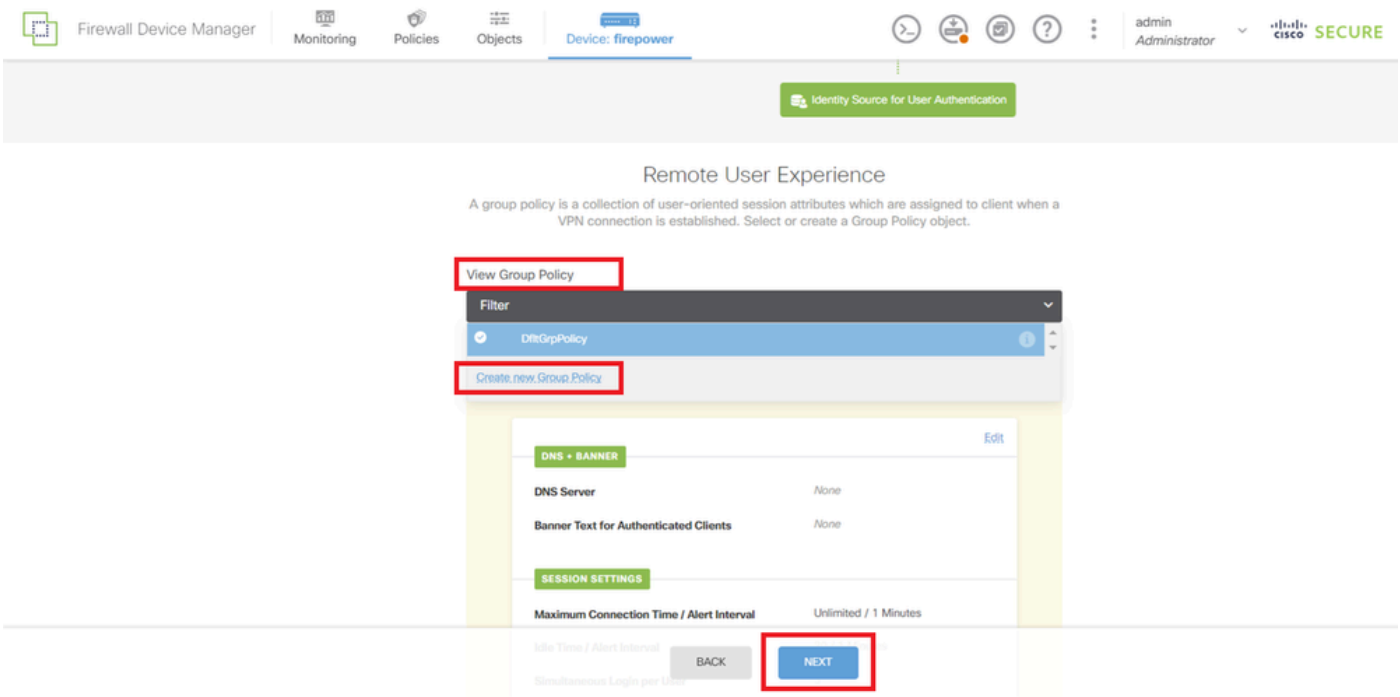
- Nome: ftdvpn-aaa-cert-pool
- Tipo: Intervalo
- Intervalo de IPs: 172.16.1.40-172.16.1.50



Detalhes do Pool de Endereços IPv4

Etapa 5. Adicionar Política de Grupo para Perfil de Conexão

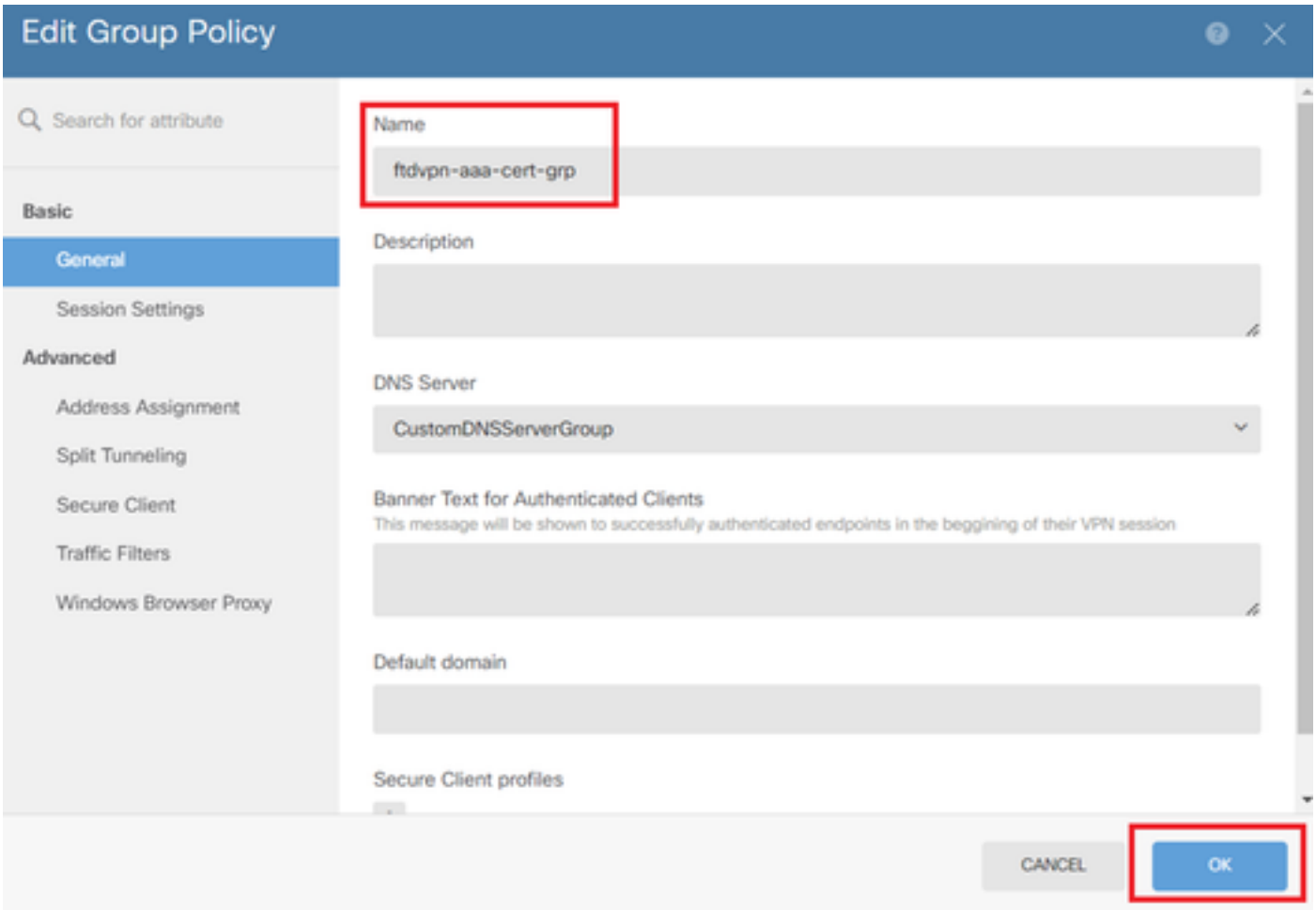
Clique em Create new Group Policy no item View Group Policy.



