Circuit matching voor beveiligde clientautorisatie op FTD via FDM configureren

Inhoud

Inleiding

Dit document beschrijft hoe u Cisco Secure Client met SSL op FTD via FDM kunt instellen met behulp van certificaatmatching voor verificatie.

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
- Profieleditor (Windows) 5.1.4.74

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

CertificateMatch is een functie waarmee beheerders criteria kunnen configureren die de client moet gebruiken om een clientcertificaat te selecteren voor verificatie met de VPN-server. Deze configuratie wordt gespecificeerd in het clientprofiel, dat een XML-bestand is dat kan worden beheerd met de profieleditor of handmatig kan worden bewerkt. De optie CertificateMatch kan worden gebruikt om de beveiliging van VPN-verbindingen te verbeteren door ervoor te zorgen dat alleen een certificaat met specifieke kenmerken wordt gebruikt voor de VPN-verbinding.

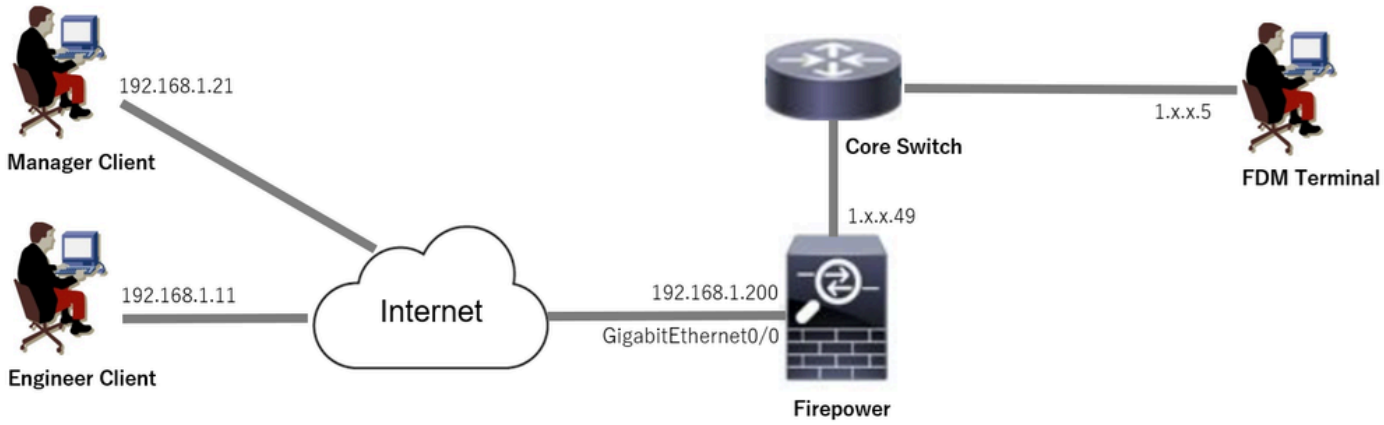
Dit document beschrijft hoe u de Cisco Secure Client kunt verifiëren met behulp van de algemene naam van een SSL-certificaat.

In deze certificaten staat een gemeenschappelijke benaming, die voor vergunningsdoeleinden wordt gebruikt.

- CA: ftd-ra-ca-common-name
- Engineer VPN Clientcertificaat: vpnEngineerClientCN
- VPN-clientcertificaat voor Manager: vpnManagerClientCN
- 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

Navigeer naar apparaat > Interfaces > Alle interfaces weergeven, configureer binnen en buiten interface voor FTD in tabblad Interfaces.

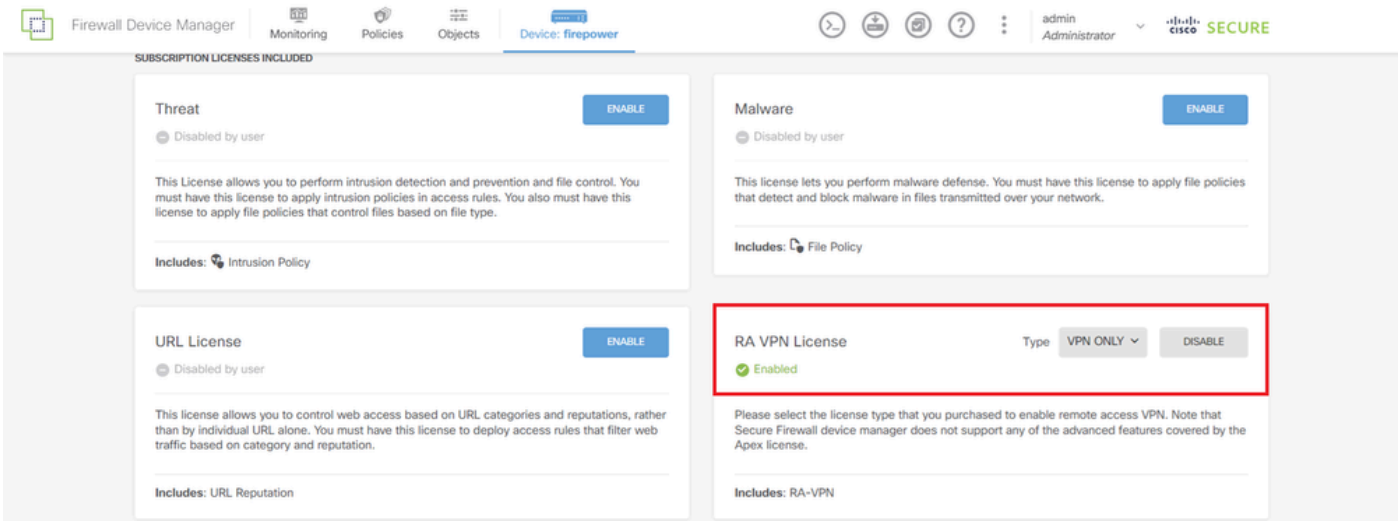
Voor Gigabit Ethernet0/0,

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

FTD-interface

Stap 2. Cisco Secure-clientlicentie bevestigen

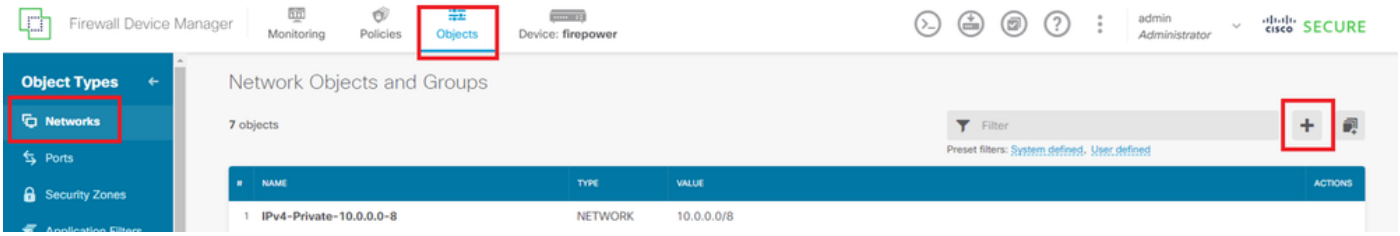
Navigeer naar apparaat > slimme licentie > Configuratie bekijken, bevestig de Cisco Secure Client-licentie in Licentie voor RA VPN.



Secure-clientlicentie

Stap 3. Adresgroep toevoegen

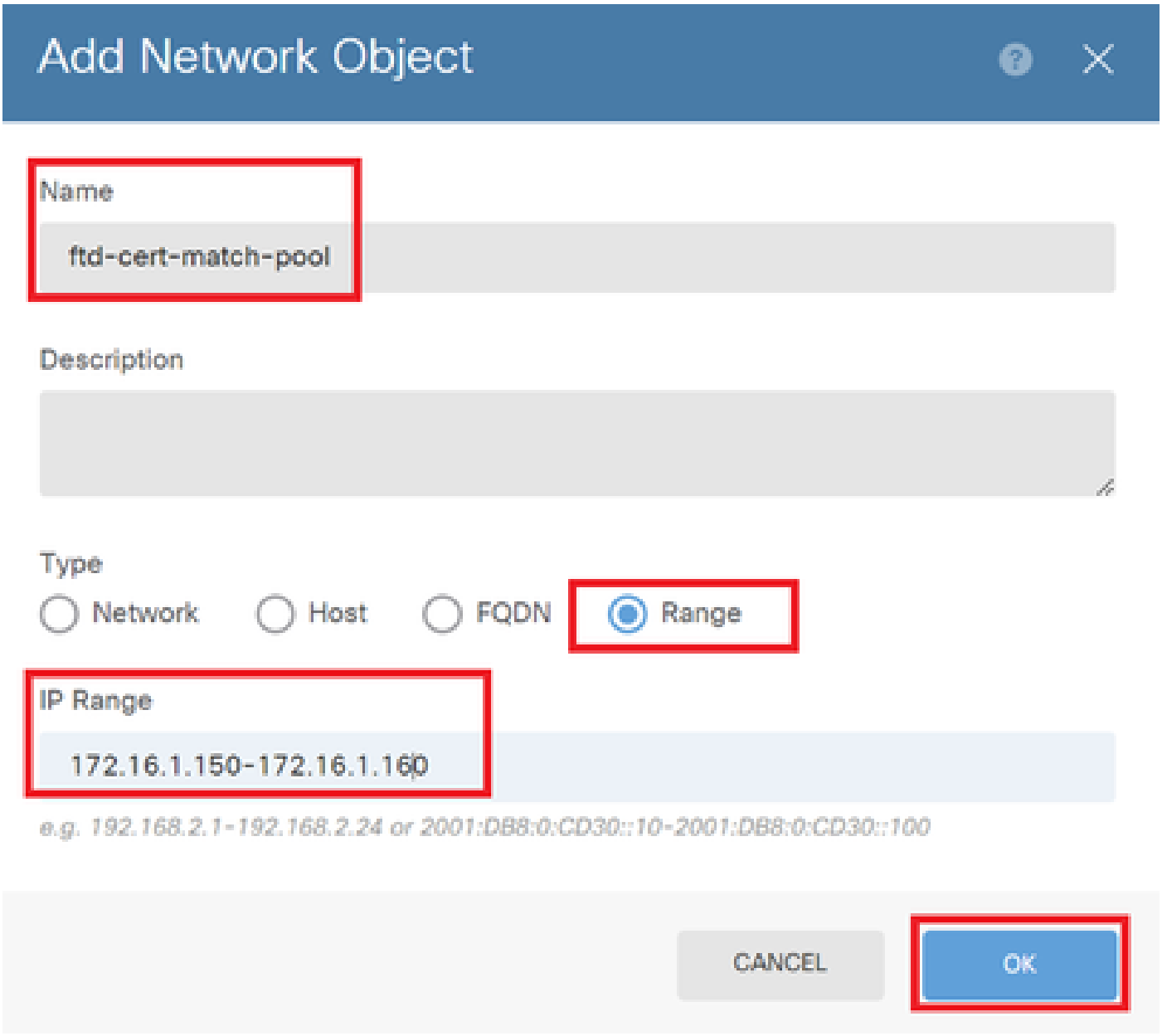
Navigeer naar Objecten > Netwerken en klik op +.



Adresgroep toevoegen

Voer de benodigde informatie in om een nieuwe IPv4-adresgroep toe te voegen. klik op OK knop.

