AAA- en Cert-autorisatie voor beveiligde client configureren op FTD via FDM

Inhoud

Inleiding

Dit document beschrijft de stappen voor het configureren van Cisco Secure Client over SSL op FTD die wordt beheerd door FDM met AAA- en certificaatverificatie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Firepower Device Manager (FDM) virtueel
- Firewall Threat Defense (FTD) virtueel
- VPN-verificatiestroom

Gebruikte componenten

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

- Cisco Secure-client 5.1.4.7

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

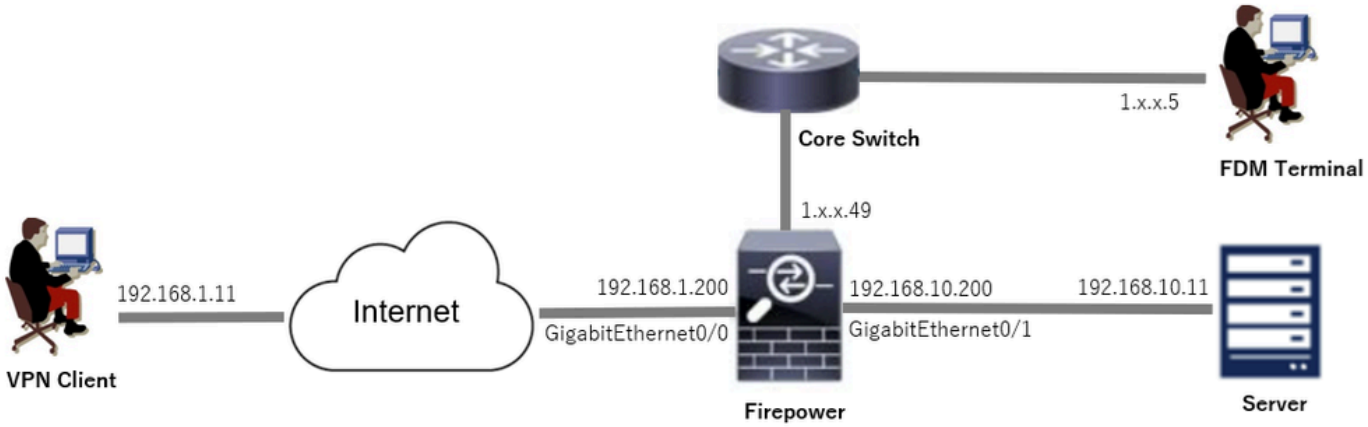
Firepower Device Manager (FDM) is een vereenvoudigde, webgebaseerde beheerinterface die wordt gebruikt voor het beheer van Cisco Firepower Threat Defence (FTD)-apparaten. Met Firepower Device Manager kunnen netwerkbeheerders hun FTD-apparaten configureren en beheren zonder gebruik te maken van het meer complexe Firepower Management Center (FMC). FDM biedt een intuïtieve gebruikersinterface voor basisbewerkingen zoals het instellen van netwerkinterfaces, beveiligingszones, toegangscontrolemaatregelen en VPN's, evenals voor het bewaken van de prestaties van het apparaat en beveiligingsgebeurtenissen. Het is geschikt voor kleine tot middelgrote implementaties waar vereenvoudigd beheer gewenst is.
Dit document beschrijft hoe u voorgevulde gebruikersnamen kunt integreren met Cisco Secure Client op FTD die wordt beheerd door FDM.
Als u FTD met FMC beheert, raadpleegt u de handleiding AAA en Cert Auth for Secure Client configureren op FTD via FMC.

Dit is de certificaatketen met de gemeenschappelijke naam van elk certificaat dat in het document wordt gebruikt.

- CA: ftd-ra-ca-common-name
- Clientcertificaat: sslVPNClientCN
- Servercertificaat: 192.168.1.200

Netwerkdiagram

Dit beeld toont de topologie die bij het voorbeeld van dit document wordt gebruikt.



Netwerkdiagram

Configuraties

Configuratie in FDM

Stap 1. FTD-interface configureren

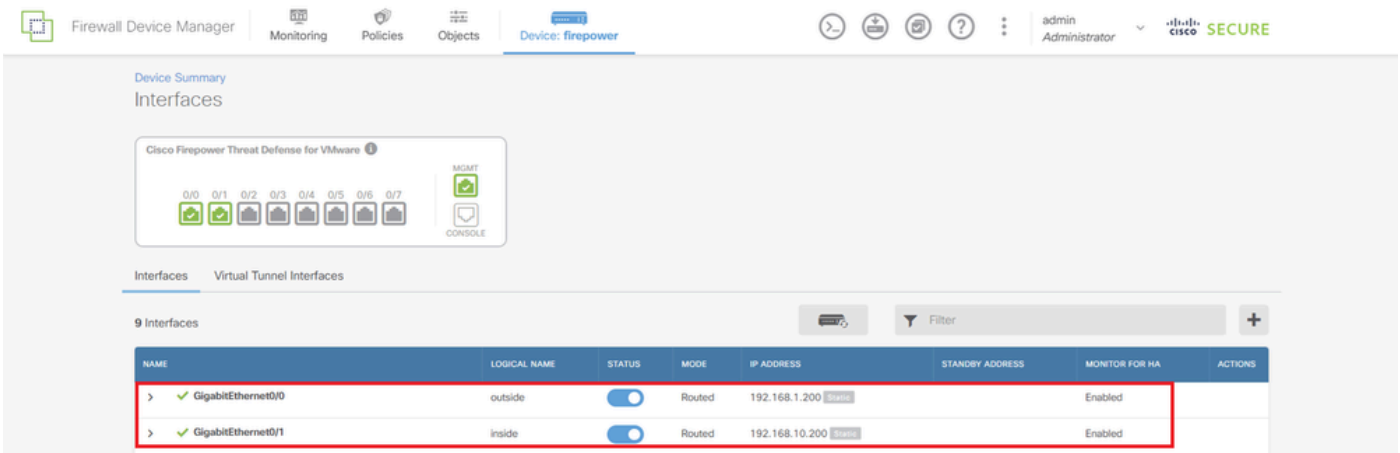
Navigeren naar apparaat > Interfaces > Alle interfaces weergeven, binnen en buiten interface configureren voor FTD in Interfacestab.

Voor Gigabit Ethernet0/0,

- Naam: buiten
- IP-adres: 192.168.1.200/24

Voor Gigabit Ethernet0/1,

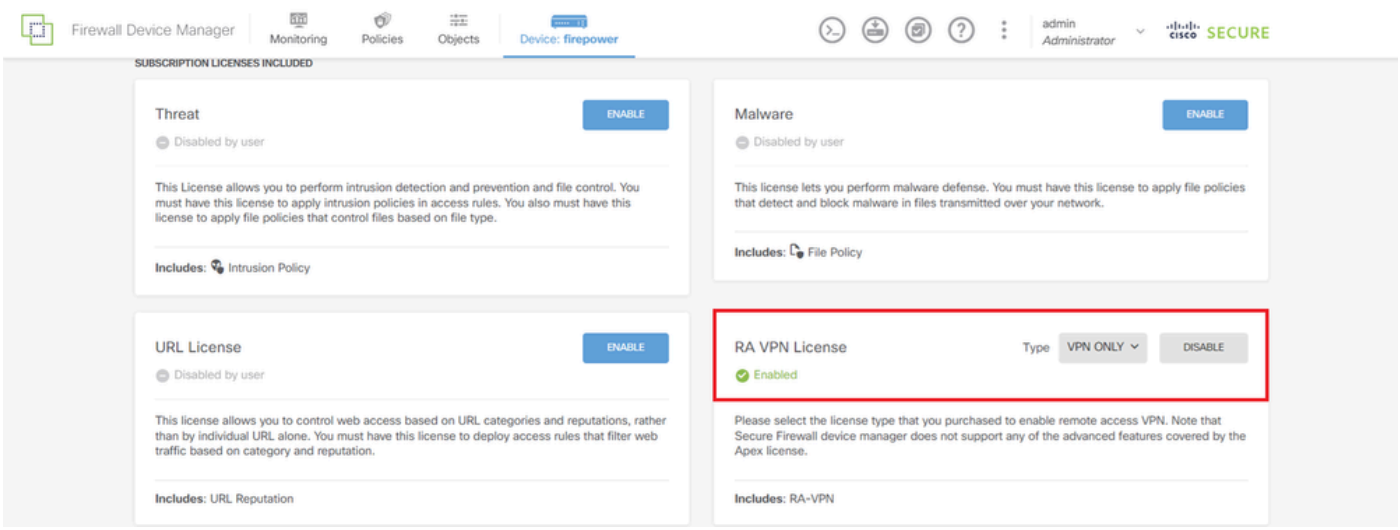
- Naam: binnen
- IP-adres: 192.168.10.200/24