Adicionar Política de Grupo

Insira as informações necessárias para adicionar uma nova política de grupo e clique no botão OK. Selecione a nova diretiva de grupo adicionada para o perfil de conexão.

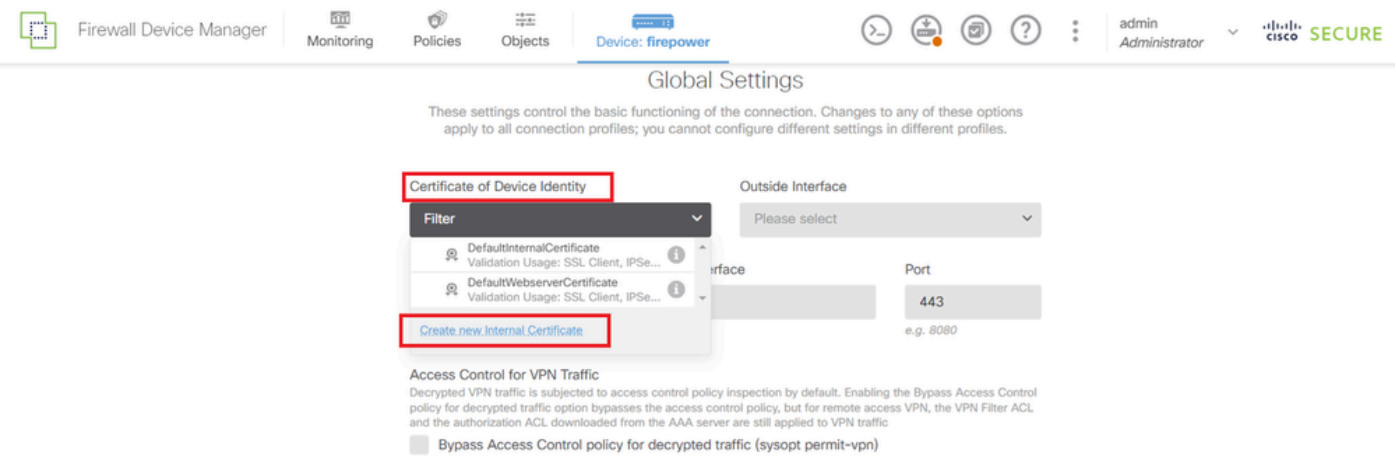
- Nome: ftdvpn-aaa-cert-grp



Detalhes da Política de Grupo

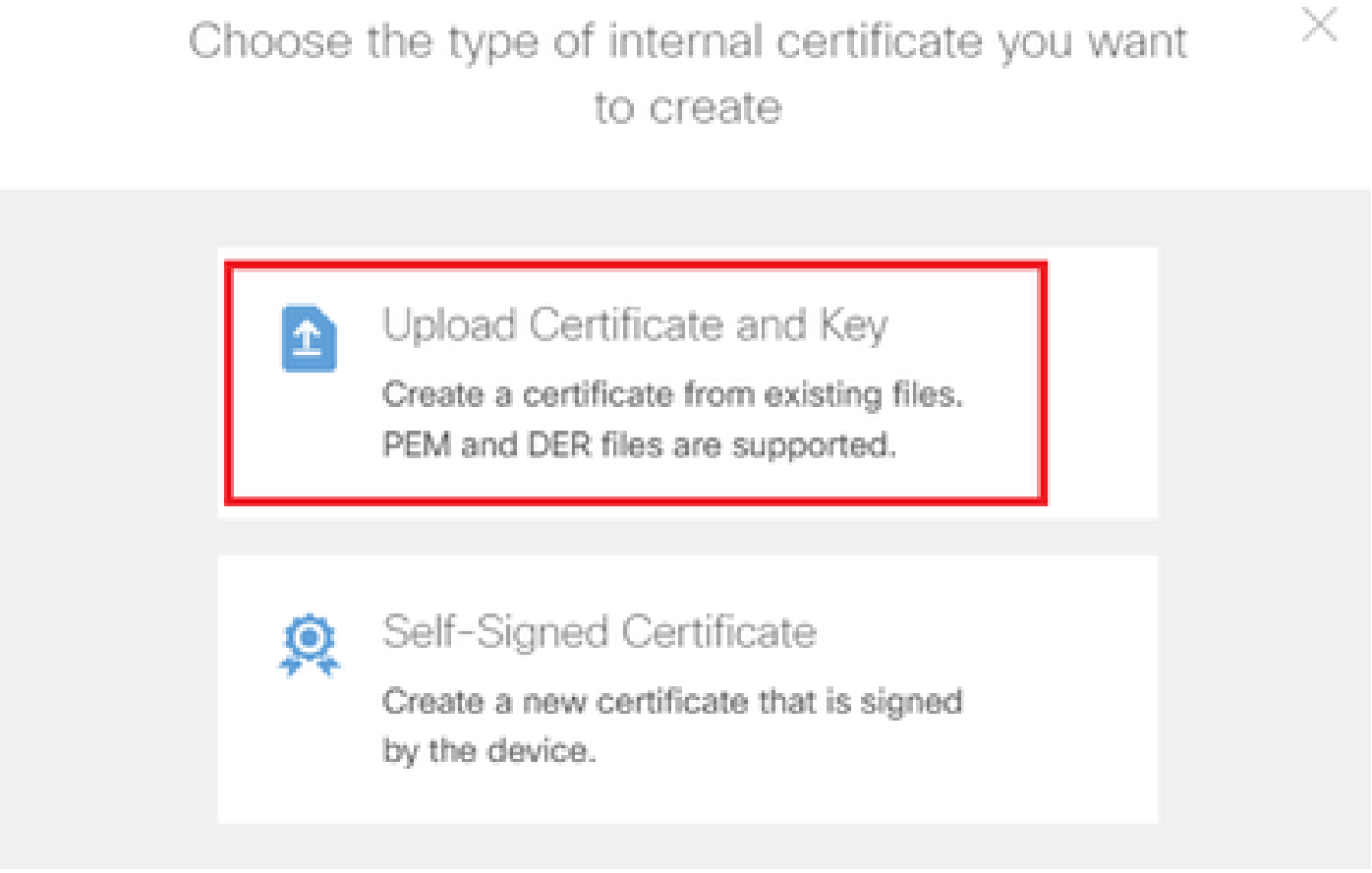
Etapa 6. Configurar Certificado de Identidade do Dispositivo e Interface Externa para Perfil de Conexão