- Naam: ftd-cert-match-pool
- Type: bereik
- IP-bereik: 172.16.1.150-172.16.1.160

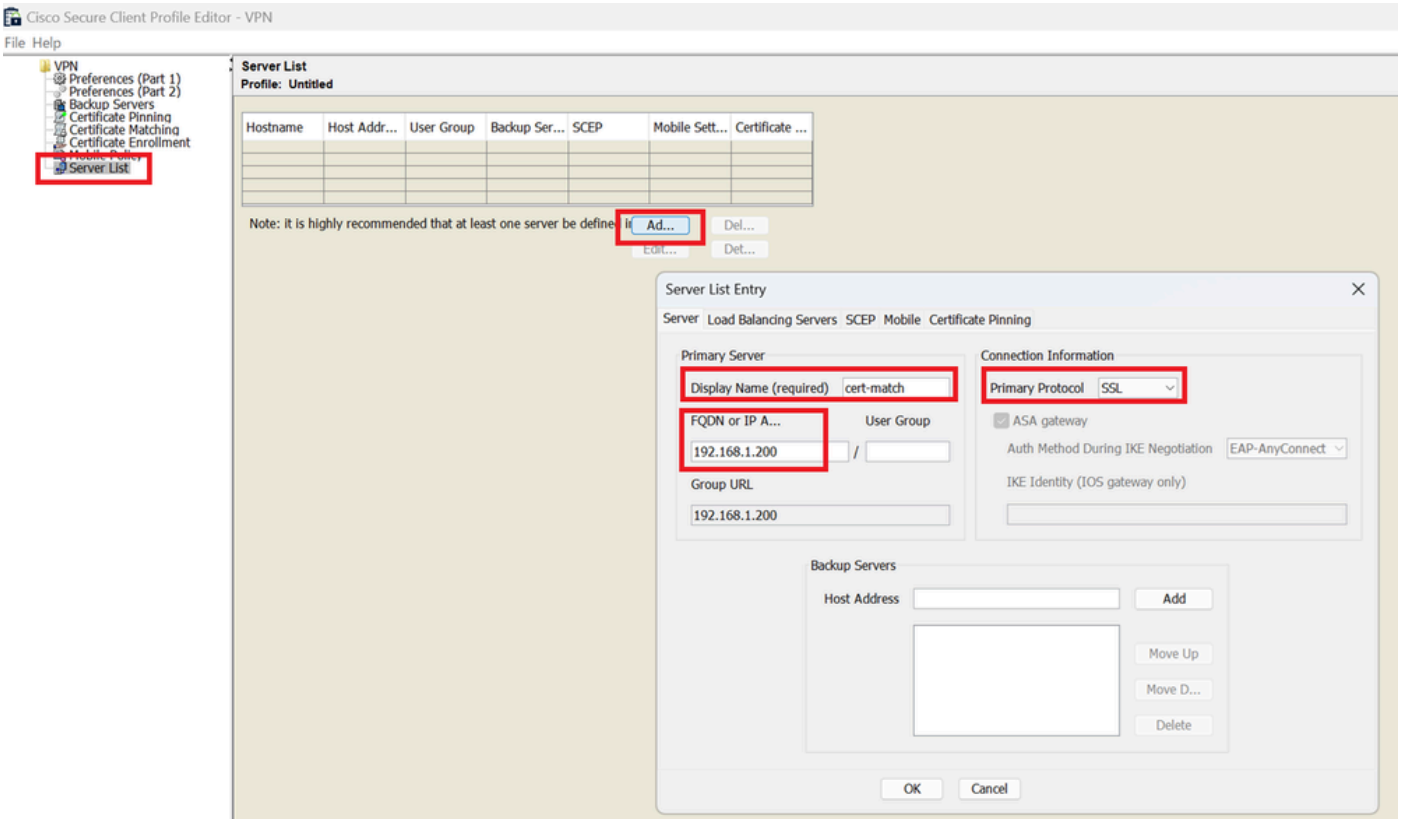


Gedetailleerde informatie over IPv4-adresgroep

Stap 4. Beveiligd clientprofiel maken

Download en installeer de Secure Client Profile Editor van de Cisco Software-site. Navigeer naar de serverlijst en klik op de knop Toevoegen. Voer de benodigde informatie in om een serverlijst toe te voegen en klik op OK.

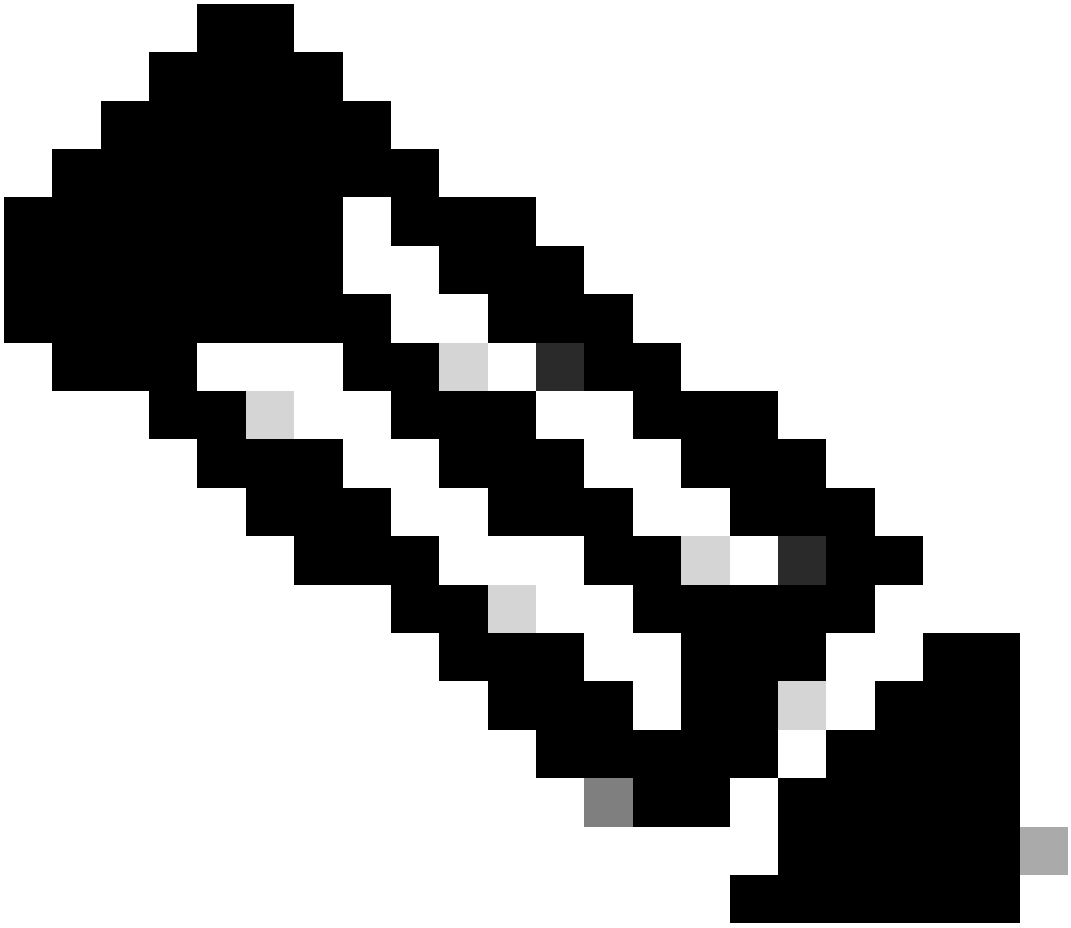
- Display Naam: cert-match
- FQDN- of IP-adres: 192.168.1.2010
- Primair protocol: SSL



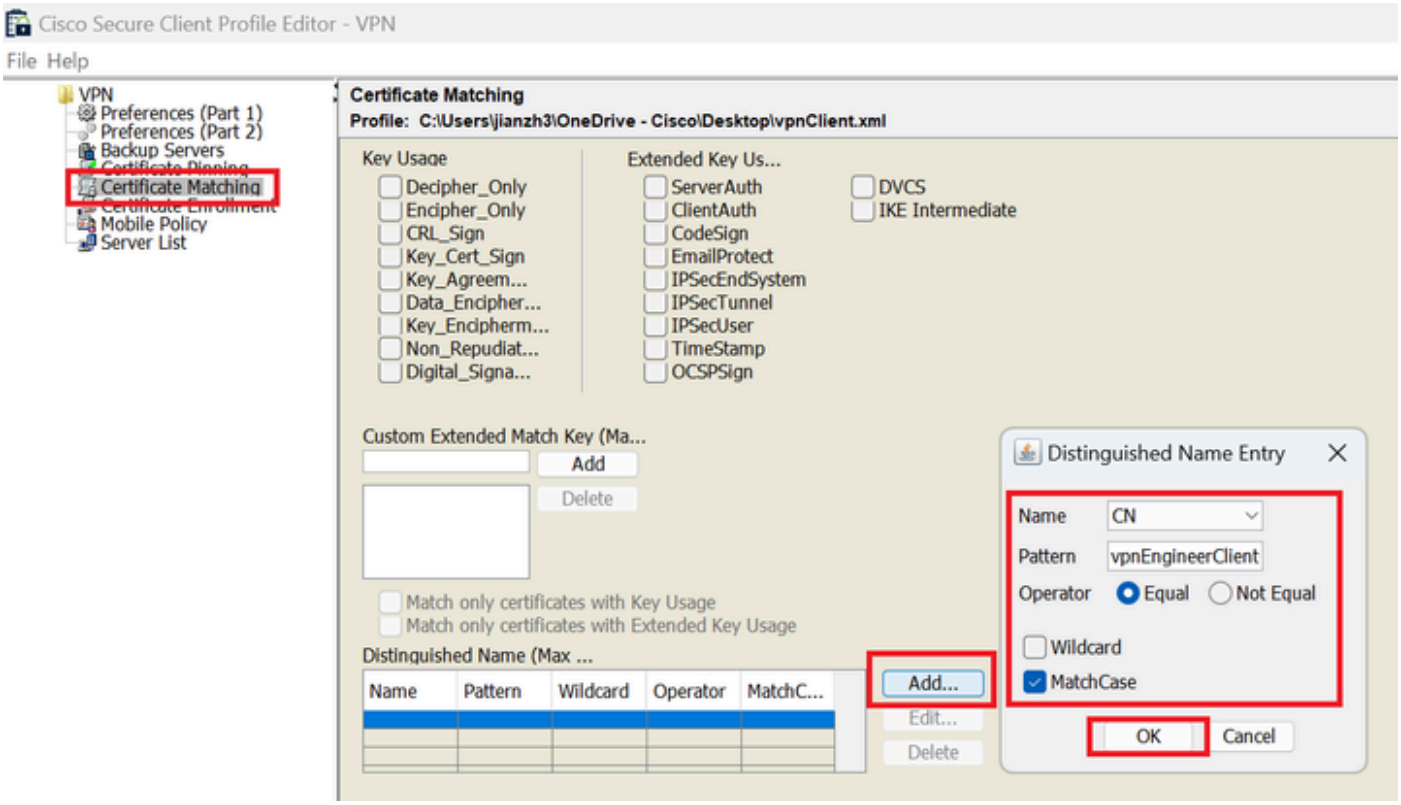
Invoer in serverlijst

Klik op de knop Toevoegen om naar Certificaat-matching te navigeren. Voer de benodigde informatie in om een onderscheidende naamvermelding toe te voegen en klik op OK.

- Naam: CN
- Patroon: vpnEngineerClientCN
- Exploitant: gelijk



Opmerking: controleer de optie MatchCase in dit document.