FTD-interface

Stap 2. Cisco Secure-clientlicentie bevestigen

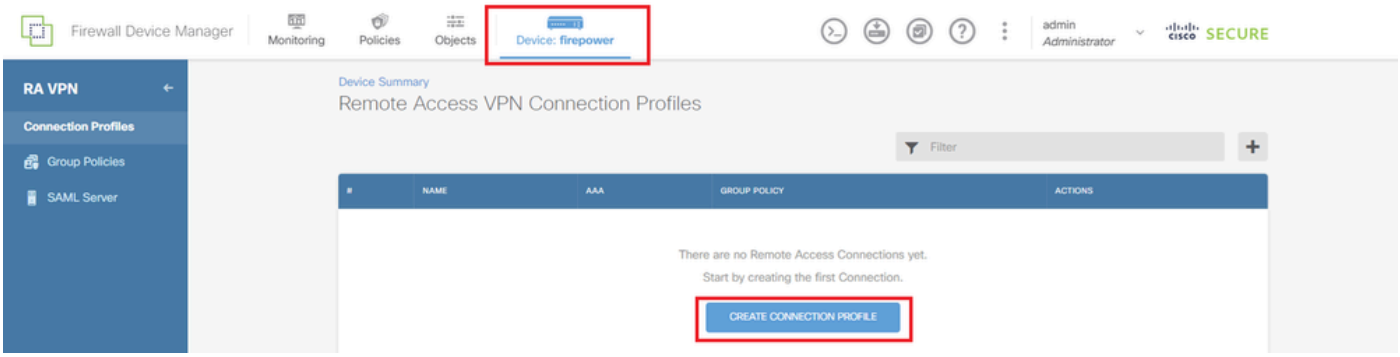
Navigeer naar apparaat > slimme licentie > Configuratie bekijken, bevestig de Cisco Secure Client-licentie in RA VPN-licentie.



Secure-clientlicentie

Stap 3. VPN-verbindingsprofiel voor externe toegang toevoegen

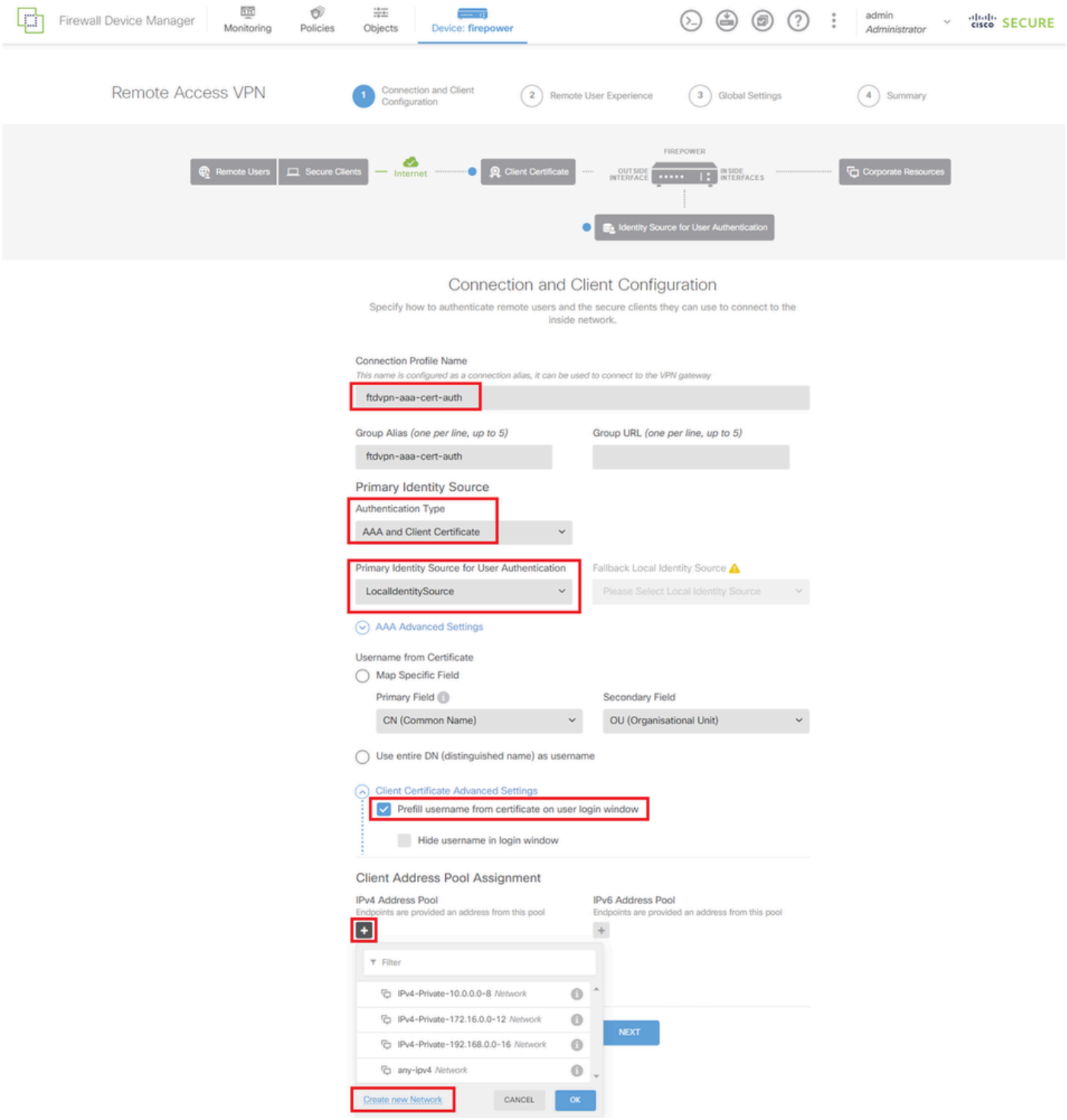
Navigeer naar Apparaat > Externe toegang VPN > Configuratie bekijken, klik op de knop VERBINDINGSPROFIEL MAKEN.



VPN-verbindingsprofiel voor externe toegang toevoegen

Voer de informatie in die nodig is voor het verbindingsprofiel en klik op de knop Nieuw netwerk maken in de optie IPv4-adresgroep.

- Naam verbindingsprofiel: ftdvpn-aaa-cert-auth
- Verificatietype: AAA- en clientcertificaat
- Primaire identiteitsbron voor gebruikersverificatie: LocalIdentitySource
- Geavanceerde instellingen clientcertificaat: gebruikersnaam vooraf invullen van certificaat in het inlogvenster van de gebruiker

