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

Inhoud

Inleiding

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

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

- Cisco Firepower Management Center voor VMware 7.4.1
- Cisco Firewall Threat Defense Virtual 7.4.1

- Cisco Secure-client 5.1.3.62

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

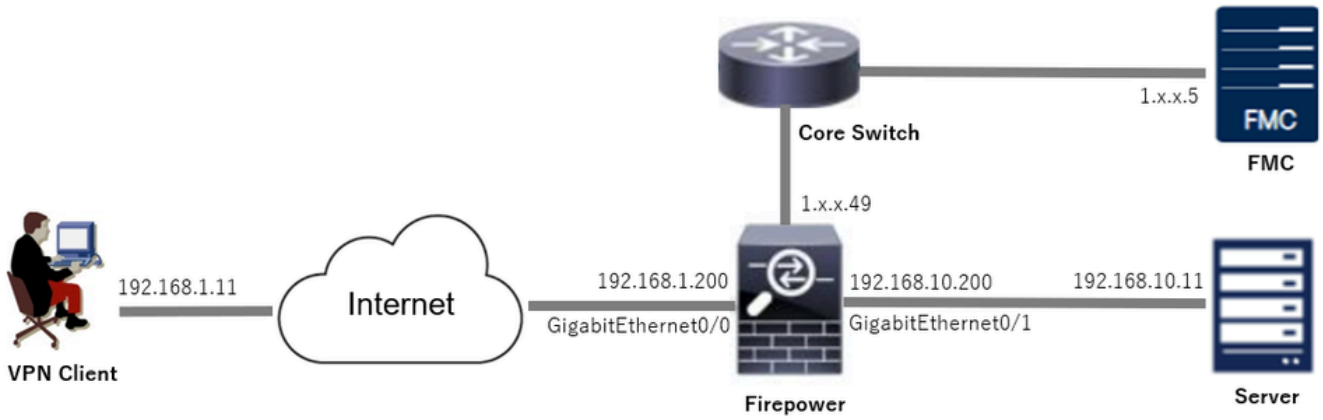
Aangezien organisaties striktere beveiligingsmaatregelen nemen, is het combineren van twee-factor-authenticatie (2FA) met op certificaten gebaseerde authenticatie een gangbare praktijk geworden om de beveiliging te verbeteren en bescherming te bieden tegen onbevoegde toegang. Een van de functies die de gebruikerservaring en beveiliging aanzienlijk kunnen verbeteren, is de mogelijkheid om de gebruikersnaam vooraf in de Cisco Secure-client in te vullen. Deze functie vereenvoudigt het inlogproces en verbetert de algehele efficiëntie van toegang op afstand.
Dit document beschrijft hoe u een voorgevulde gebruikersnaam kunt integreren met Cisco Secure Client op FTD, zodat gebruikers snel en veilig verbinding kunnen maken met het netwerk.

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

- CA : ftd-ra-ca-common-name
- Clientcertificaat: sslVPNClientCN
- Servercertificaat : 192.168.1.2000

Netwerkdiagram

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



Netwerkdiagram

Configuraties

Configuratie in VCC

Stap 1. FTD-interface configureren

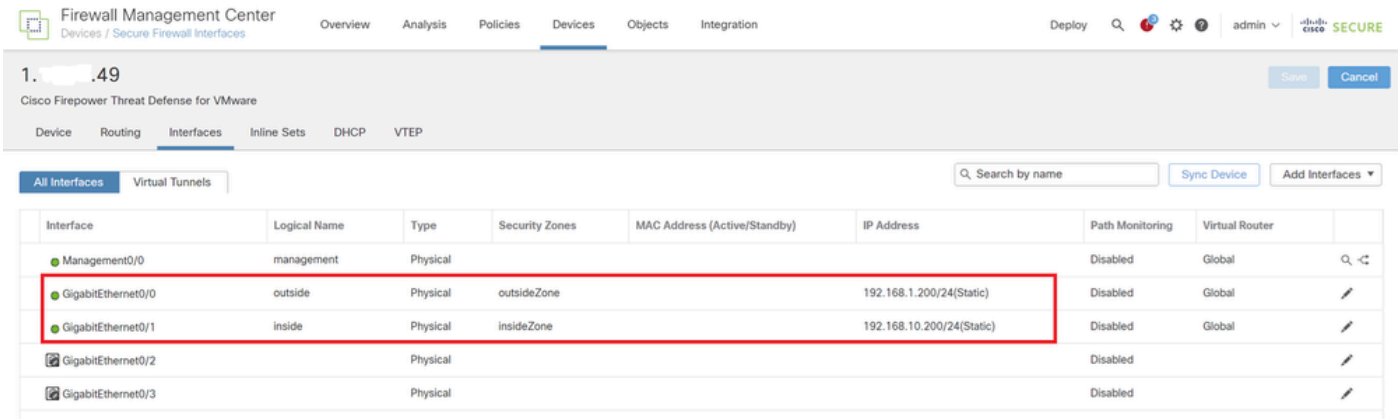
Navigeren naar Apparaten > Apparaatbeheer, bewerken van het FTD-doelapparaat, configureren binnen en buiten interface voor FTD in het tabblad Interfaces.