Benoemde naam

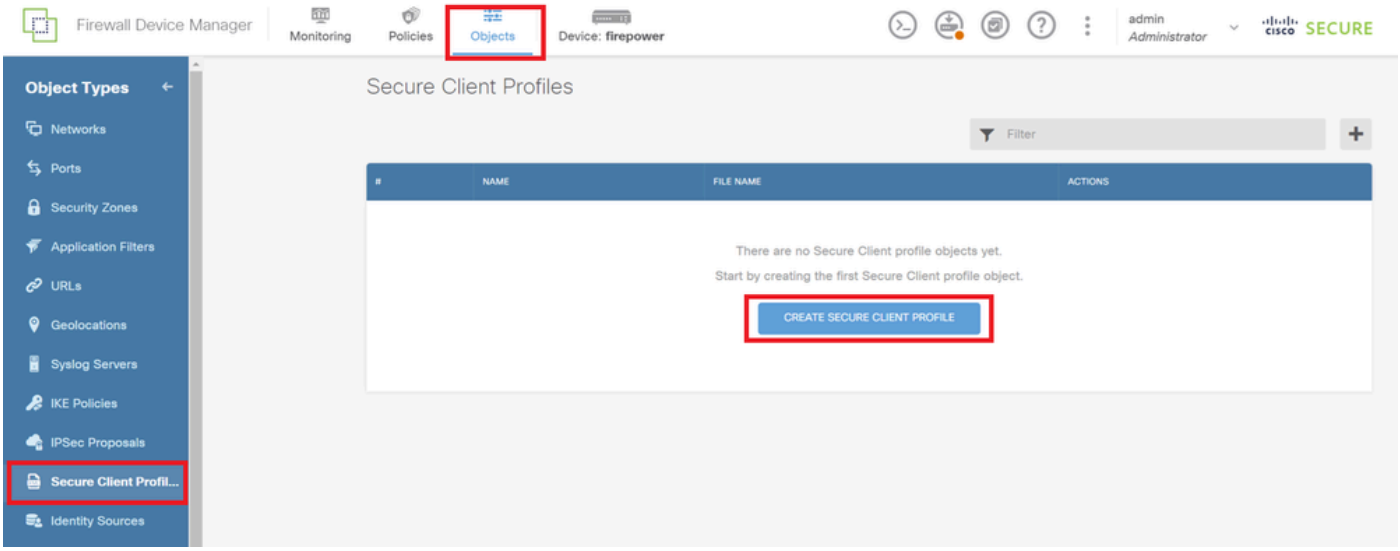
Sla het beveiligde clientprofiel op de lokale computer op en bevestig de gegevens van het profiel.

```
▼<CertificateMatch>
  <MatchOnlyCertsWithKU>false</MatchOnlyCertsWithKU>
  ▼<DistinguishedName>
    ▼<DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled" MatchCase="Enabled">
      <Name>CN</Name>
      <Pattern>vpnEngineerClientCN</Pattern>
    </DistinguishedNameDefinition>
  </DistinguishedName>
</CertificateMatch>
▼<EnableAutomaticServerSelection UserControllable="false">
  false
  <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
  <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false </RetainVpnOnLogoff>
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
▼<ServerList>
  ▼<HostEntry>
    <HostName>cert-match</HostName>
    <HostAddress>192.168.1.200</HostAddress>
  </HostEntry>
</ServerList>
</AnyConnectProfile>
```

Beveiligd clientprofiel

Stap 5. Beveiligd clientprofiel uploaden naar FDM

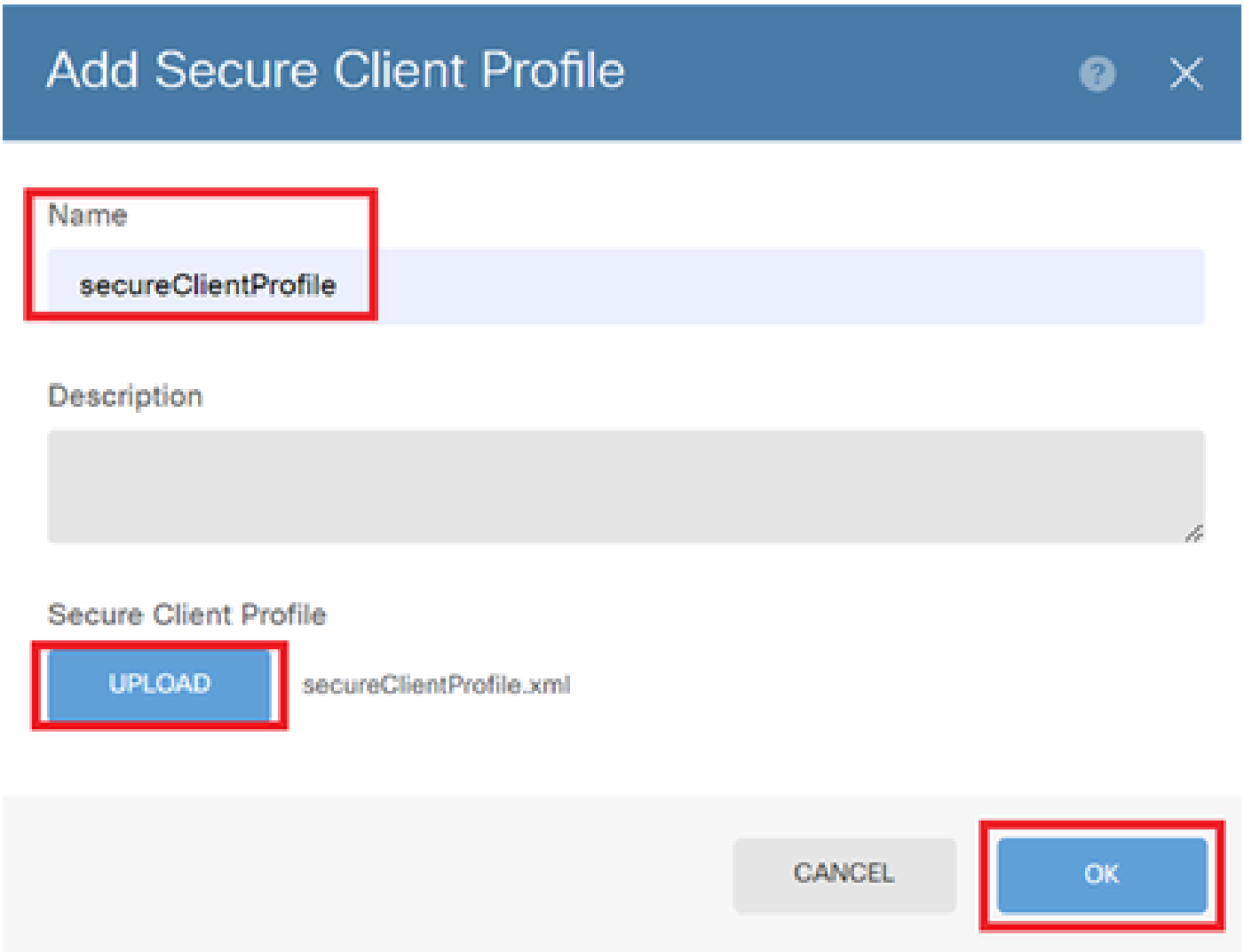
Navigeer naar Objecten > Beveiligd clientprofiel en klik op de knop BEVEILIGD CLIENTPROFIEL MAKEN.



Beveiligd clientprofiel maken

Voer de benodigde informatie in om een beveiligd clientprofiel toe te voegen en klik op OK.

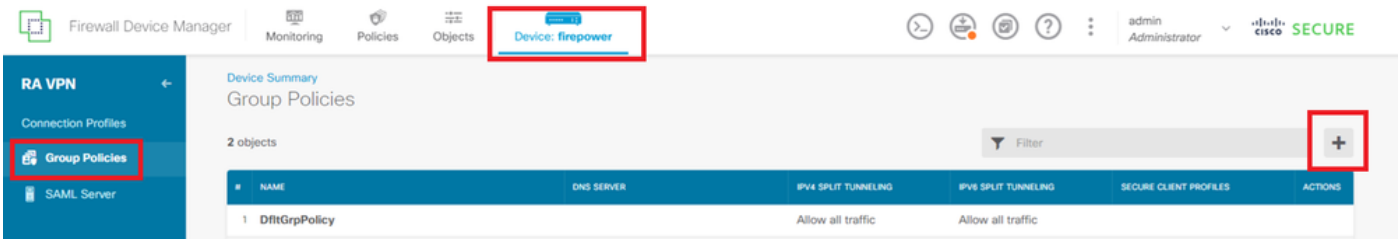
- Naam: SecureClientProfile
- Secure Client Profile: SecureClientProfile.xml (uploaden vanaf lokale computer)



Beveiligd clientprofiel toevoegen

Stap 6. Groepsbeleid toevoegen

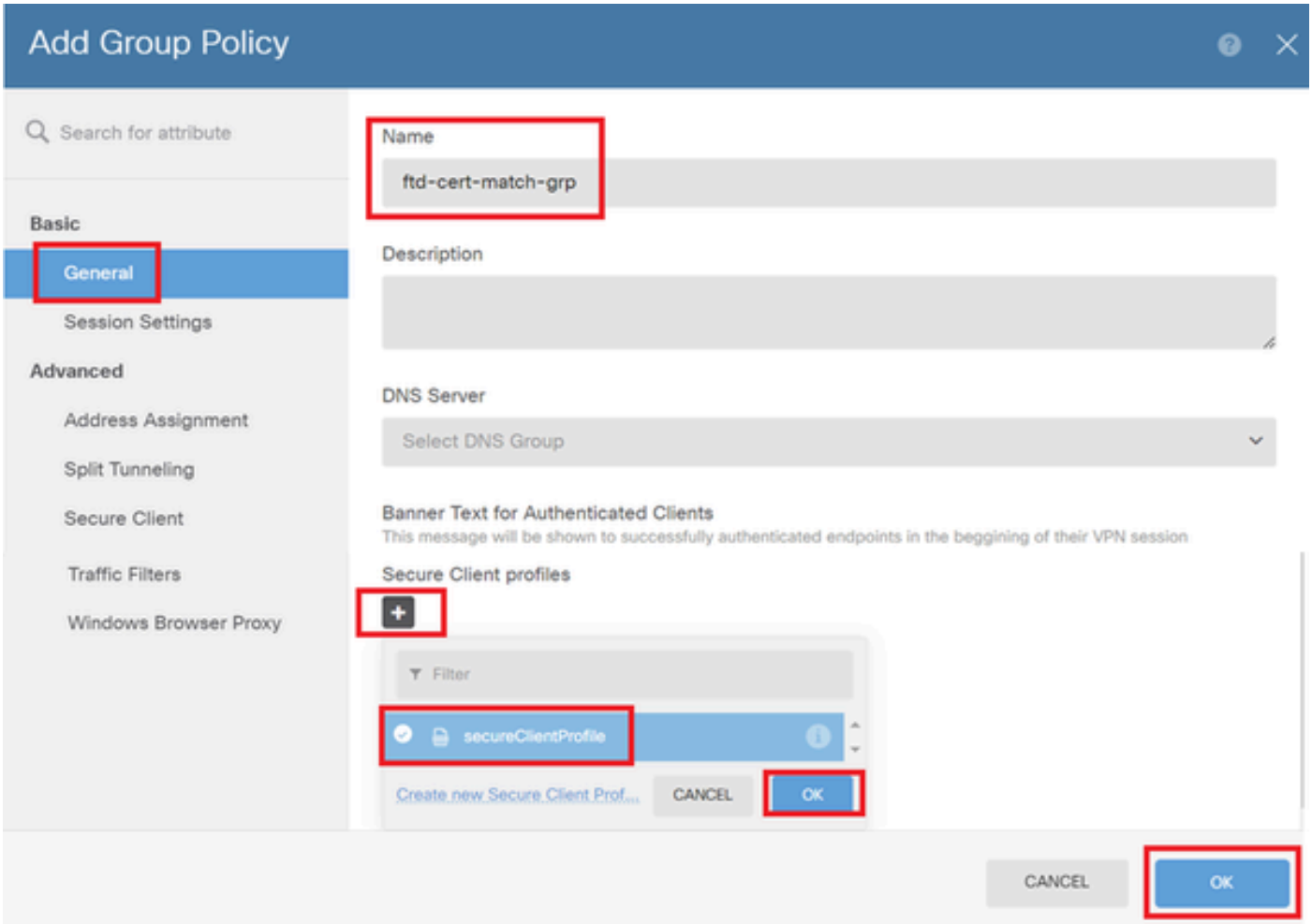
Navigeer naar Apparaat > Externe toegang VPN > Configuratie bekijken > Groepsbeleid, klik op + knop.



Groepsbeleid toevoegen

Voer de benodigde informatie in om een groepsbeleid toe te voegen en klik op OK.