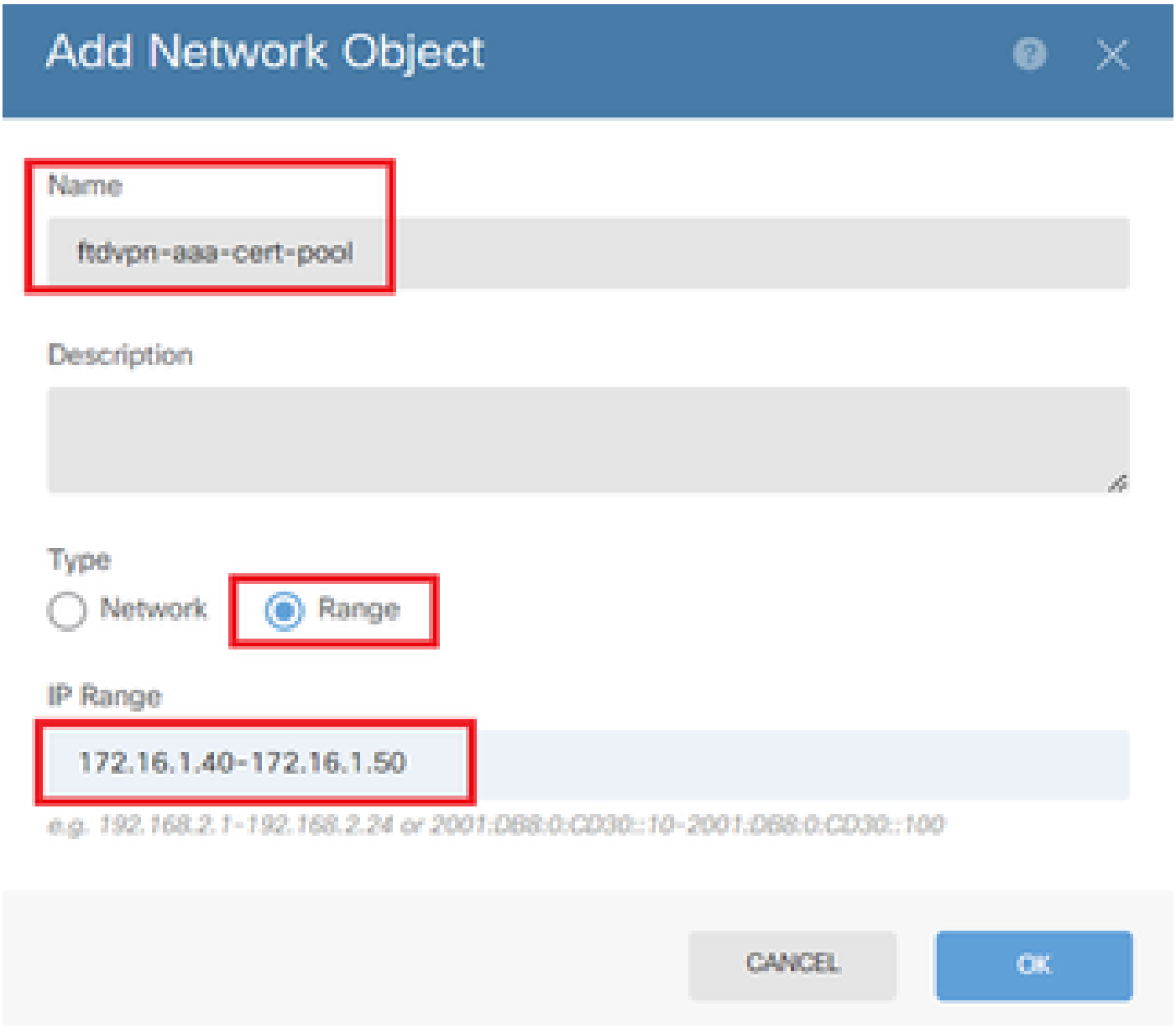


Details van VPN-verbindingsprofiel

Stap 4. Adresgroep toevoegen voor verbindingsprofiel

Voer de benodigde informatie in om een nieuwe IPv4-adresgroep toe te voegen. Selecteer nieuwe toegevoegde IPv4-adresgroep voor een verbindingsprofiel en klik op Volgende.

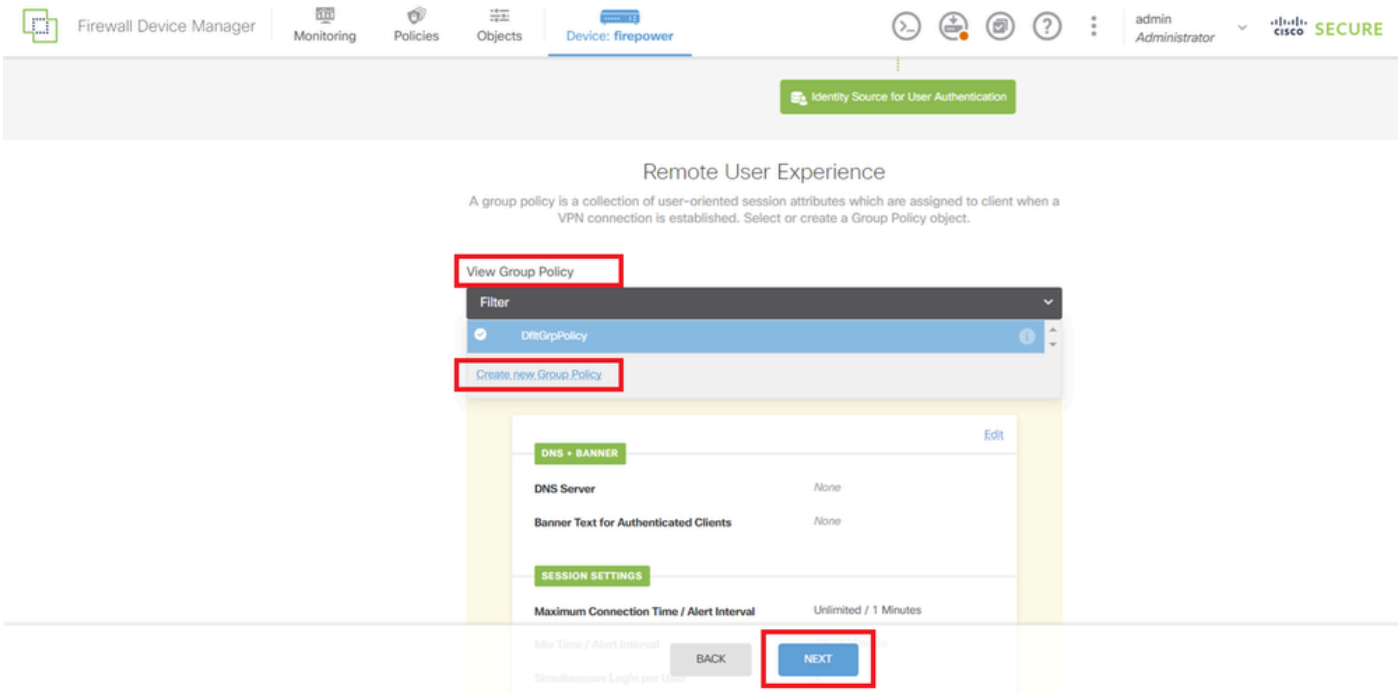
- Naam: ftdvpn-aaa-cert-pool
- Type: bereik
- IP-bereik: 172.16.1.40-172.16.1.50



Details van IPv4-adresgroep

Stap 5. Groepsbeleid toevoegen voor verbindingsprofiel

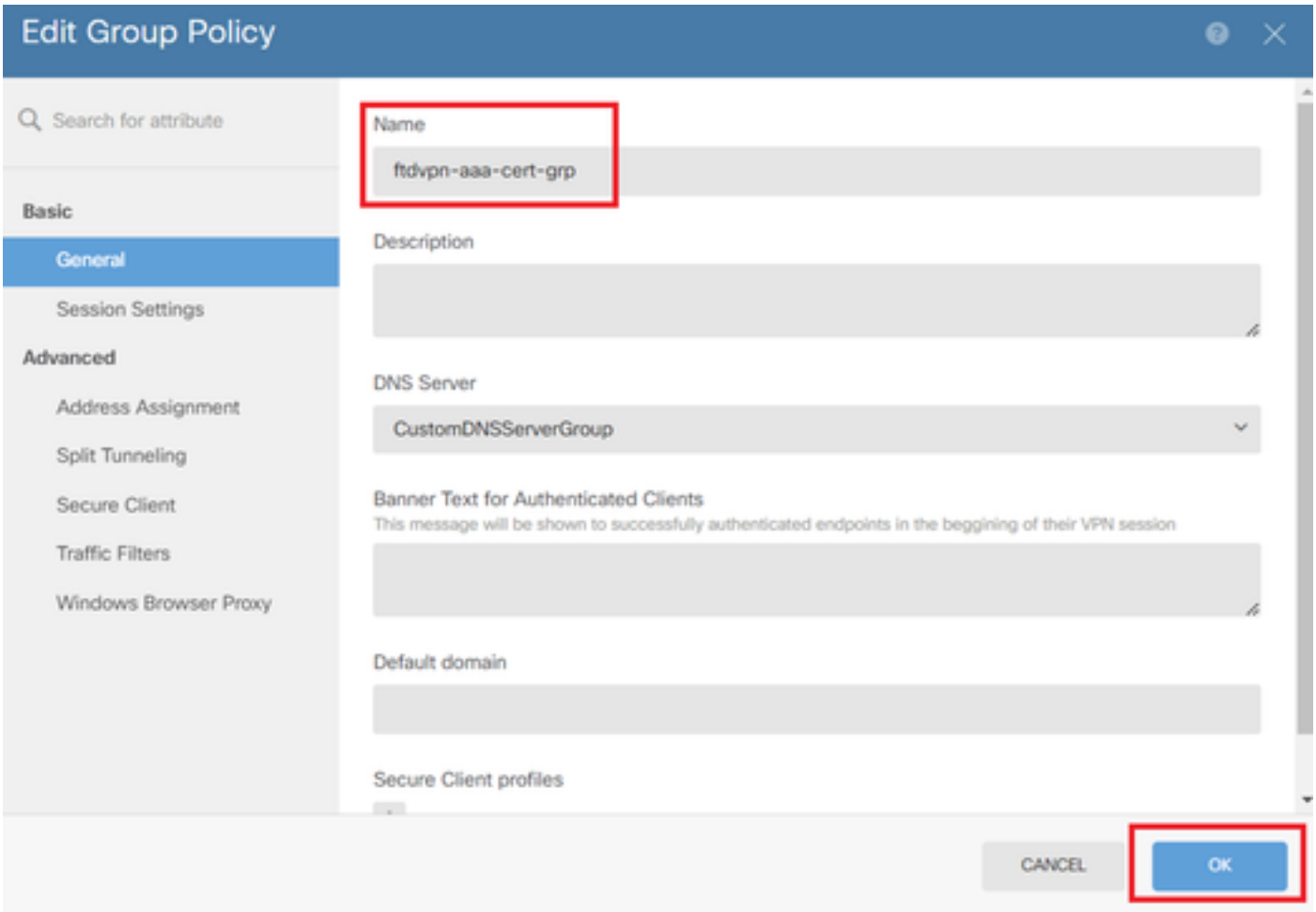
Klik op Nieuw groepsbeleid maken in de optie Groepsbeleid bekijken.