Voor Gigabit Ethernet0/0,

- Naam : buiten
- Security Zone: buitenZone
- IP-adres: 192.168.1.200/24

Voor Gigabit Ethernet0/1,

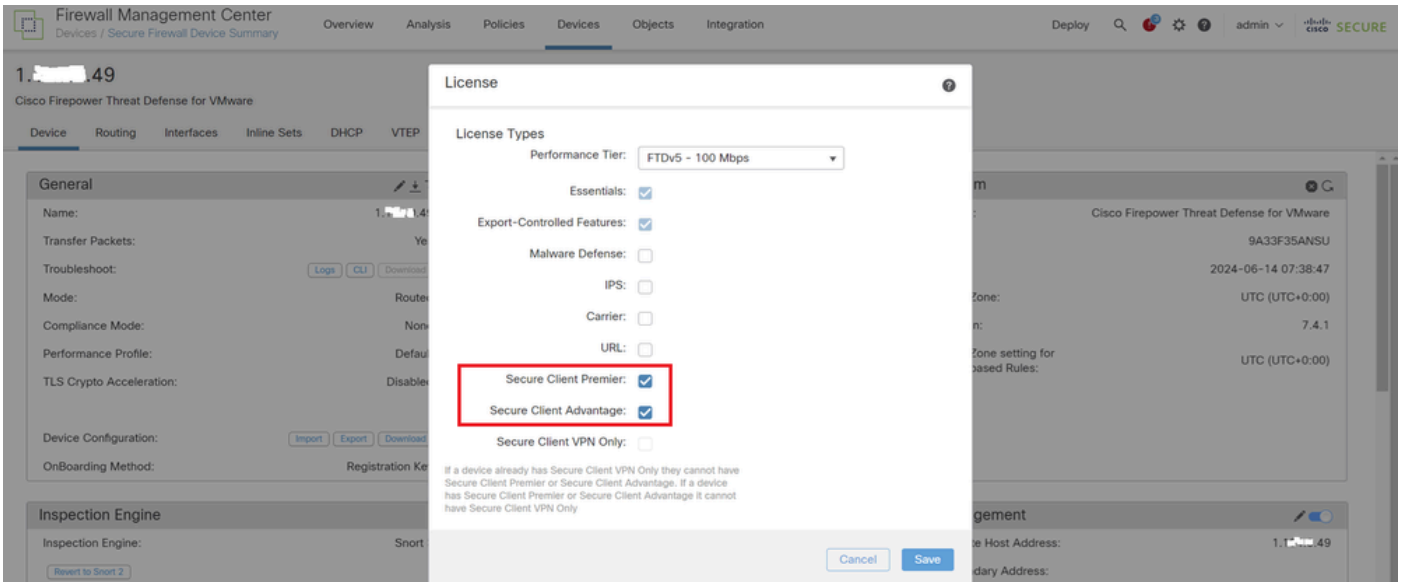
- Naam : binnen
- Security Zone: binnenZone
- IP-adres: 192.168.10.200/24