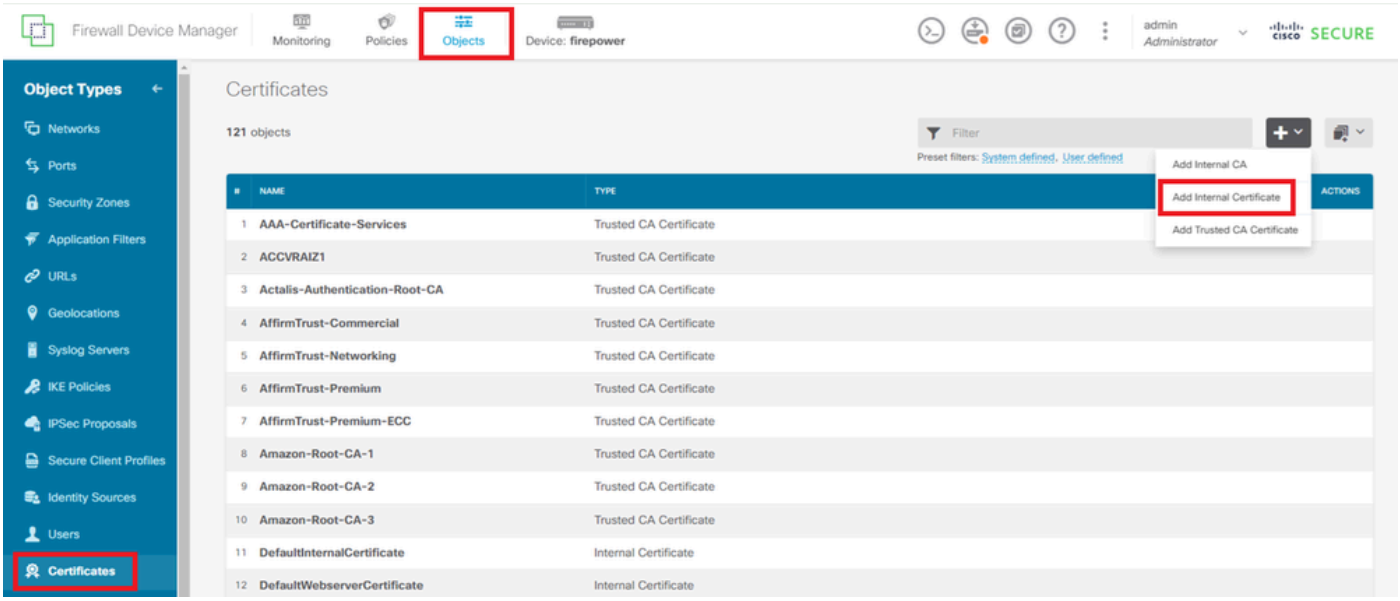
- Naam: ftd-cert-match-grp
- Beveiligde clientprofielen: beveiligdClientprofiel



Details van groepsbeleid

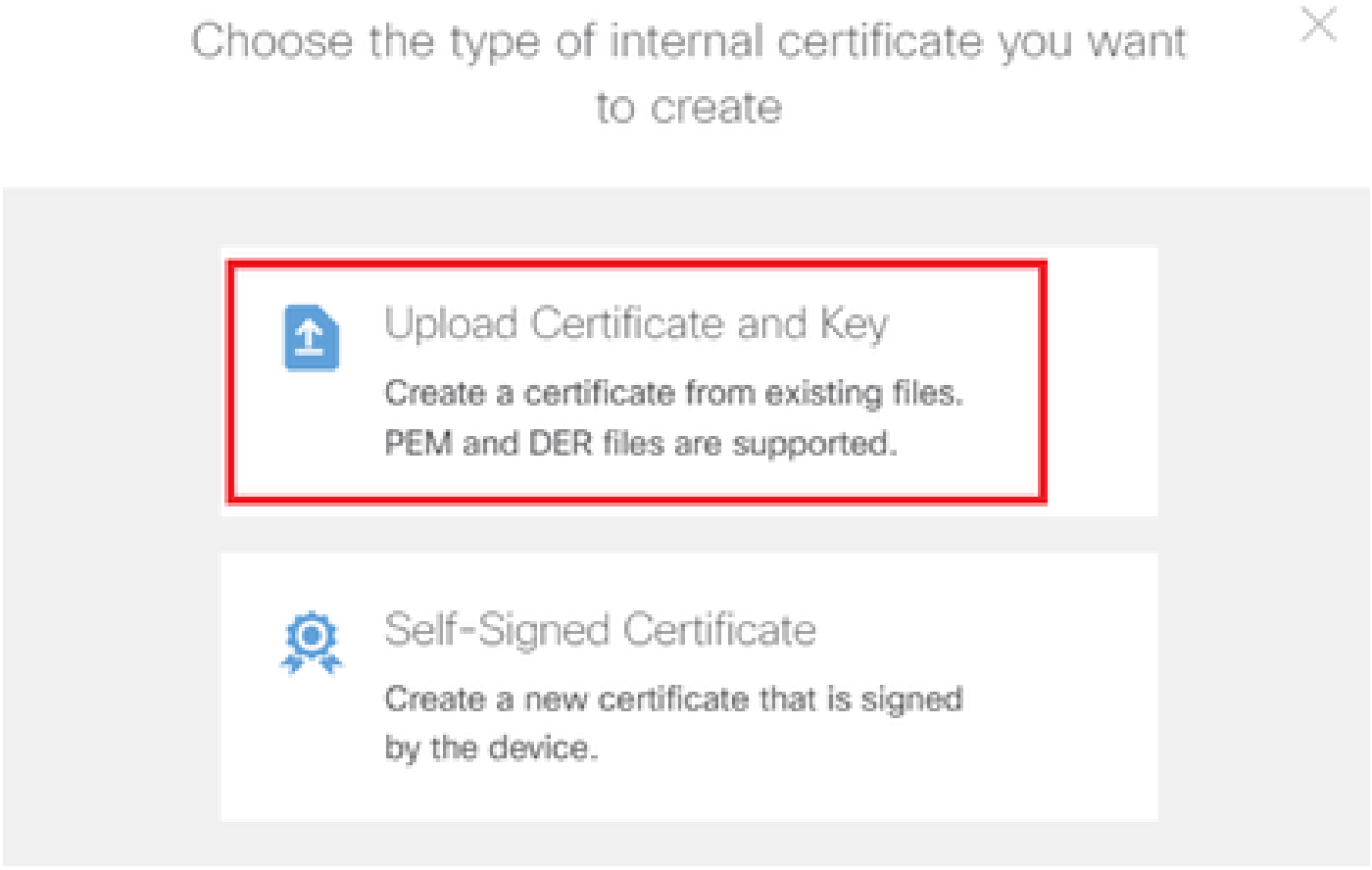
Stap 7. FTD-certificaat toevoegen

Navigeer naar Objecten > Certificaten, klik op Intern certificaat toevoegen vanuit + item.



Intern certificaat toevoegen

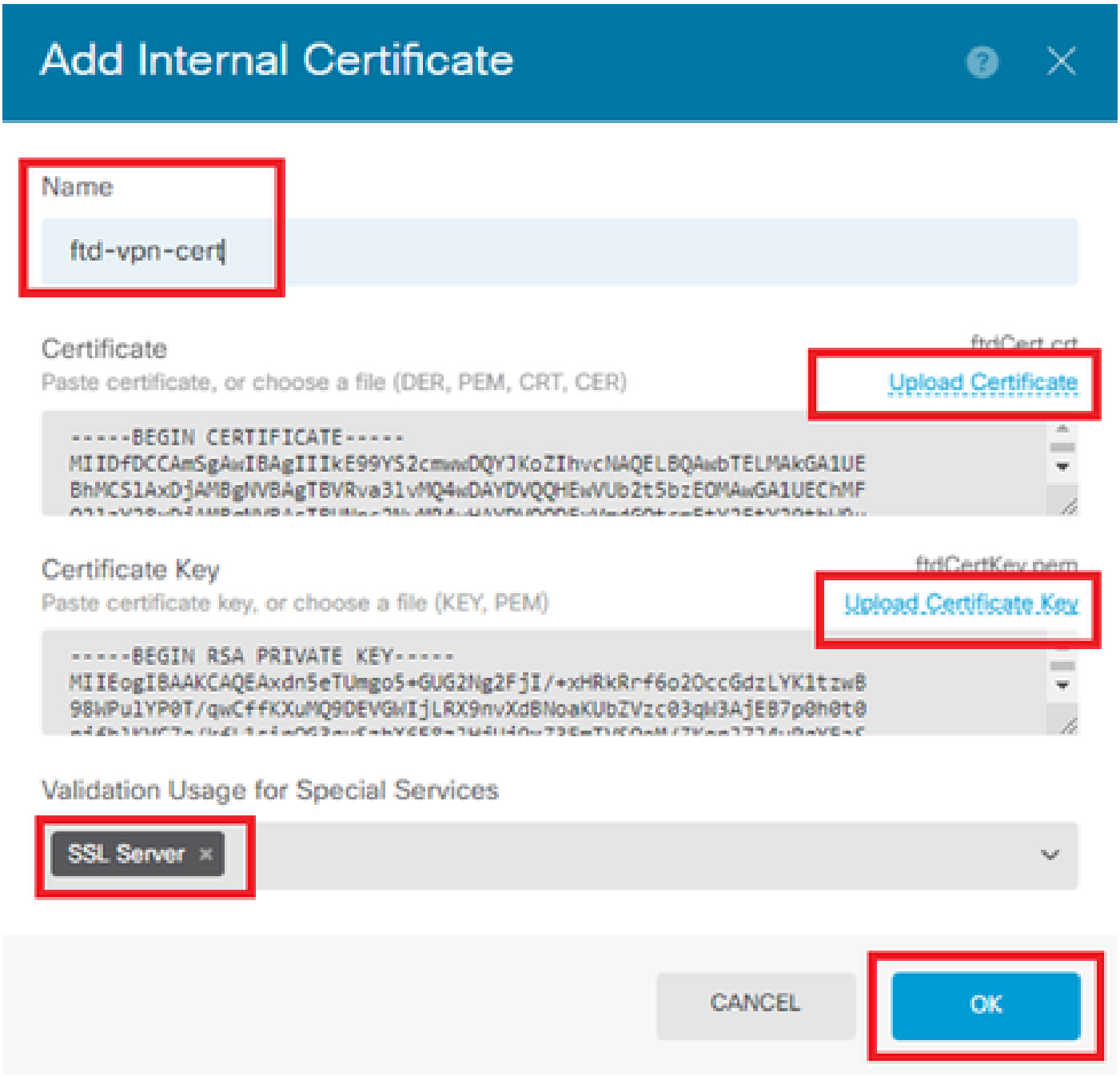
Klik op Certificaat en sleutel uploaden.



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.