Clique em Create new Internal certificate no item Certificate of Device Identity.



Adicionar certificado interno

Clique em Carregar certificado e chave.

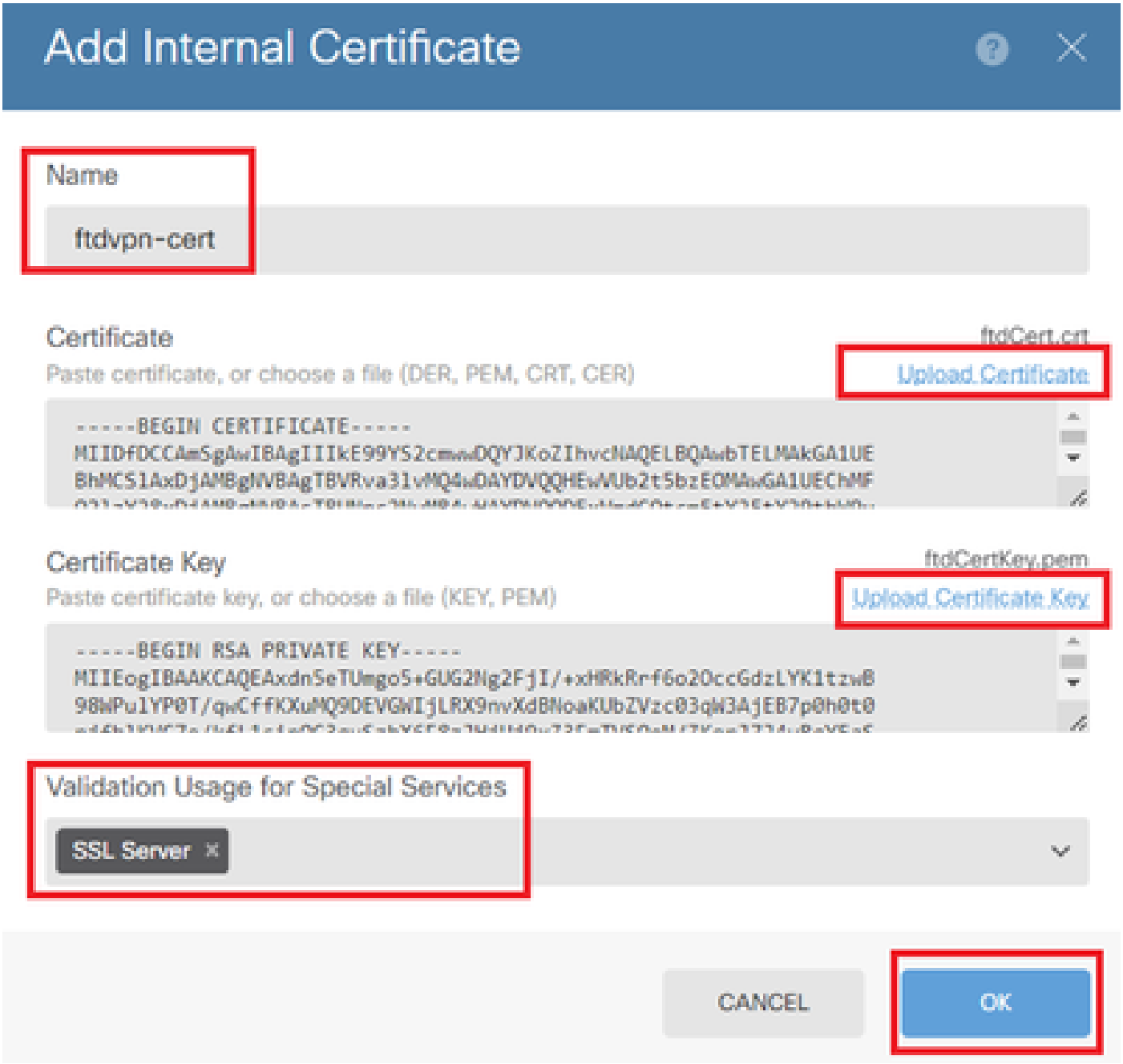


Carregar certificado e chave

Insira as informações necessárias para o certificado FTD, importe um certificado e uma chave de

certificado do computador local e clique no botão OK.