Groepsbeleid toevoegen

Voer de benodigde informatie in om een nieuw groepsbeleid toe te voegen en klik op OK. Selecteer nieuw toegevoegd groepsbeleid voor verbindingsprofiel.

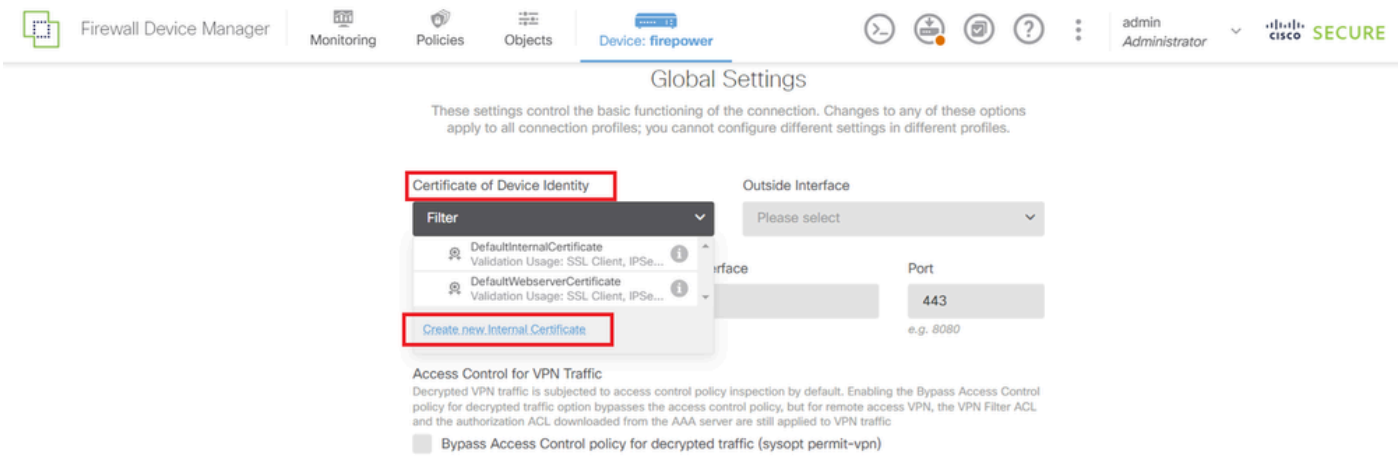
- Naam: ftdvpn-aaa-cert-grp



Details van groepsbeleid

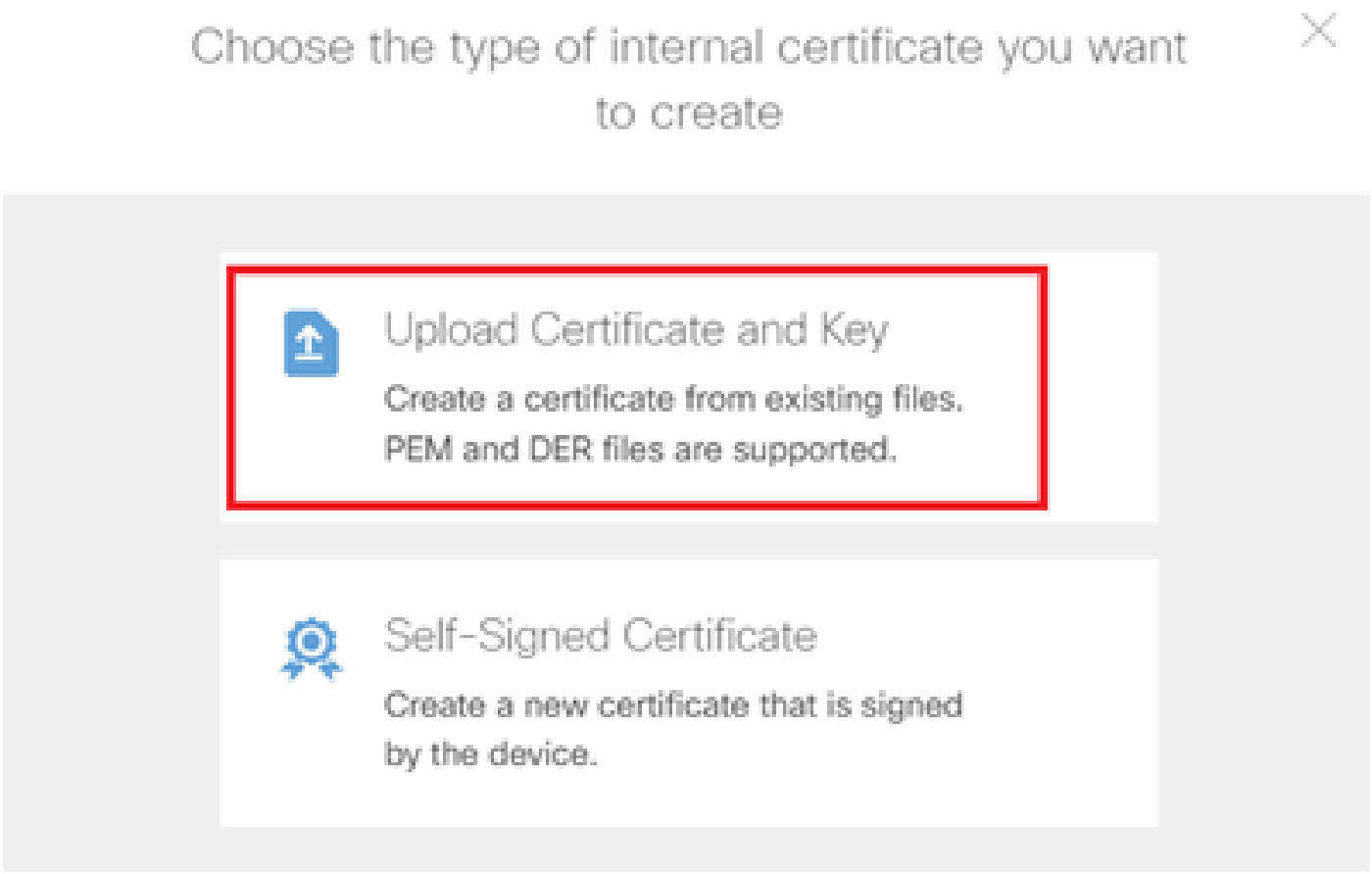
Stap 6. Certificaat van apparaatidentiteit en buiteninterface voor verbindingsprofiel configureren

Klik op Nieuw intern certificaat maken in het item Certificaat van identiteit apparaat.



Intern certificaat toevoegen

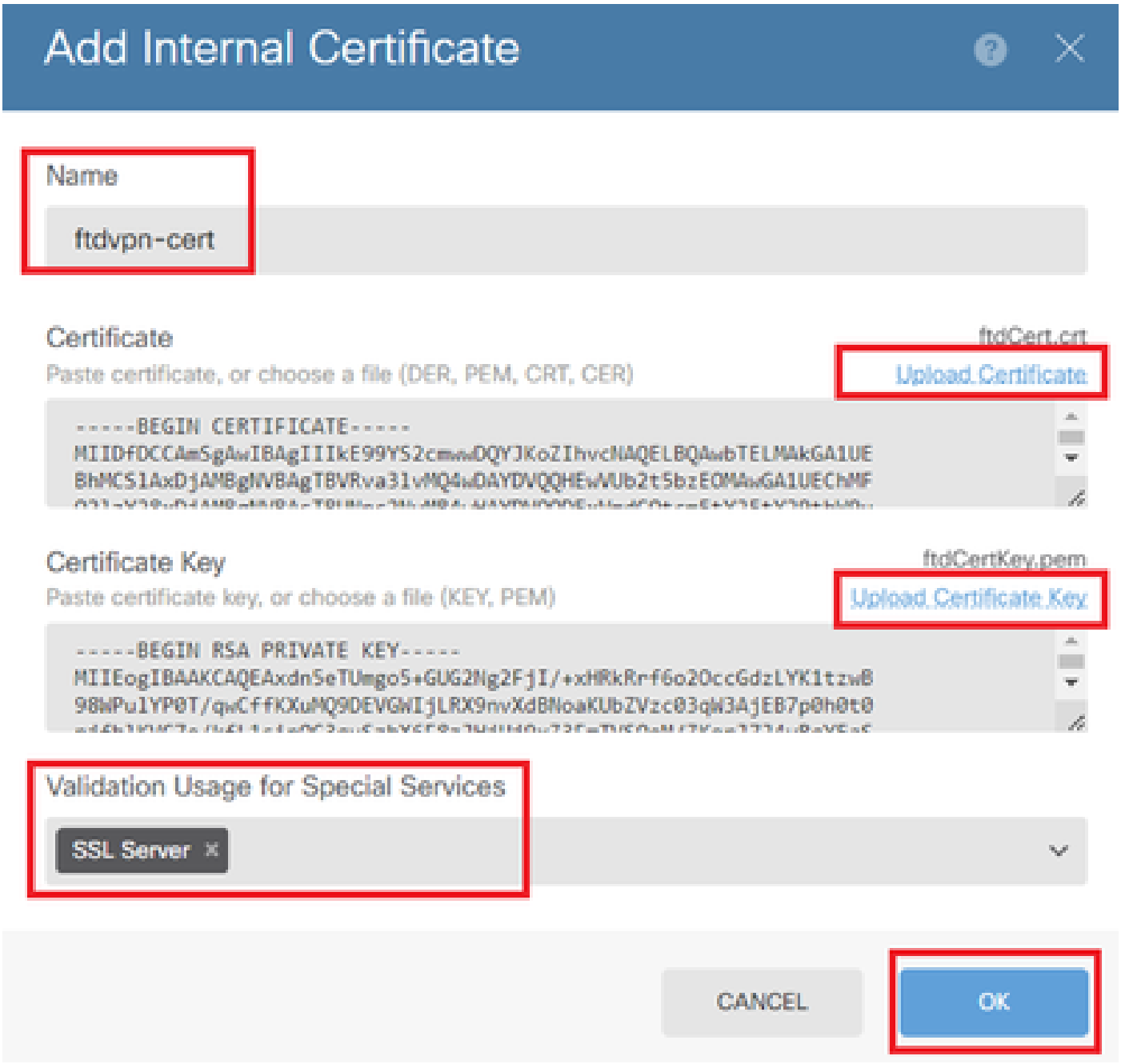
Klik op Certificaat en sleutel uploaden.