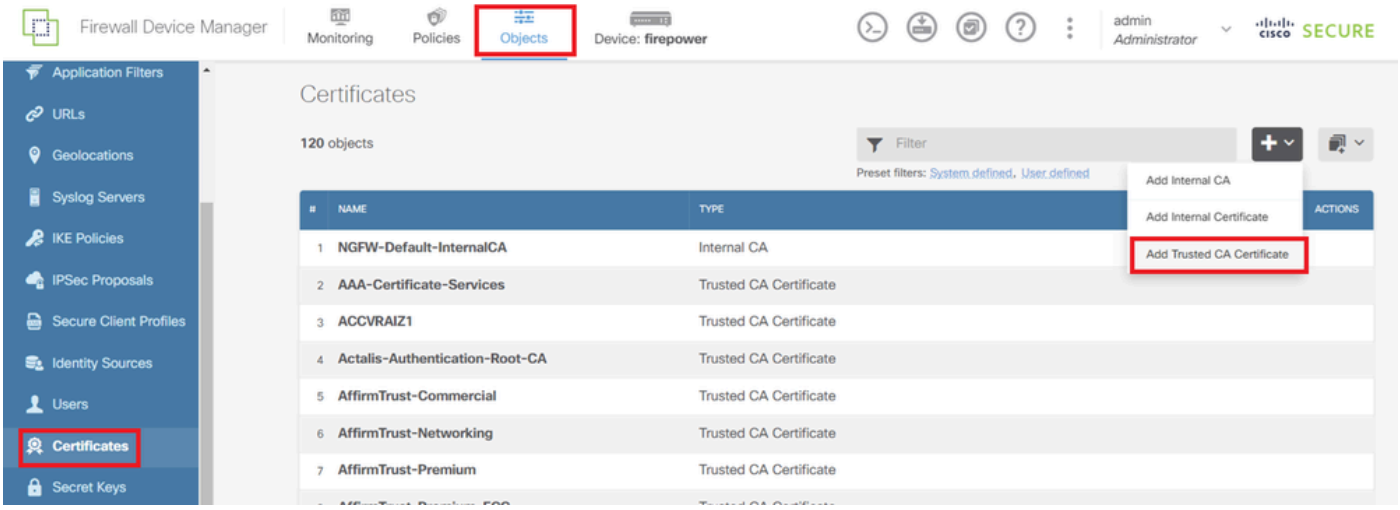
- Naam: ftd-vpn-cert
- Gebruik van validatie voor speciale services: SSL-server



Gegevens van het interne certificaat

Stap 8. CA aan FTD toevoegen

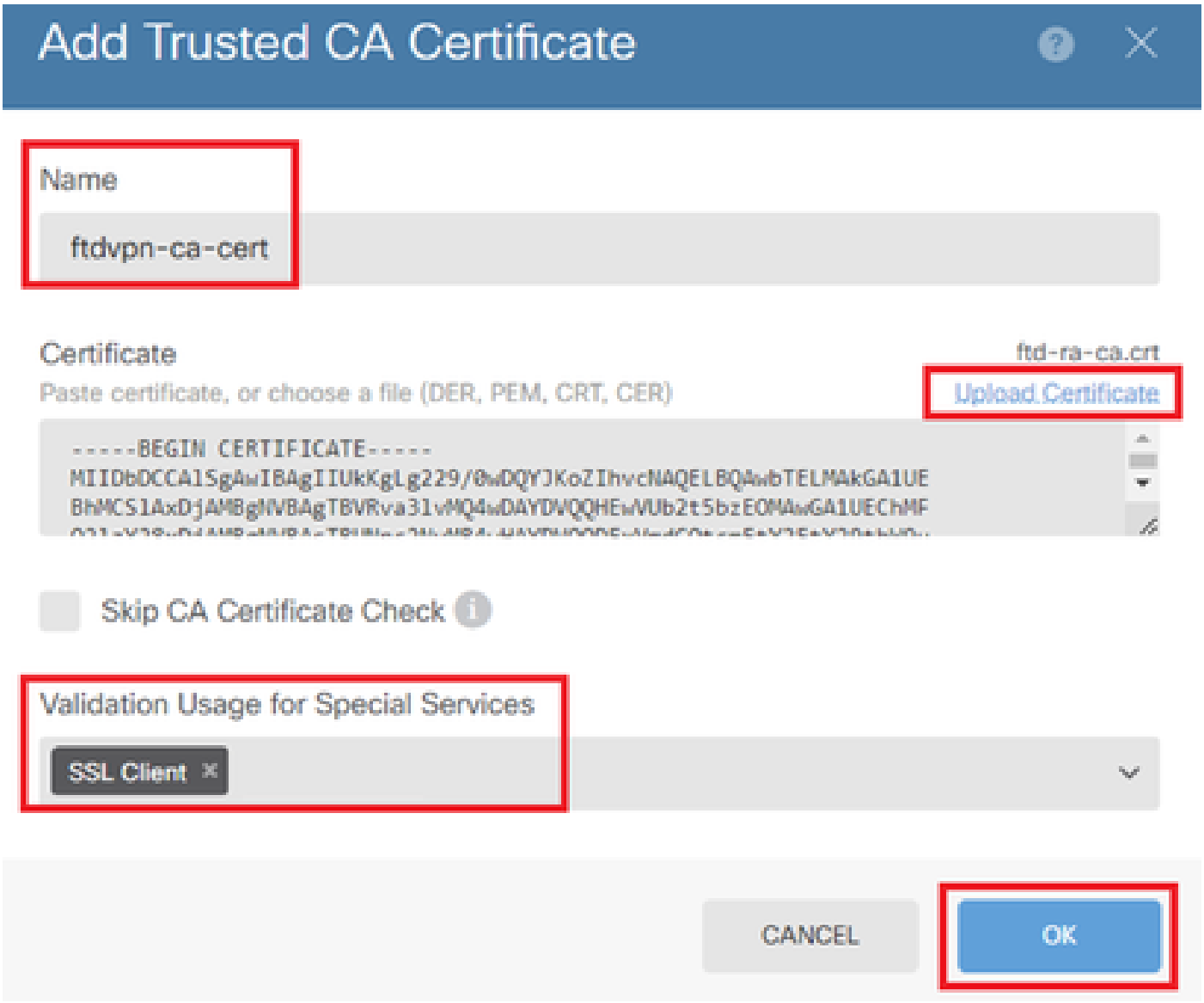
Navigeer naar Objecten > Certificaten, klik op Vertrouwde CA-certificaat toevoegen vanuit + item.



Vertrouwde CA-certificaat toevoegen

Voer de benodigde informatie voor CA in en importeer een certificaat van een lokale computer.

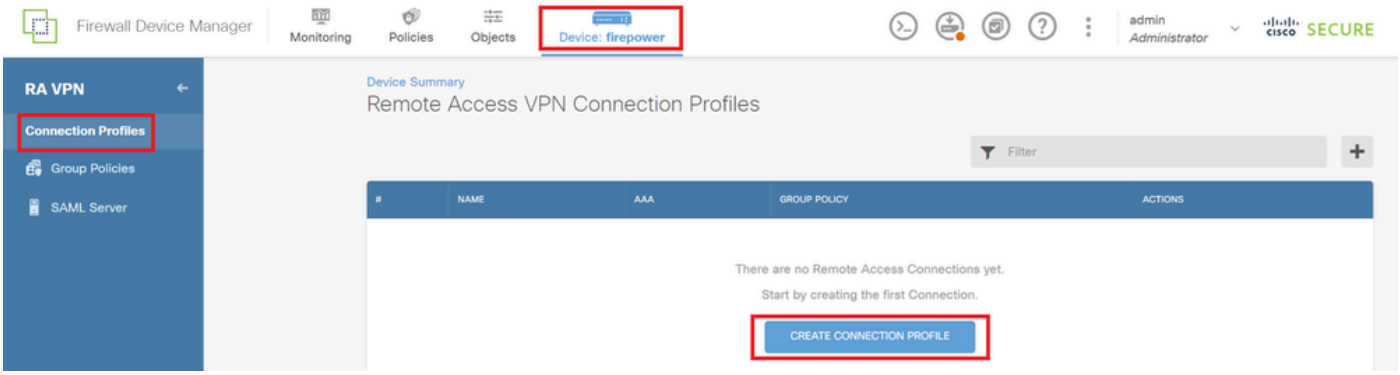
- Naam: ftdvpn-ca-cert
- Gebruik van validatie voor speciale services: SSL-client



Gegevens van het Trusted CA-certificaat

Stap 9. VPN-verbindingsprofiel voor externe toegang toevoegen

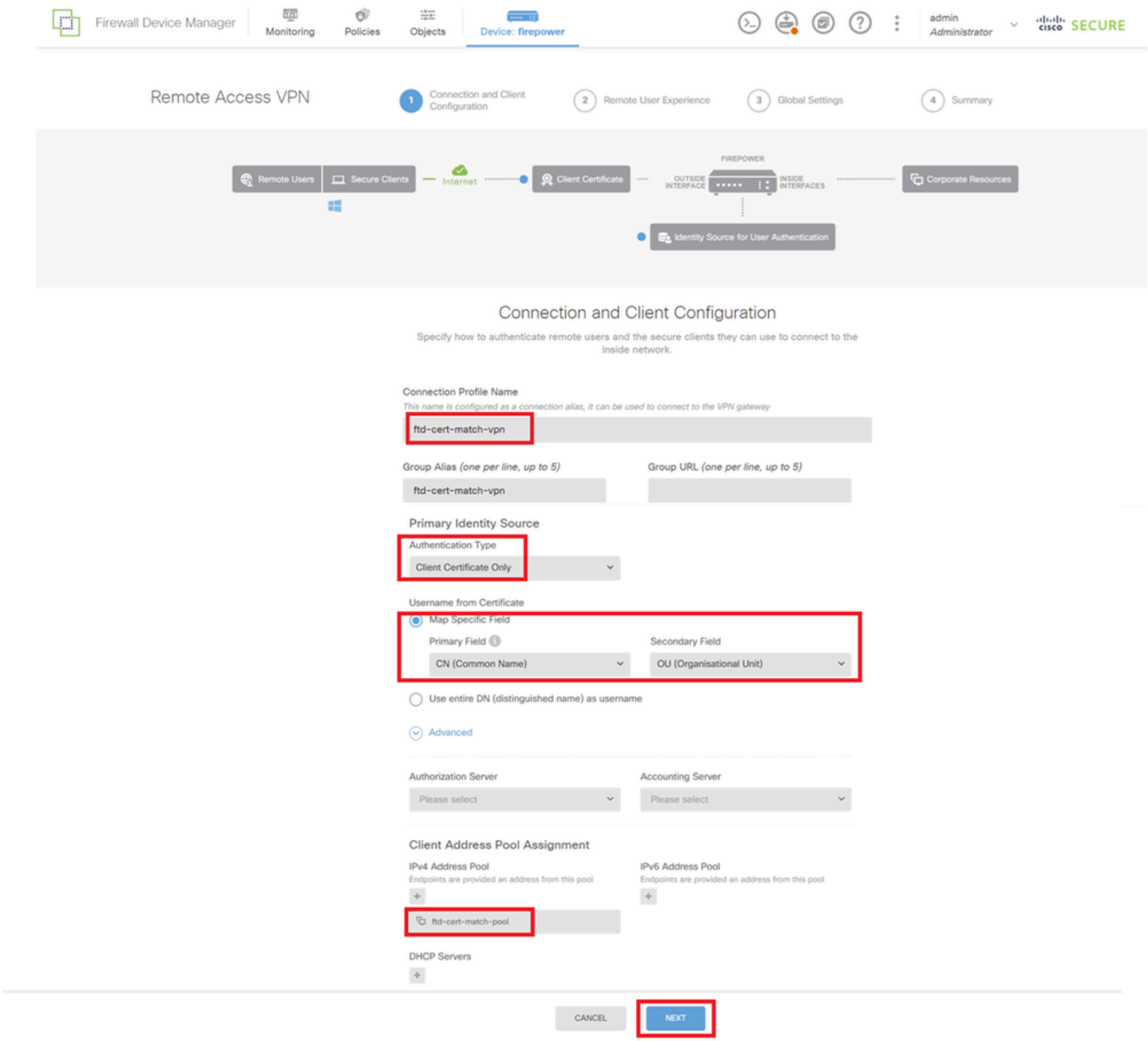
Navigeer naar Apparaat > Externe toegang VPN > Configuratie bekijken > Verbindingsprofielen, klik op de knop VERBINDINGSPROFIEL MAKEN.



VPN-verbindingsprofiel voor externe toegang toevoegen

Voer de benodigde informatie in voor het verbindingsprofiel en klik op Volgende knop.