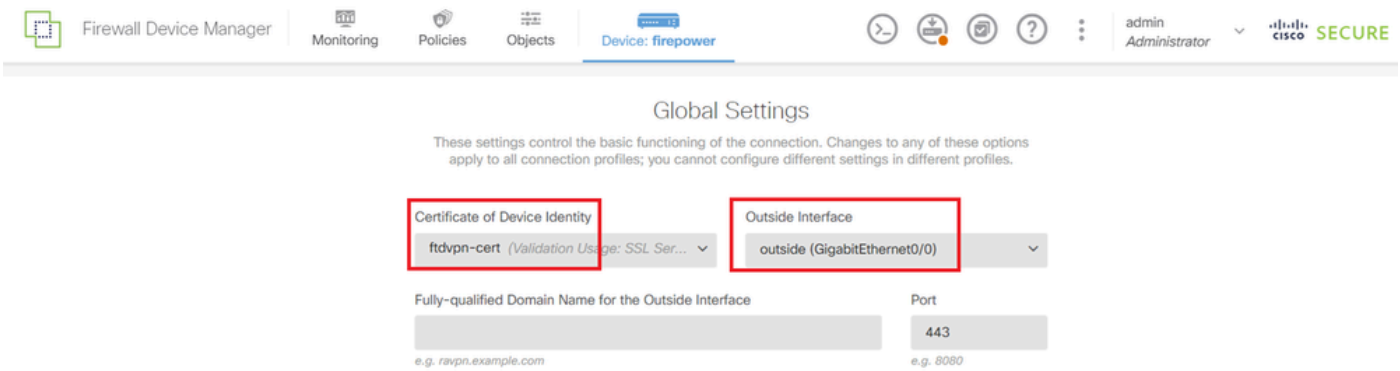
- Nome: ftdvpn-cert
- Uso da validação para serviços especiais: servidor SSL



Detalhes do certificado interno

Selecione Certificate of Device Identity e Outside Interface para conexão VPN.

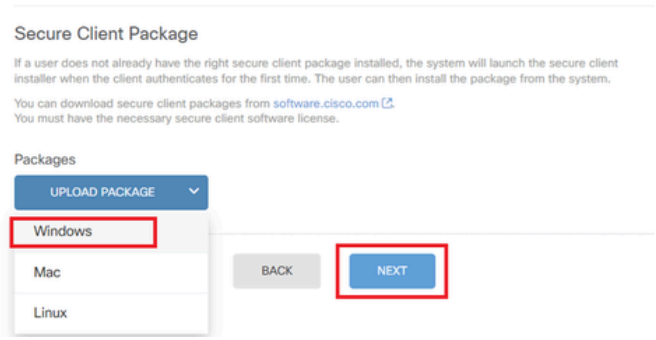
- Certificado de identidade do dispositivo: ftdvpn-cert
- Interface externa: externa (GigabitEthernet0/0)



Detalhes das configurações globais

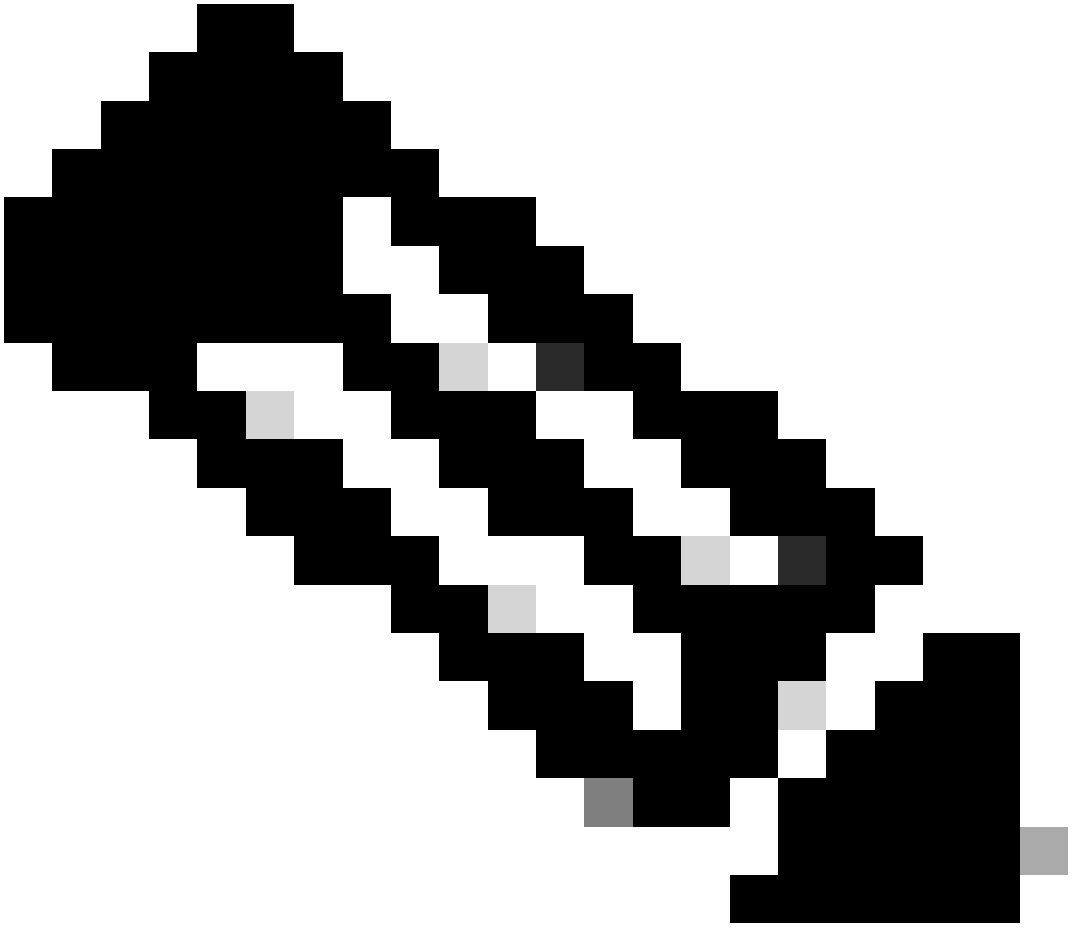
Passo 7. Configurar Imagem de Cliente Seguro para Perfil de Conexão