Uploadcertificaat en sleutel

Voer de benodigde informatie voor FTD-certificaat in, importeer een certificaat en een certificaatsleutel van een lokale computer en klik vervolgens op OK.

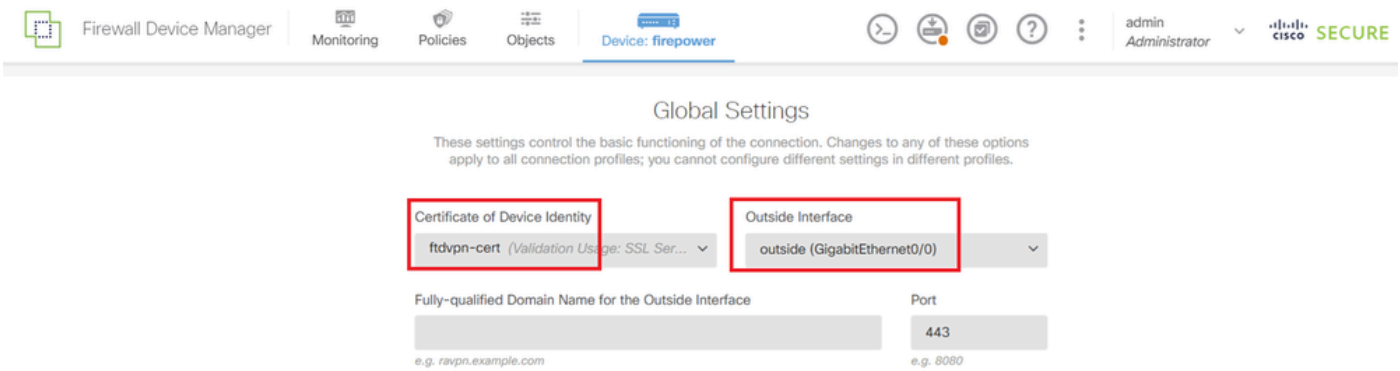
- Naam: ftdvpn-cert
- Gebruik van validatie voor speciale services: SSL-server



Gegevens van het interne certificaat

Selecteer Certificaat van Apparaatidentiteit en Buiteninterface voor VPN-verbinding.

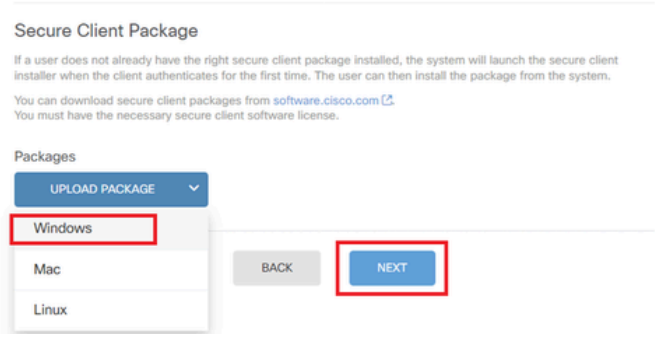
- Certificaat van Apparaatidentiteit: ftdvpn-cert
- Externe interface: buiten (Gigabit Ethernet0/0)



Details van wereldwijde instellingen

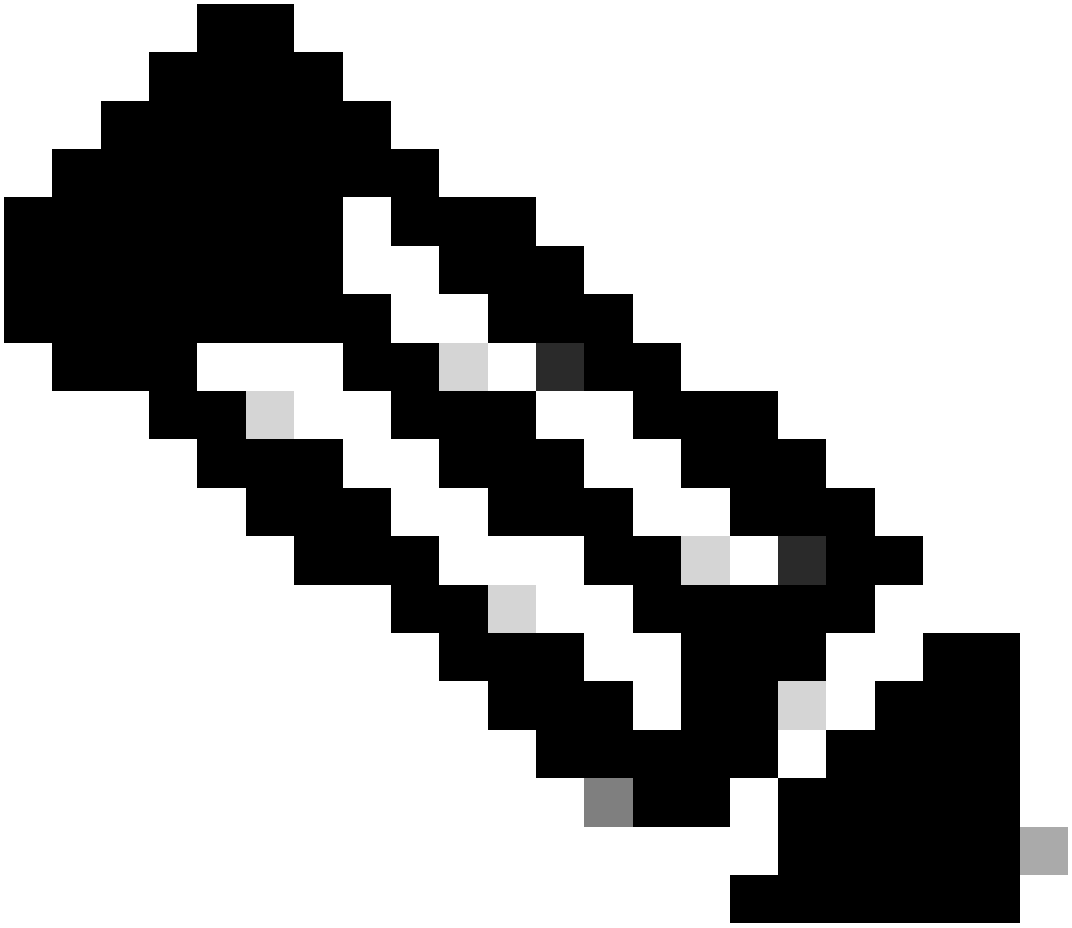
Stap 7. Beveiligde clientafbeelding voor verbindingsprofiel configureren