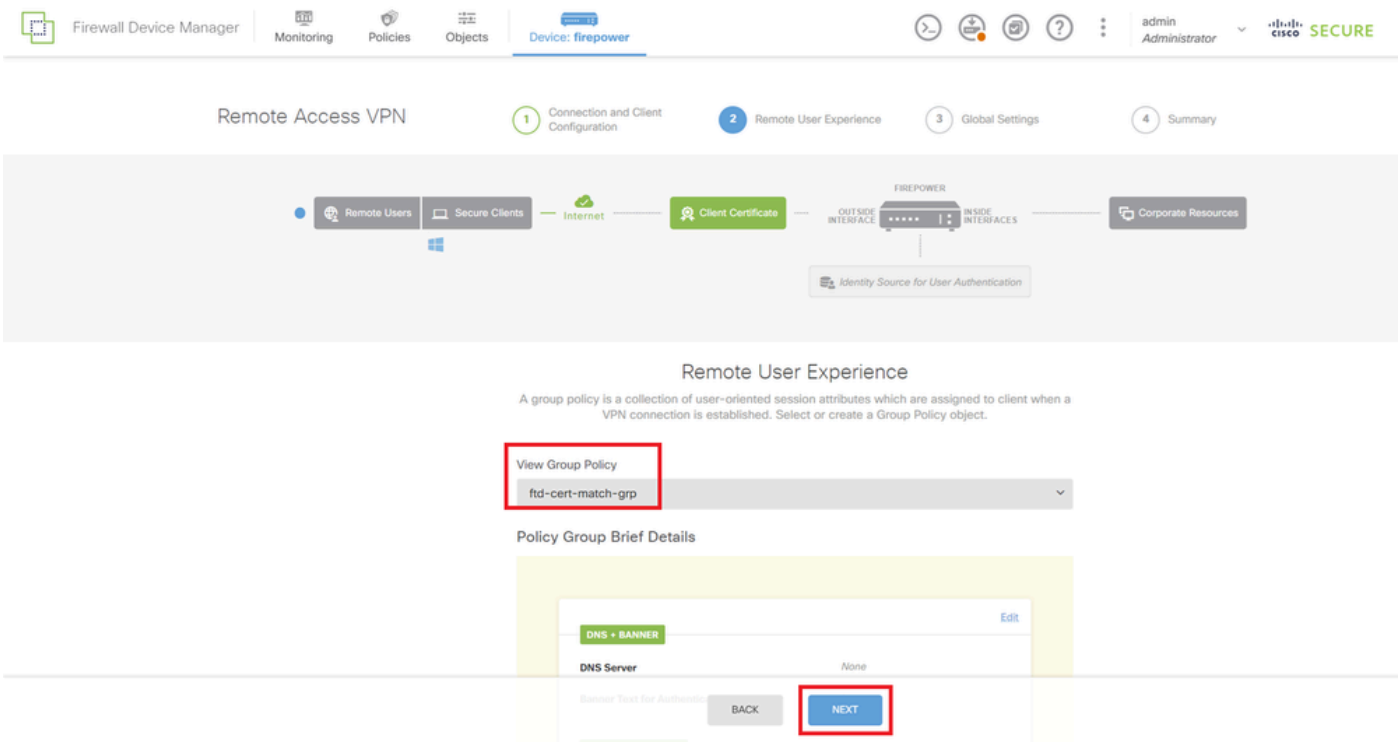
- Profielnaam verbinding: ftd-cert-match-vpn
- Verificatietype: alleen clientcertificaat
- Gebruikersnaam van certificaat: Kaartspecifiek veld
- Primair veld: CN (algemene naam)
- Secundair veld: OU (organisatorische eenheid)
- IPv4-adresgroepen: ftd-cert-match-pool



Details van VPN-verbindingsprofiel

Voer de benodigde informatie voor groepsbeleid in en klik op Volgende knop.

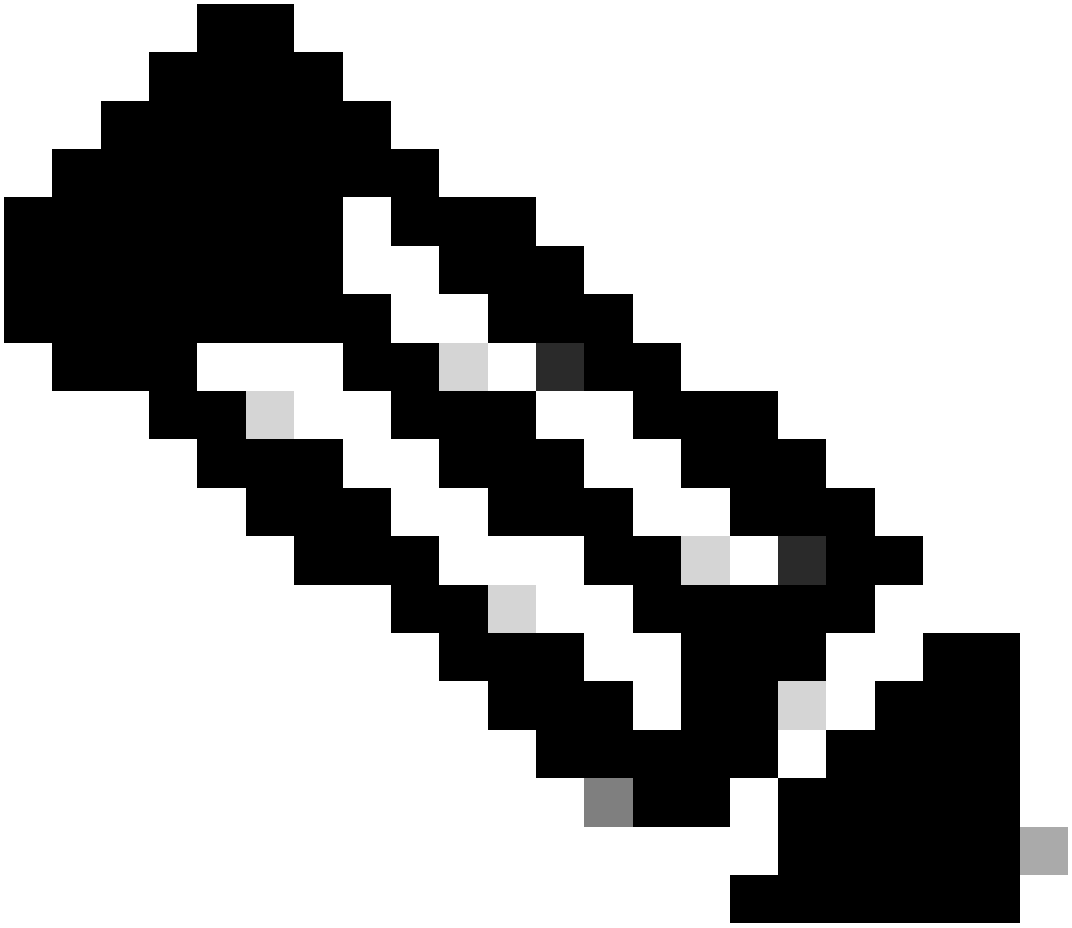
- Bekijk het groepsbeleid: ftd-cert-match-grp



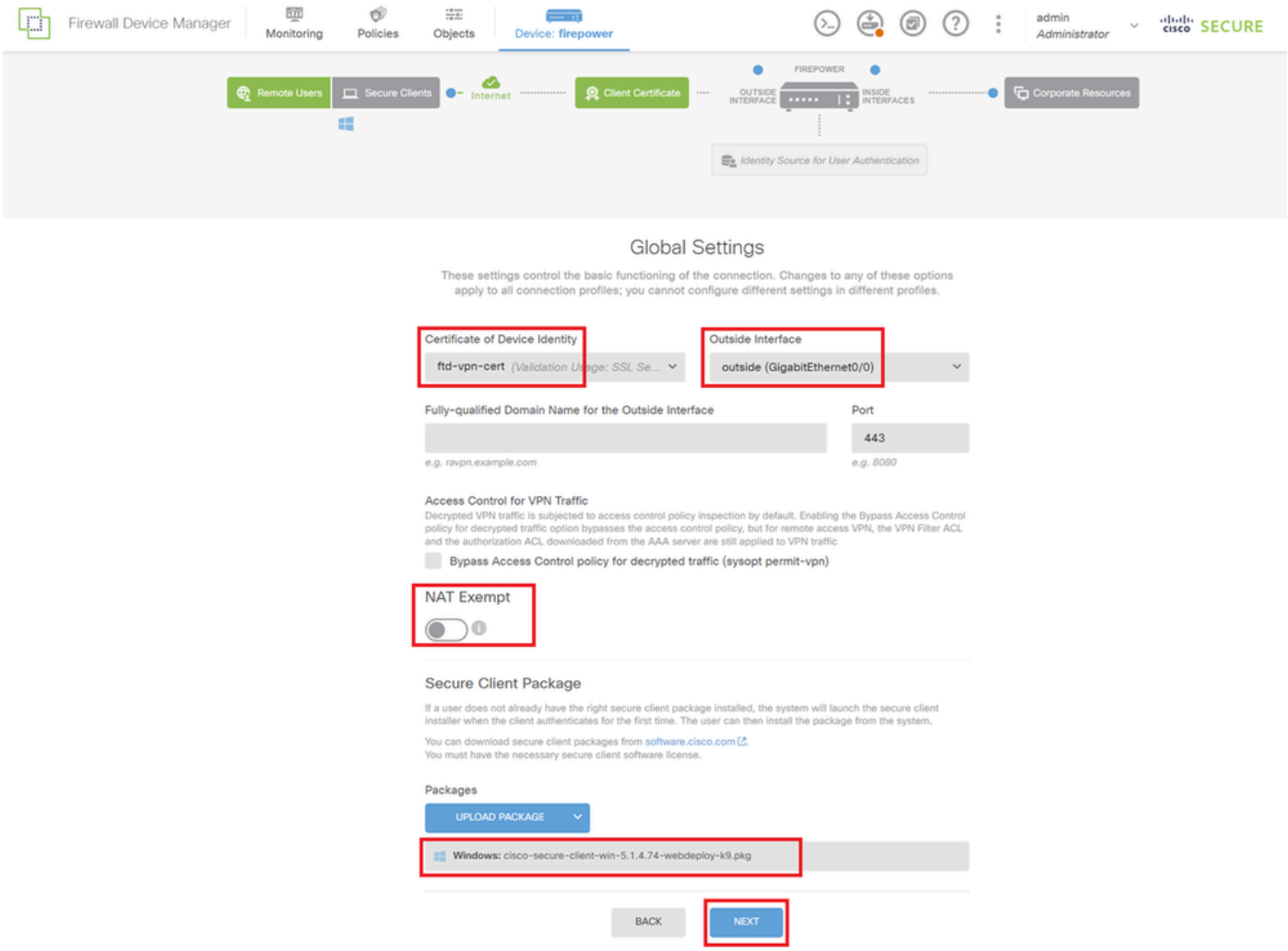
Groepsbeleid selecteren

Selecteer Certificaat van Apparaatidentiteit, Buiteninterface, Beveiligd clientpakket voor VPN-verbinding.

- Certificaat van identiteit apparaat: ftd-vpn-cert
- Externe interface: buiten (Gigabit Ethernet0/0)
- Secure-clientpakket: cisco-secure-client-win-5.1.4.74-webimplementation-k9.pkg