Selecione o item Windows em Pacotes

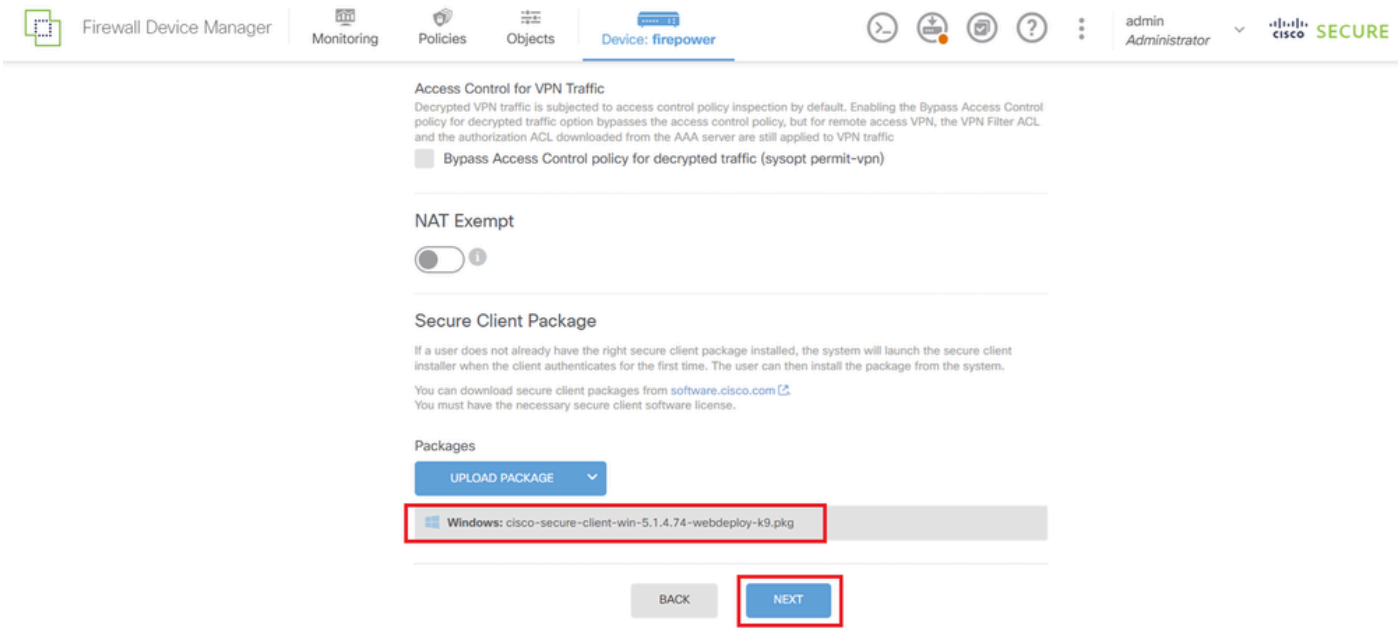


Carregar Pacote de Imagem de Cliente Seguro

Carregue o arquivo de imagem de cliente seguro do computador local e clique no botão Avançar.



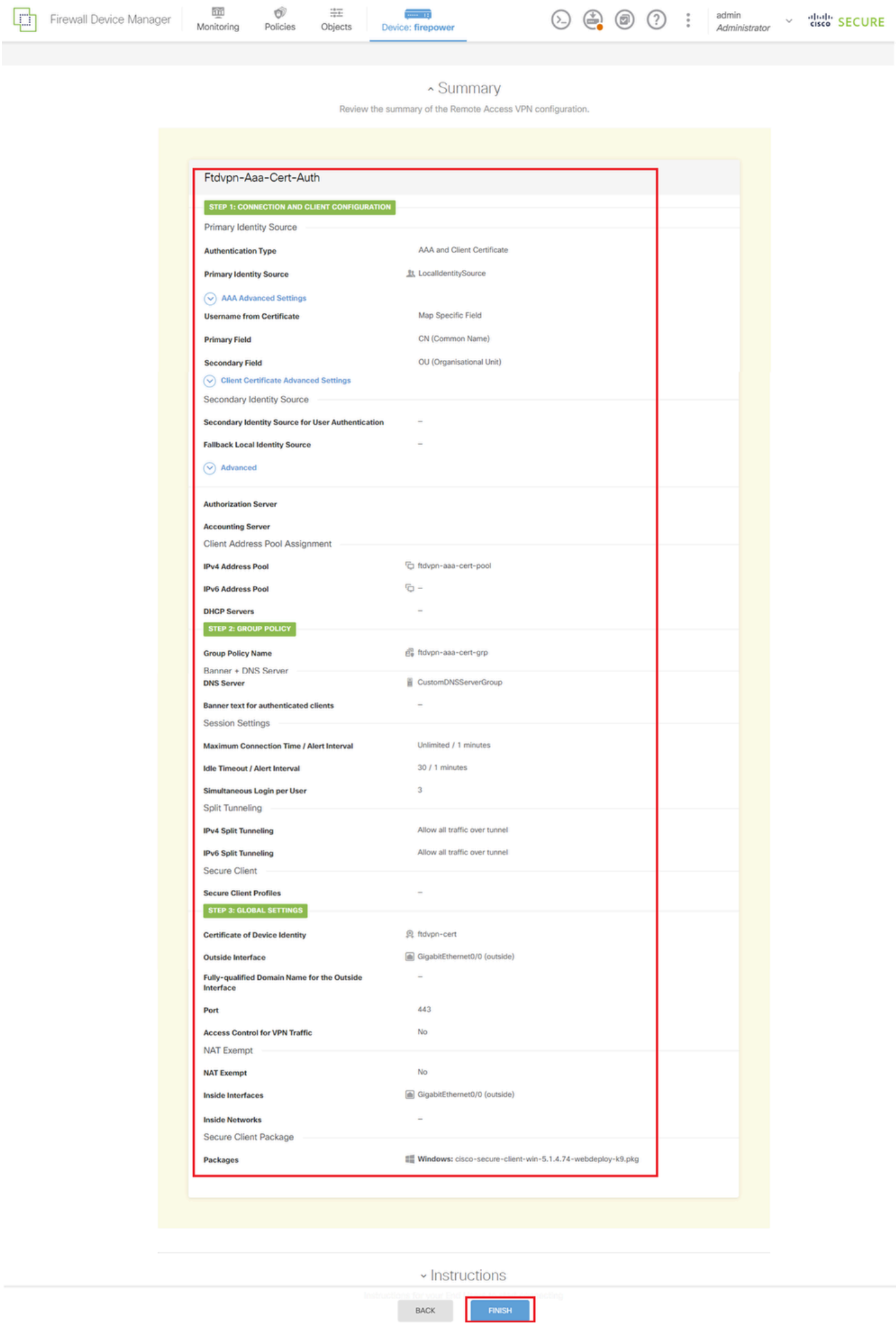
Observação: o recurso NAT Exempt está desabilitado neste documento. Por padrão, a opção Bypass Access Control policy for decrypted traffic (sysopt permit-vpn) está desabilitada, o que significa que o tráfego de VPN descriptografado está sujeito à inspeção da política de controle de acesso.