Selecteer Windows in het item Pakketten

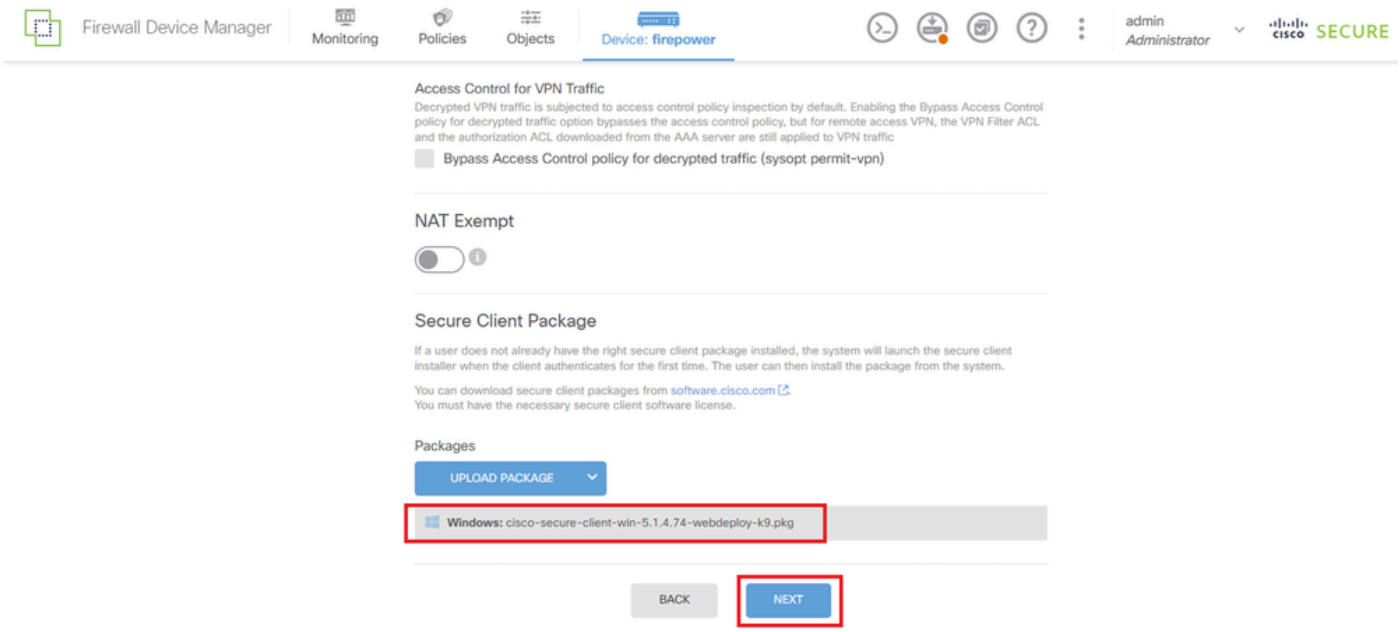


Pakket met beveiligde clientafbeeldingen uploaden

Upload een beveiligd clientbeeldbestand vanaf een lokale computer en klik op Volgende.



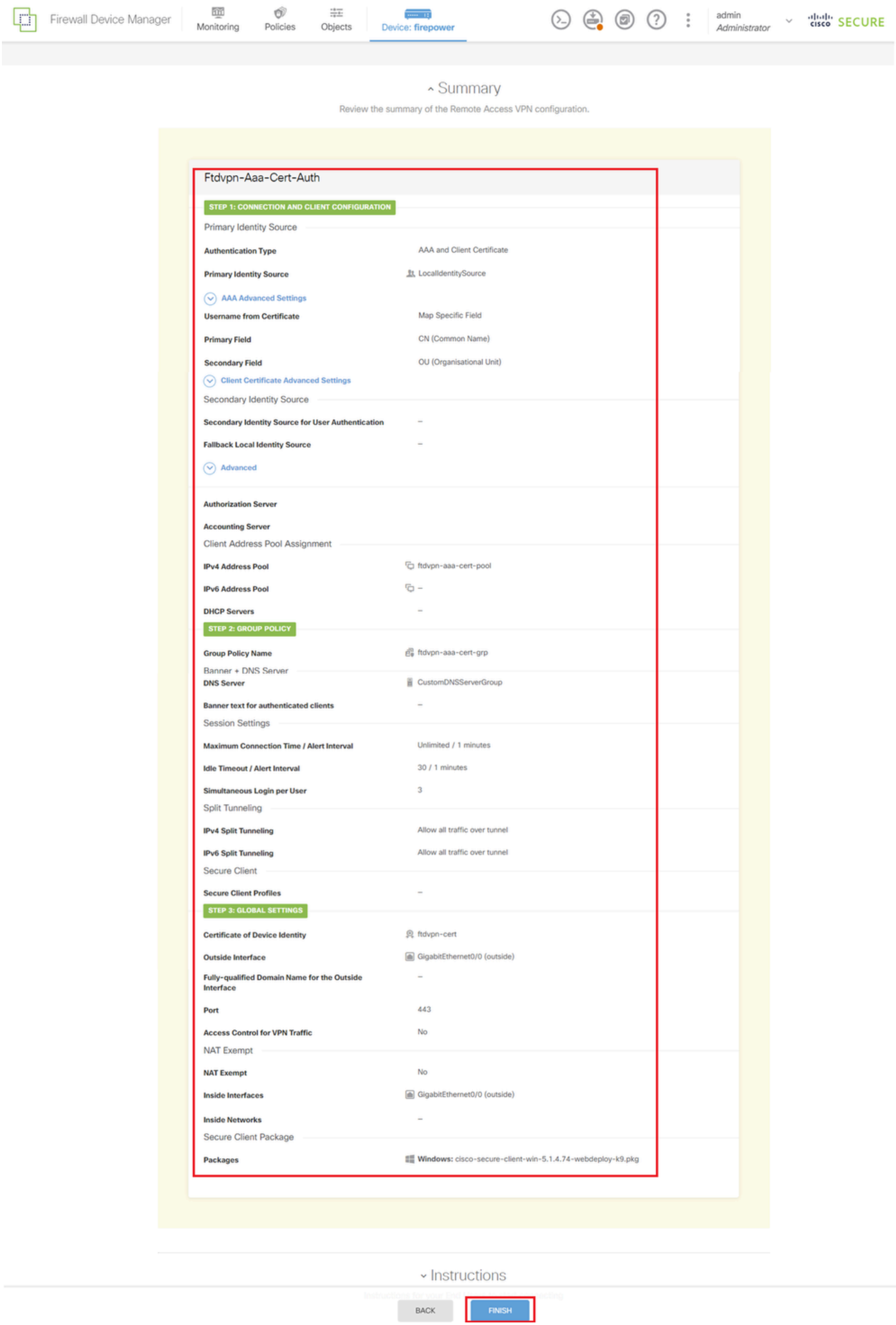
Opmerking: de functie NAT-vrijstelling is in dit document uitgeschakeld. Standaard is de optie Omzeilen van toegangscontrole voor gedecrypteerd verkeer (sysopt license-vpn) uitgeschakeld, wat betekent dat gedecrypteerd VPN-verkeer wordt onderworpen aan inspectie van het toegangscontrolebeleid.



Selecteer een beveiligd clientbeeldpakket

Stap 8. Samenvatting voor verbindingsprofiel bevestigen

Bevestig de informatie die u hebt ingevoerd voor een VPN-verbinding en klik op FINISH.



Instellingen voor verbindingsprofiel bevestigen

```
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
```