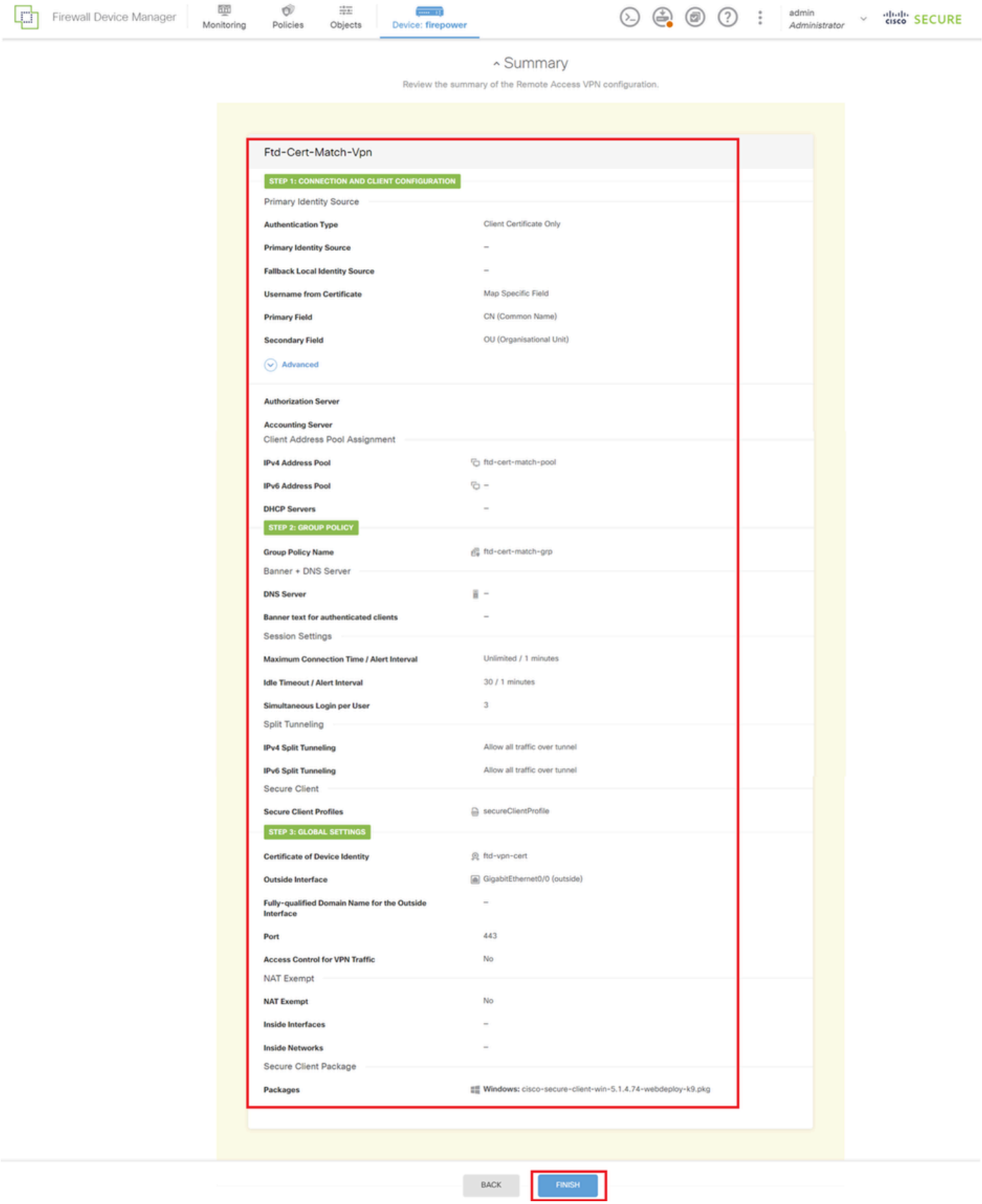
Opmerking: NAT-vrijstelling in dit document is uitgeschakeld.