Selecionar Pacote de Imagem de Cliente Seguro

Etapa 8. Confirmar resumo do perfil de conexão

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



Confirmar configurações do perfil de conexão

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

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

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

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

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

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

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

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

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

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

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

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

Confirmar no cliente VPN

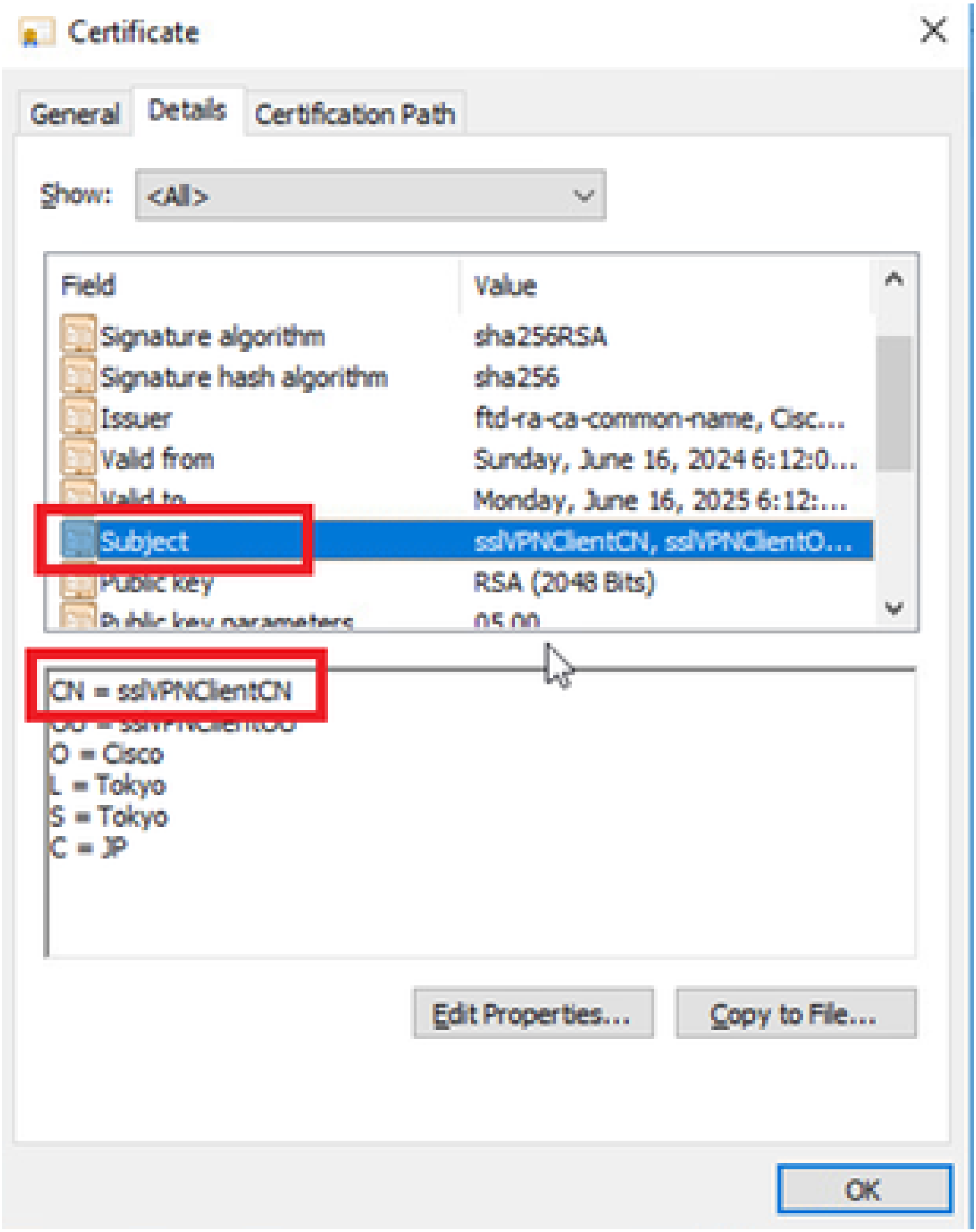
Etapa 1. Confirmar certificado do cliente

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

Confirmar certificado do cliente

Clique duas vezes no certificado do cliente, navegue paraDetails, verifique o detalhe deSubject.

- Assunto: CN = sslVPNClientCN



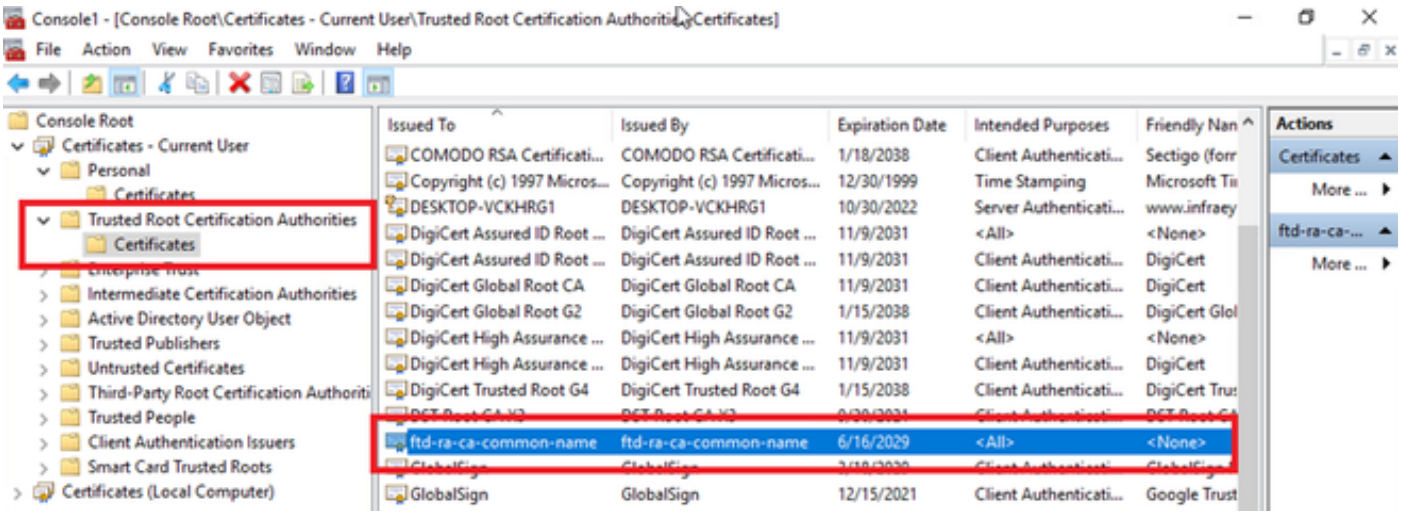
Detalhes do Certificado do Cliente

Etapa 2. Confirmar CA

Navegue para Certificados - Usuário atual > Autoridades de certificação raiz confiáveis >