Bevestigen in VPN-client

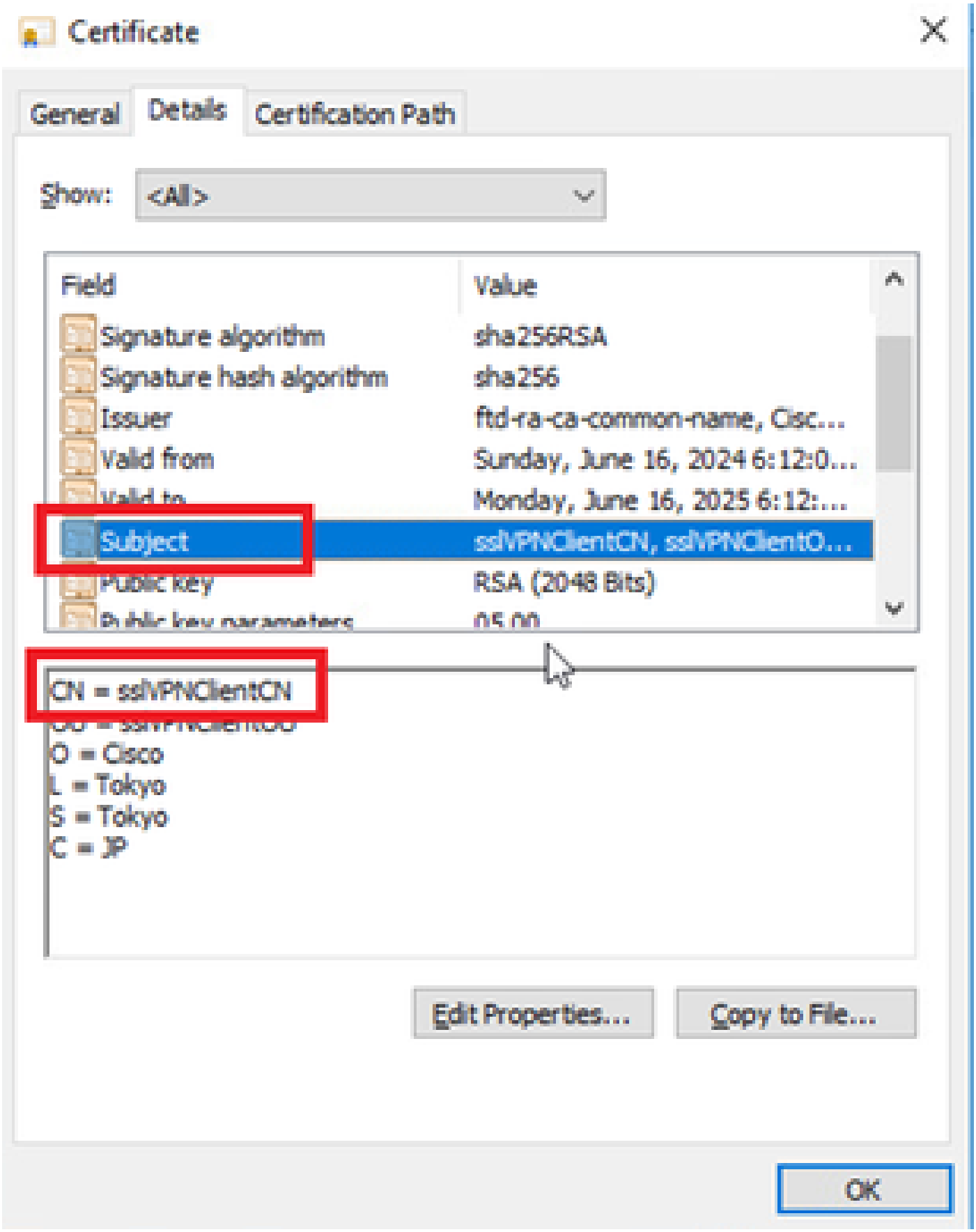
Stap 1. Clientcertificaat bevestigen

Navigeer naar certificaten - Huidige gebruiker > Persoonlijk > Certificaten, controleer het clientcertificaat dat wordt gebruikt voor verificatie.

Clientcertificaat bevestigen

Dubbelklik op het clientcertificaat, navigeer naar Details, controleer de details van Onderwerp.

- Betreft: CN = sslVPNClientCN



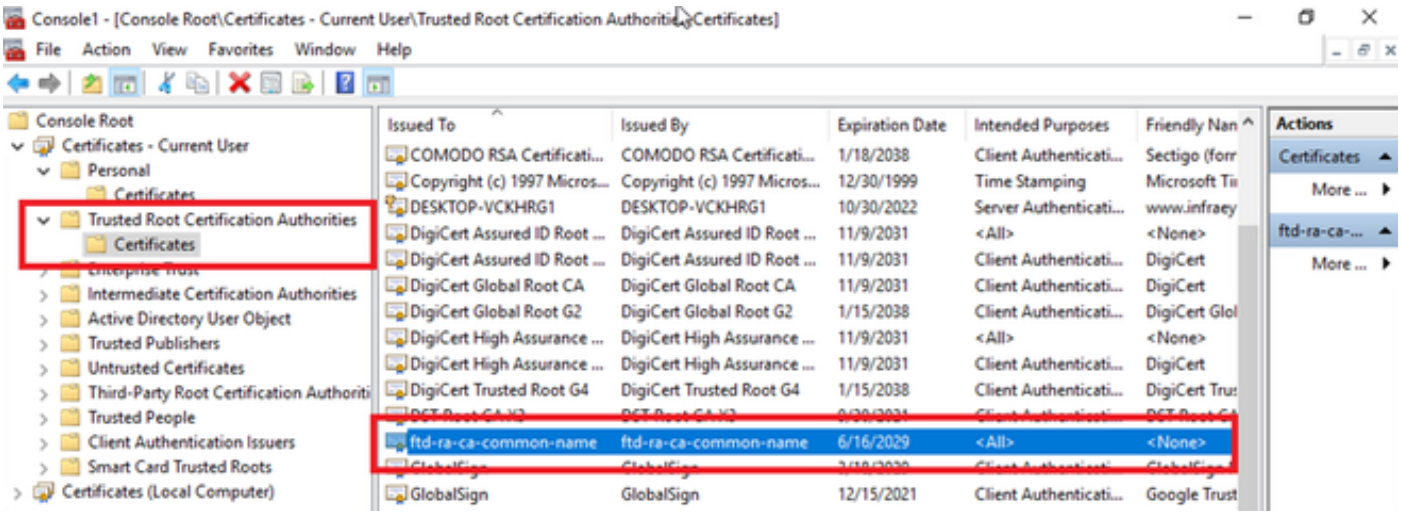
Details van clientcertificaat

Stap 2. Bevestig CA

Navigeer naar certificaten - huidige gebruiker > Trusted Root-certificeringsinstanties > Certificaten,

controleer de certificeringsinstantie die wordt gebruikt voor verificatie.

- Afgegeven door: ftd-ra-ca-common-name

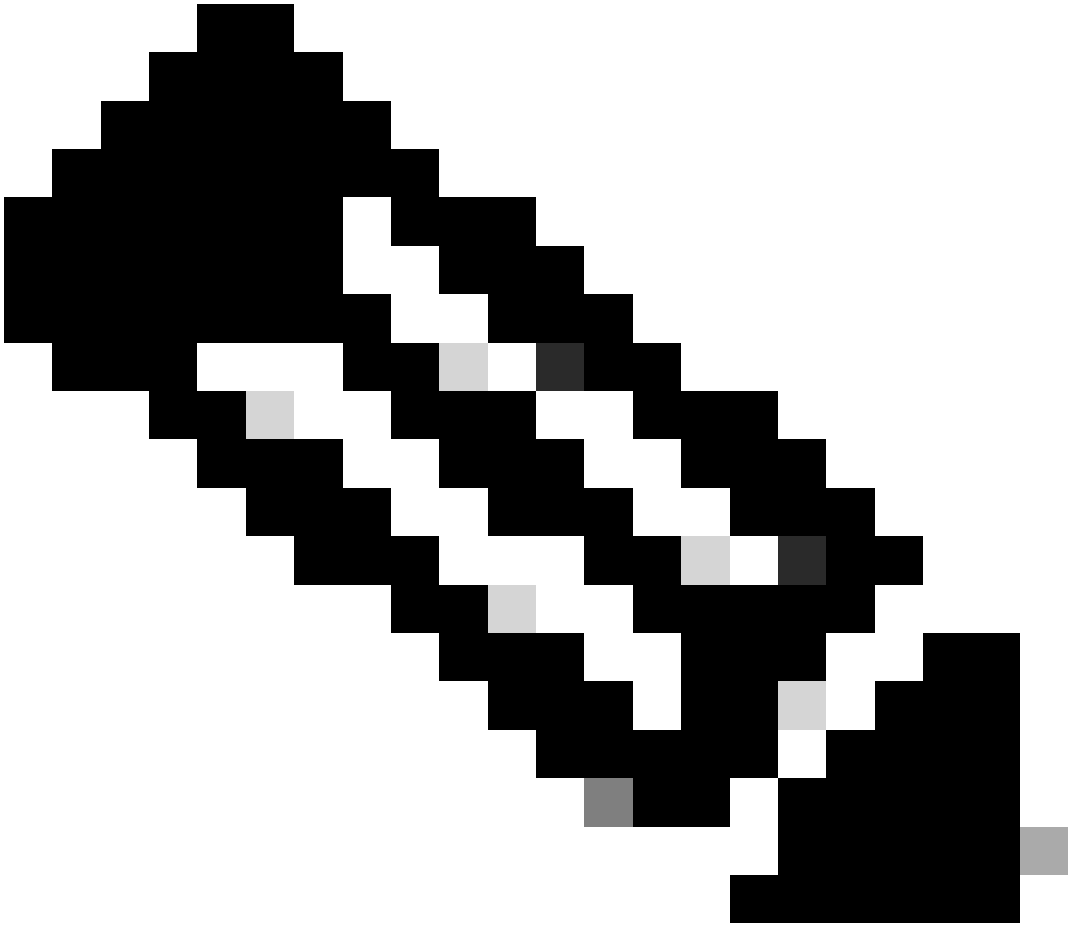


Bevestig CA

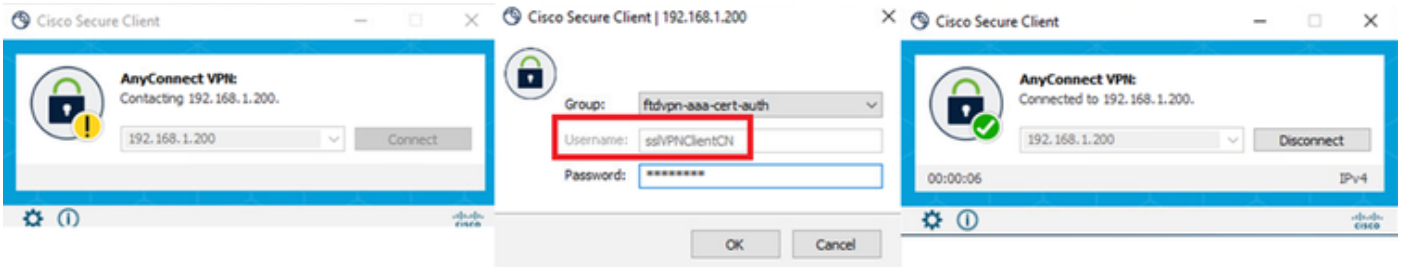
Verifiëren

Stap 1. VPN-verbinding starten

Start op het eindpunt de Cisco Secure Client-verbinding. De gebruikersnaam is afgeleid uit het clientcertificaat, u moet het wachtwoord invoeren voor VPN-verificatie.