Details van wereldwijde instellingen

Stap 10. Samenvatting voor verbindingsprofiel bevestigen

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



Samenvatting voor verbindingsprofiel bevestigen

Bevestigen in FTD CLI

Bevestig de VPN-verbindingsinstellingen in de FTD CLI na implementatie vanuit de 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
```

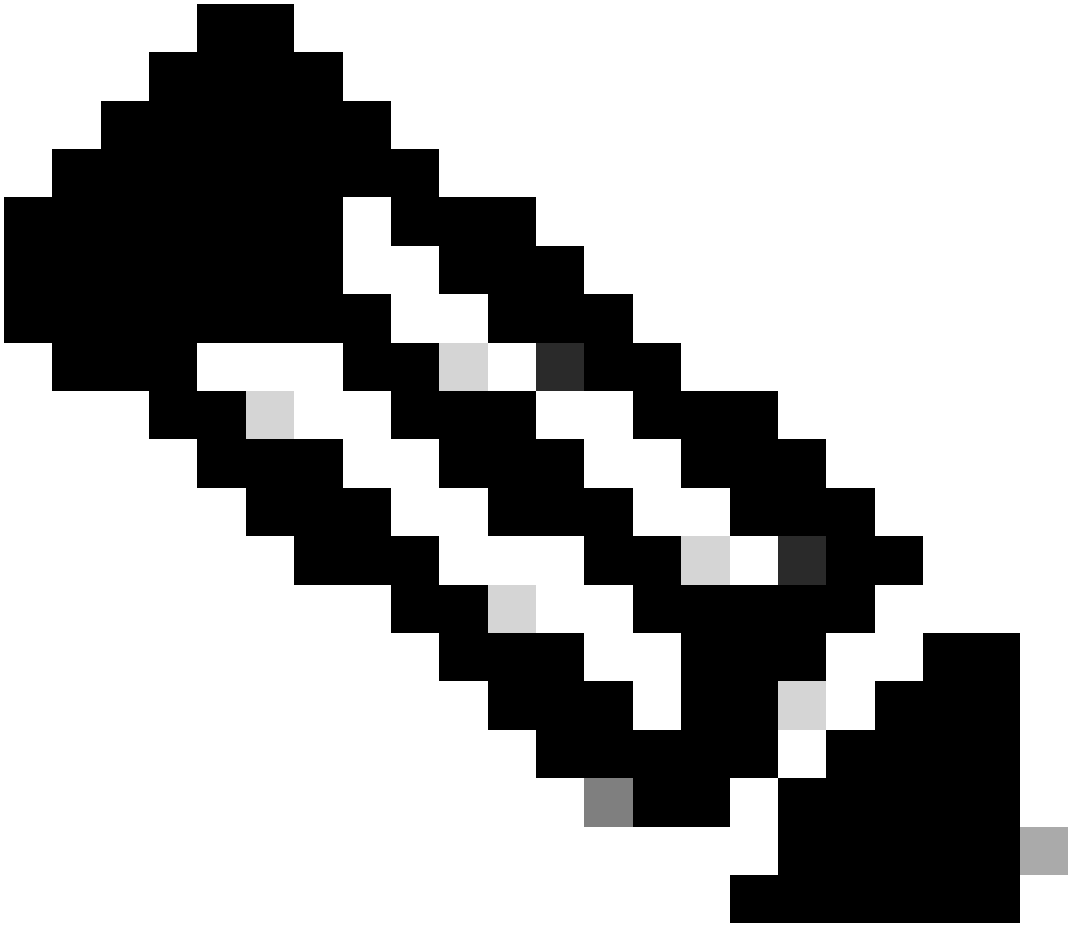
```
group-policy ftd-cert-match-grp internal
group-policy ftd-cert-match-grp attributes
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
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
```

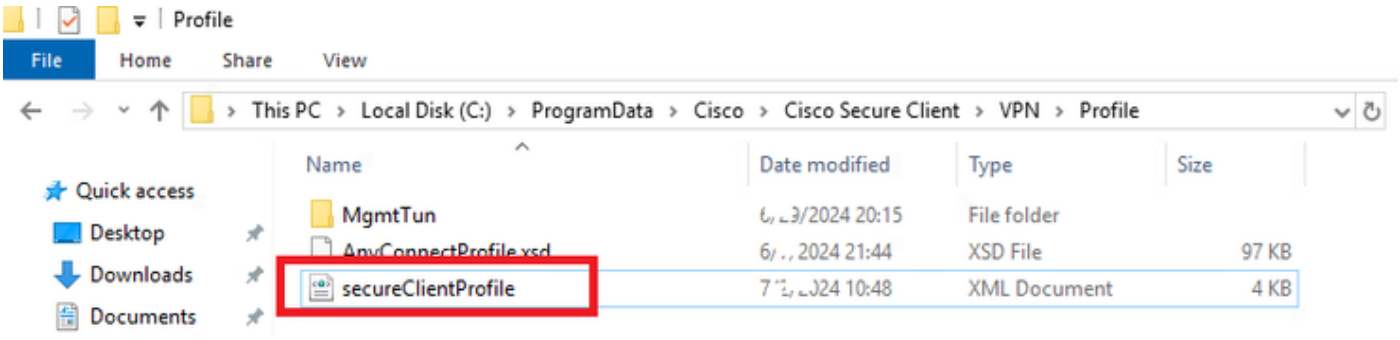
Bevestigen in VPN-client

Stap 1. Beveiligd clientprofiel naar VPN-client kopiëren

Kopieer het beveiligde clientprofiel naar de VPN-client voor engineer en beheer van VPN-client.



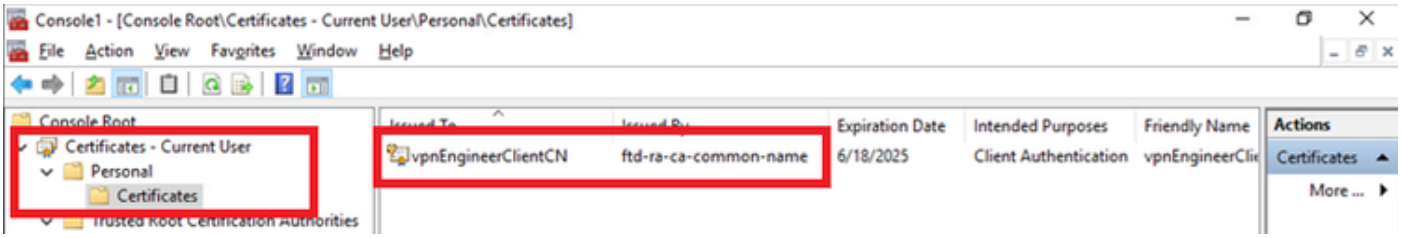
Opmerking: De map met het beveiligde clientprofiel op Windows-computer: C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile



Beveiligd clientprofiel naar VPN-client kopiëren

Stap 2. Clientcertificaat bevestigen

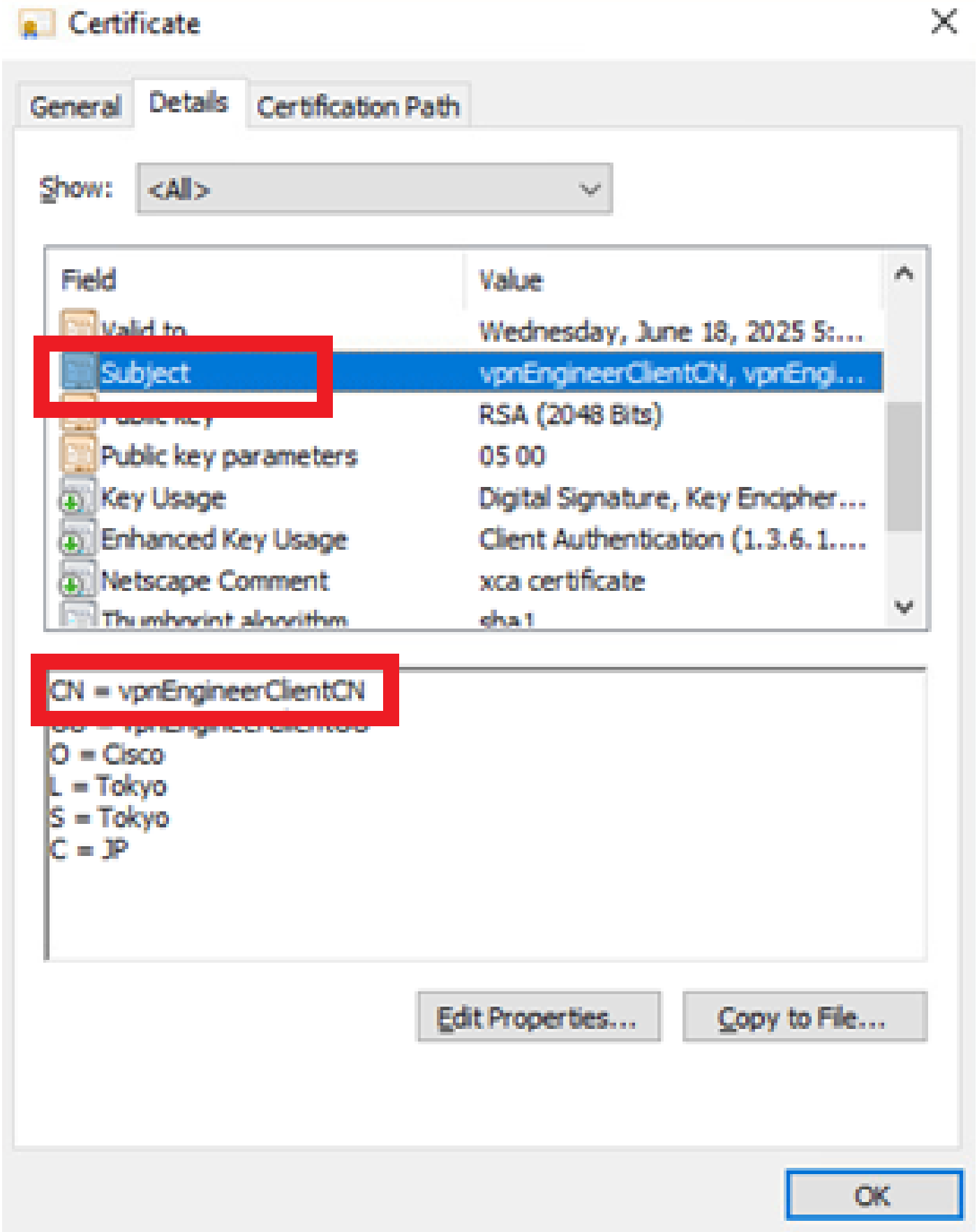
In ingenieur VPN client, navigeer naar Certificaten - Huidige Gebruiker > Persoonlijk > Certificaten, controleer het clientcertificaat dat wordt gebruikt voor verificatie.



Certificaat voor Engineer VPN-client bevestigen

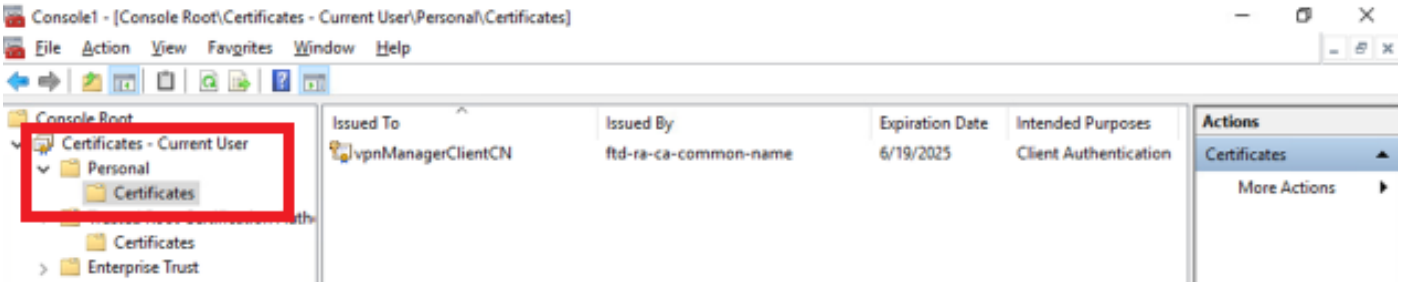
Dubbelklik op het clientcertificaat, navigeer naar Details, controleer de details van het onderwerp.

- Onderwerp: CN = vpnEngineerClientCN



Details van Engineer client certificaat

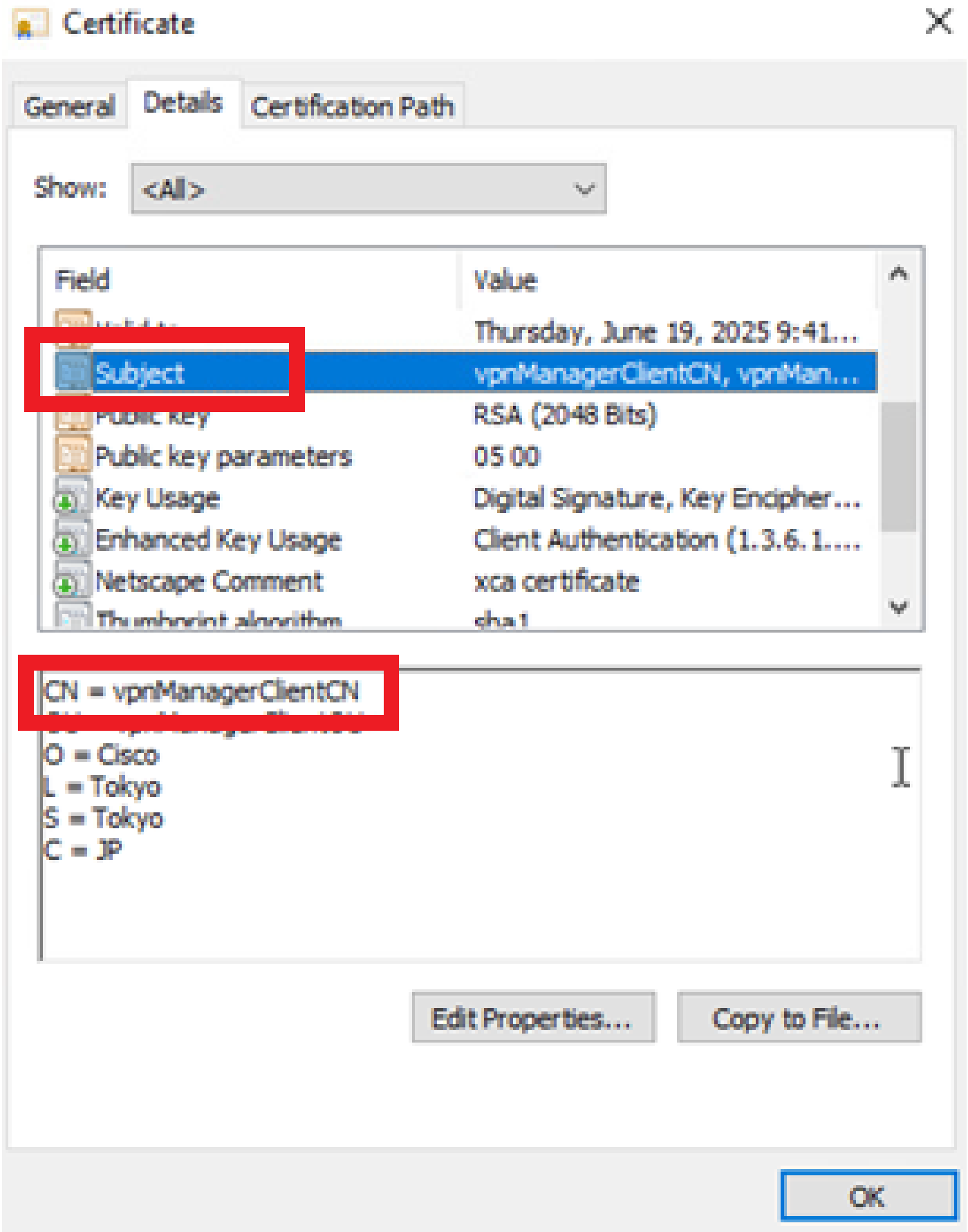
Ga in de VPN-client voor het beheer naar Certificaten - Huidige gebruiker > Persoonlijk > Certificaten, controleer het clientcertificaat dat wordt gebruikt voor verificatie.



Certificaat voor beheer VPN-client bevestigen

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

- Onderwerp: CN = vpnManagerClientCN

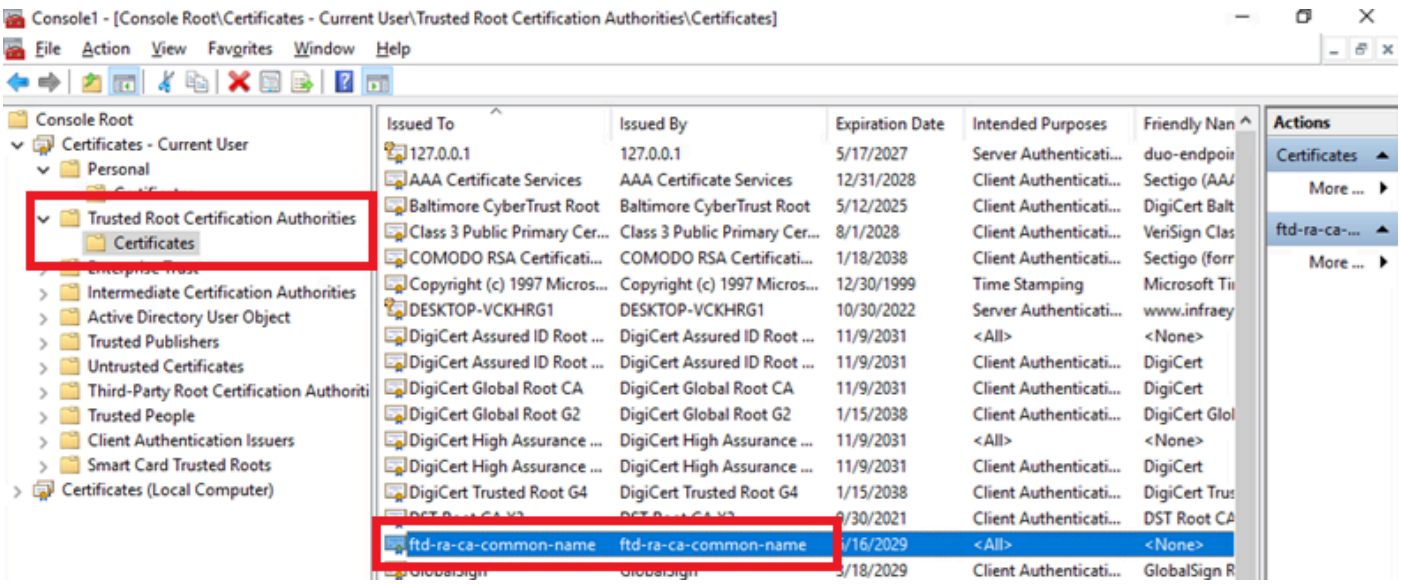


Details van clientcertificaat van Manager

Stap 3. Bevestig CA

In zowel de client van ingenieur VPN als de client van manager VPN, navigeer naar Certificaten - Huidige Gebruiker > Trusted Root Certification Authorities > Certificates, controleer de CA die gebruikt wordt voor verificatie.

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



Bevestig CA

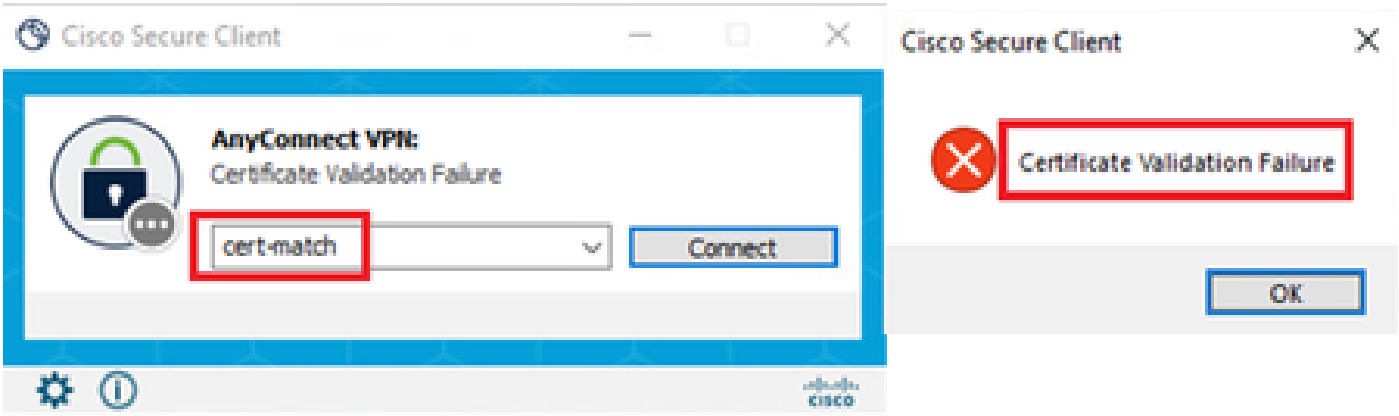
Verifiëren

Stap 1. VPN-verbinding starten

Start in Engineer VPN client de Cisco Secure Client-verbinding. U hoeft de gebruikersnaam en het wachtwoord niet in te voeren, de VPN is met succes verbonden.

VPN-verbinding geslaagd voor Engineer VPN-client

Start in het geval van een VPN-client voor beheer de Cisco Secure Client-verbinding. De VPN-verbinding is mislukt vanwege een fout in de certificaatvalidatie.



VPN-verbinding mislukt voor VPN-client voor beheer

Stap 2. VPN-sessies in FTD CLI bevestigen

show vpn-sessiondb detail anyconnect Start de opdracht in FTD (Lina) CLI om de VPN-sessies van engineer te bevestigen.

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 : 0000000000200006683932b
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

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 tijdens VPN verbinding van engineer client.

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=vpnEngineerClie
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

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.