Certificados, verifique a CA usada para autenticação.

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

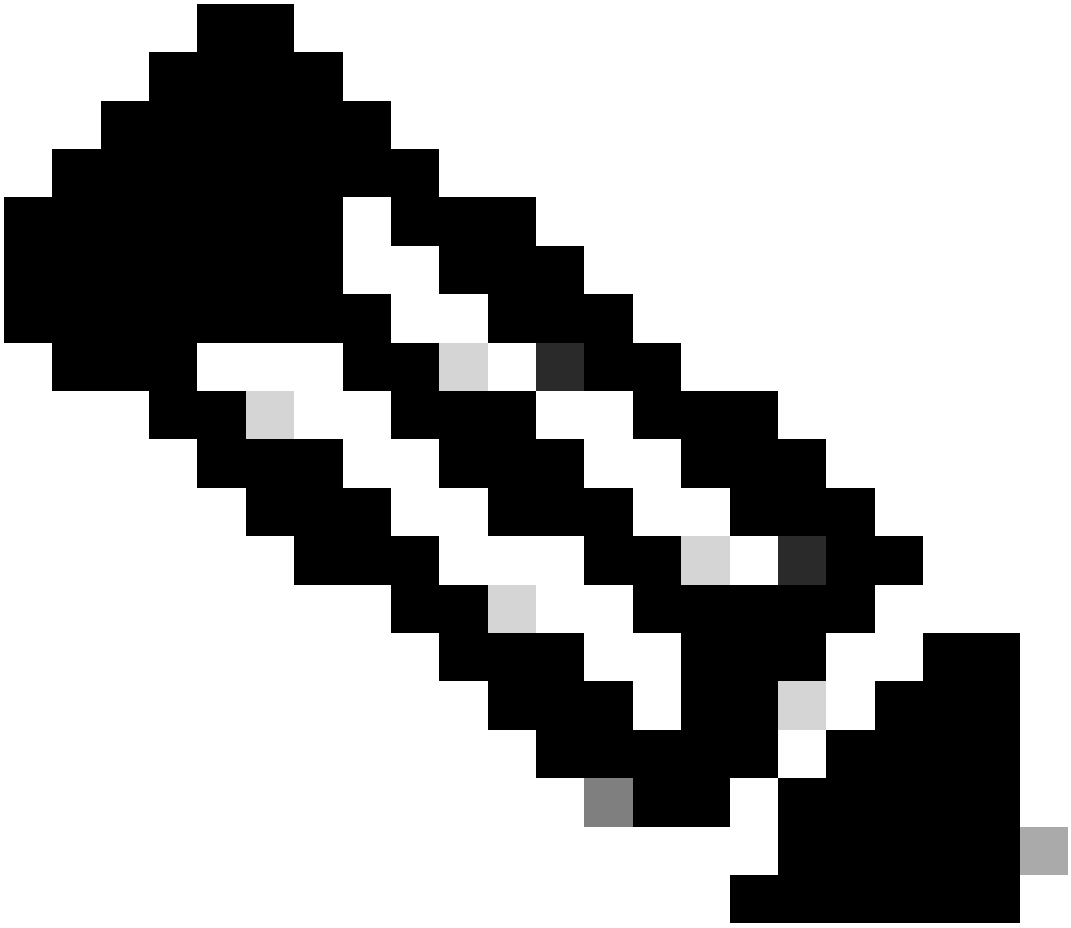


Confirmar CA

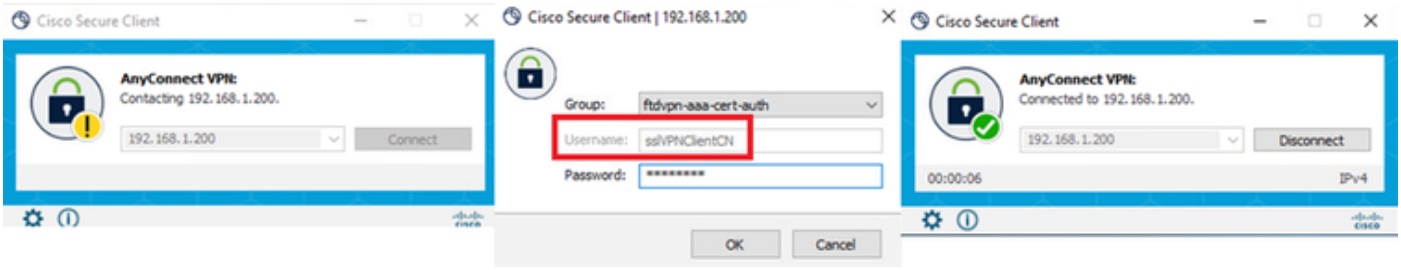
Verificar

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 Nome comum (CN) do certificado de cliente neste documento.