Opmerking: De gebruikersnaam is afgeleid uit het veld Common Name (CN) van het clientcertificaat in dit document.



VPN-verbinding starten

Stap 2. VPN-sessie in FTD CLI bevestigen

Startshow vpn-sessiondb detail anyconnect de opdracht in FTD (Lina) CLI om de VPN-sessie te bevestigen.

```
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

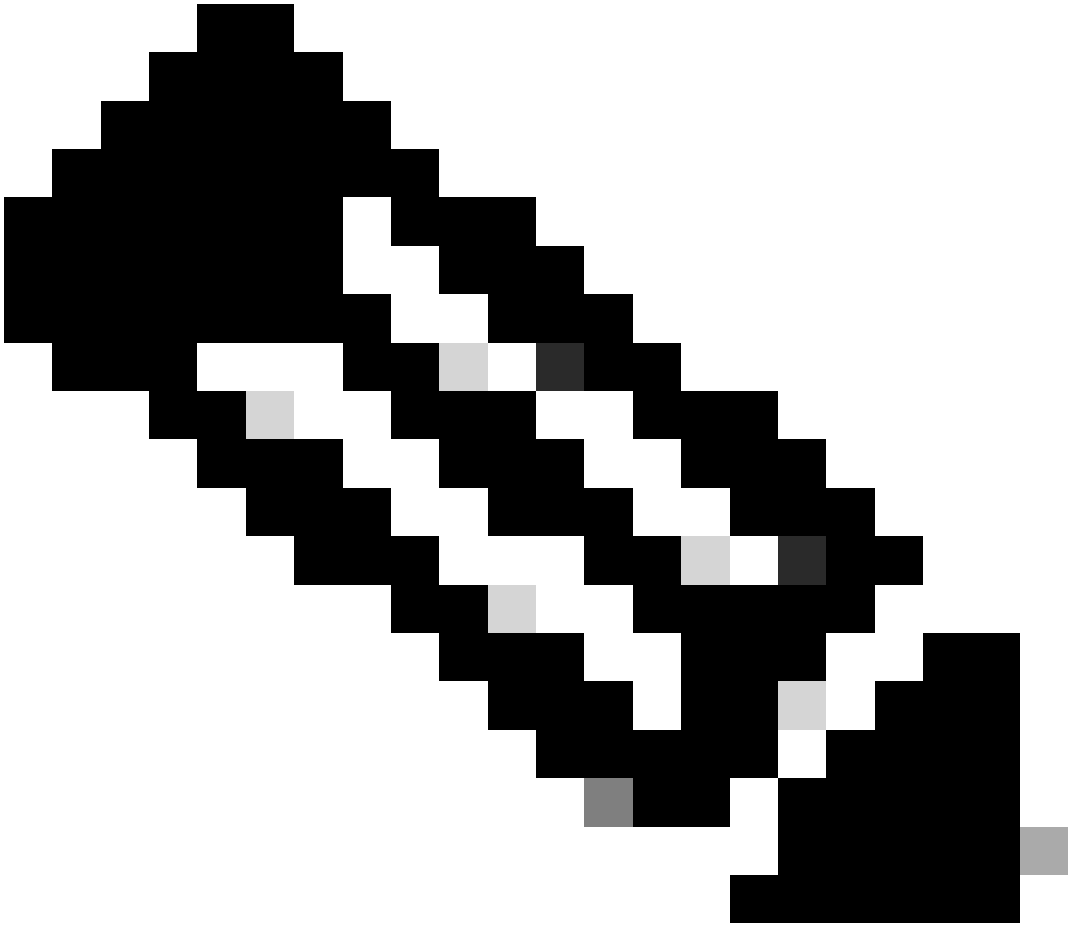
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1

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

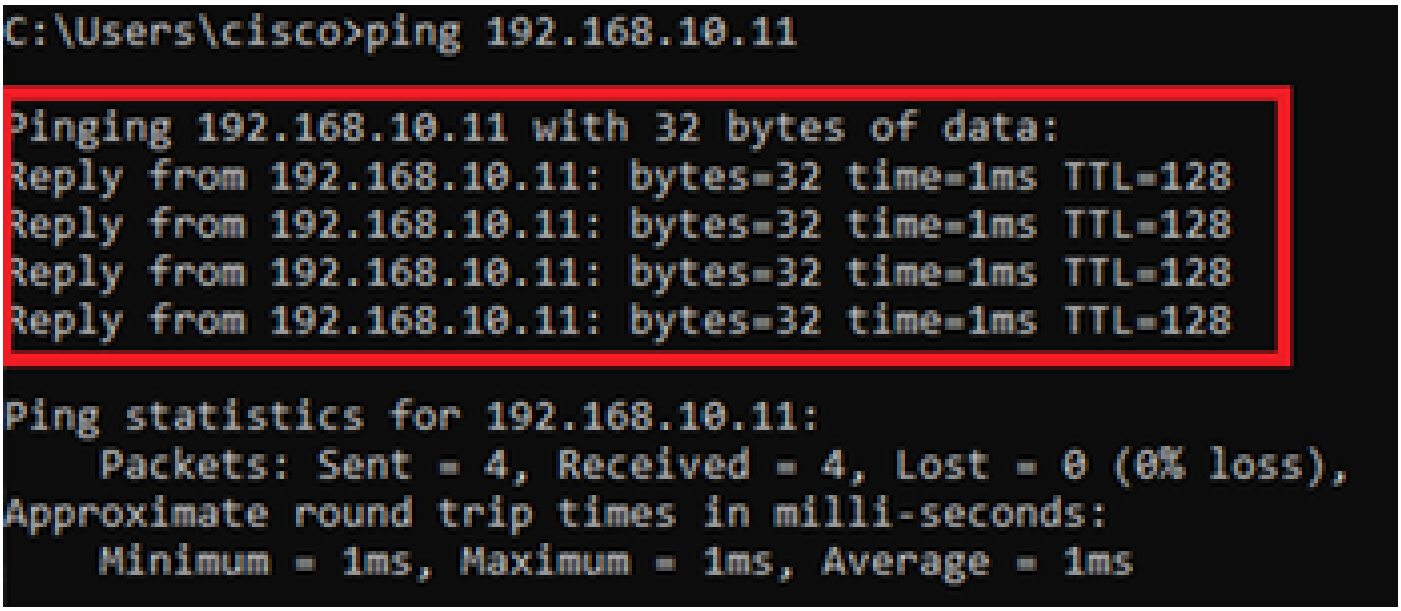
SSL-Tunnel:
Tunnel ID : 4.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 49788
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO 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

Stap 3. Communicatie met server bevestigen

Start ping van VPN-client naar server, bevestig dat de communicatie tussen de VPN-client en de server succesvol is.



Opmerking: omdat de optie Omzeilen van toegangscontrole voor gedecrypteerd verkeer (sysopt license-vpn) in stap 7 is uitgeschakeld, moet u toegangscontroleregels maken die uw IPv4-adrespool toegang tot de server geven.



Pingen gelukt

capture in interface inside real-timeRunopdracht in FTD (Lina) CLI om pakketopname te bevestigen.

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

Problemen oplossen

U kunt informatie over VPN-verificatie verwachten in de debug-syslog van Lina engine en in het DART-bestand op Windows-computer.

Dit is een voorbeeld van debug logs in de Lina engine.

// 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

Deze debugs kunnen worden uitgevoerd vanaf de diagnostische CLI van de FTD, die informatie biedt die u kunt gebruiken om problemen op te lossen met uw configuratie.

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

Gerelateerde informatie

FDM On-Box Management Service configureren voor Firepower 2100

Remote Access VPN configureren op FTD beheerde via FDM

Syslog configureren en controleren in Firepower Device Manager

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.