Iniciar conexão VPN

Etapa 2. Confirmar sessão VPN na CLI FTD

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

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

Session Type: AnyConnect Detailed

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

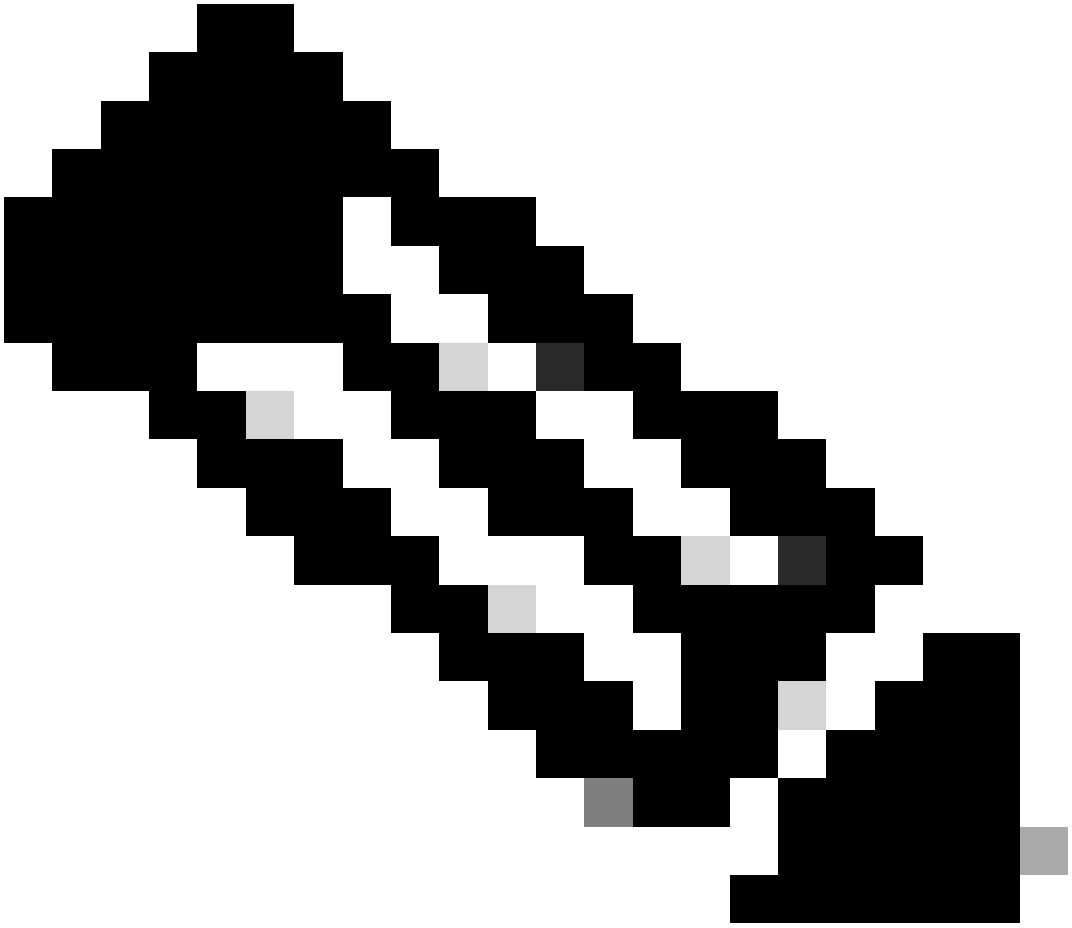
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1

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

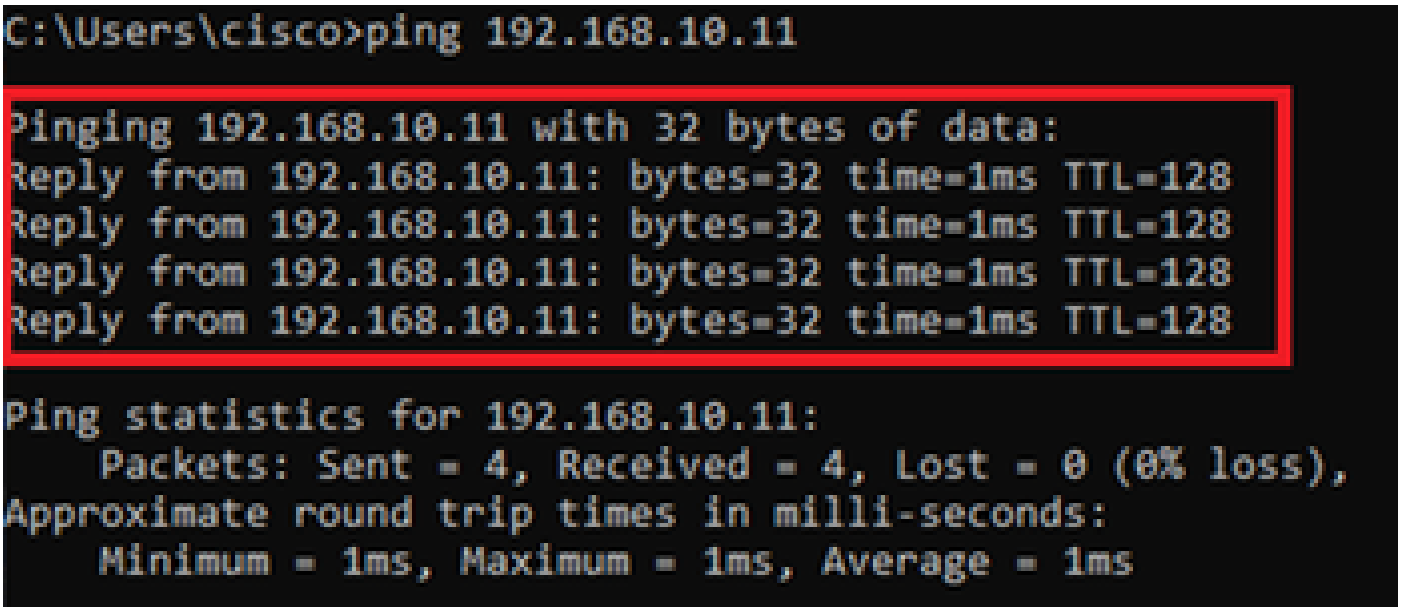
SSL-Tunnel:
Tunnel ID : 4.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 49788
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO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

Etapa 3. 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.



Observação: como a opção Ignorar política de Controle de Acesso para tráfego descriptografado (sysopt permit-vpn) está desabilitada na etapa 7, você precisa criar regras de controle de acesso que permitam o acesso do pool de endereços IPv4 ao servidor.



Ping bem-sucedido

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

firepower# capture in interface inside real-time

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

Use ctrl-c to terminate real-time capture

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

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.

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

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

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

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

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.