FTD-interface

Stap 2. Cisco Secure-clientlicentie bevestigen

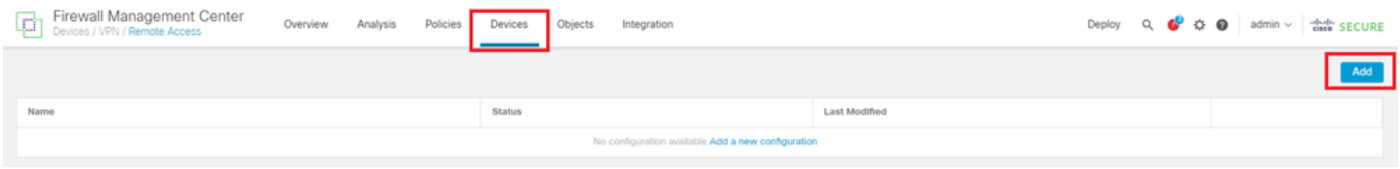
Navigeer naar Apparaten > Apparaatbeheer, bewerk het FTD-doelapparaat en bevestig de Cisco Secure Client-licentie op het tabblad Apparaat.



Secure-clientlicentie

Stap 3. Beleidstoewijzing toevoegen

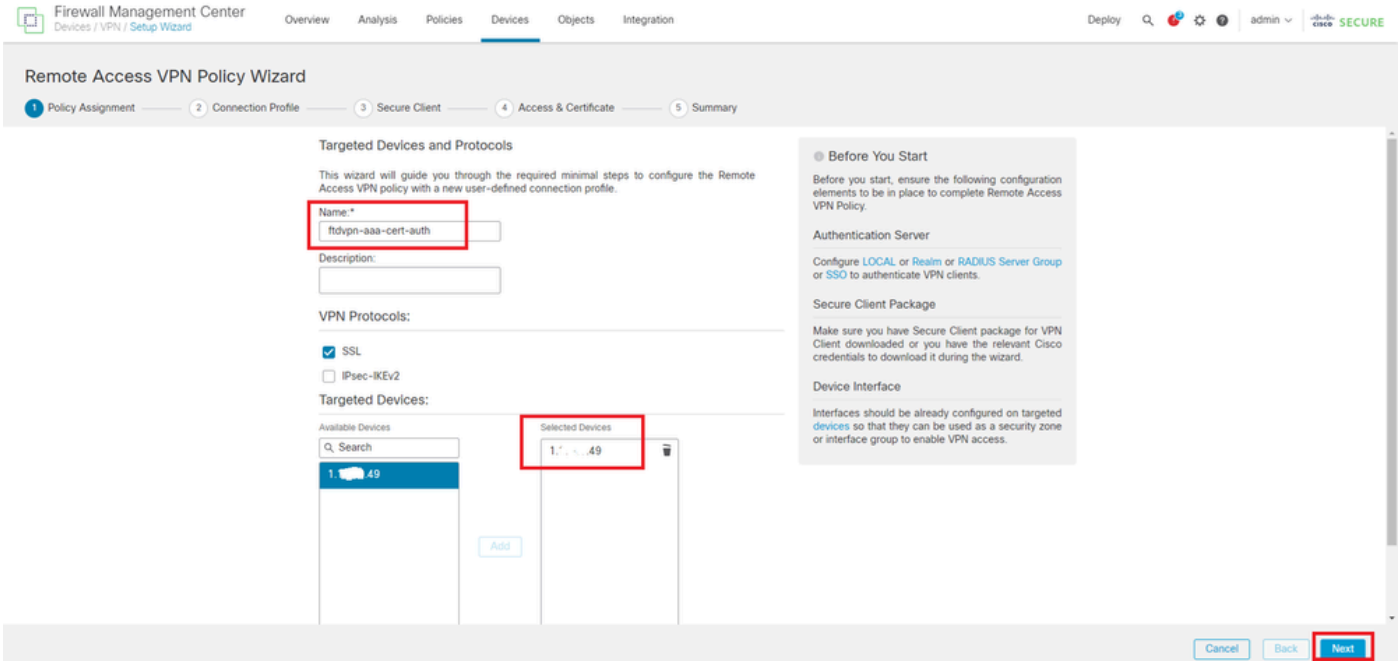
Navigeer naar Apparaten > VPN > Externe toegang en klik op de knop Toevoegen.



Voeg externe toegang toe aan VPN

Voer de gewenste informatie in en klik op Volgende.

- Naam: ftdvpn-aaa-cert-auth
- VPN-protocollen: SSL
- Gerichte apparaten: 1.x.x.49

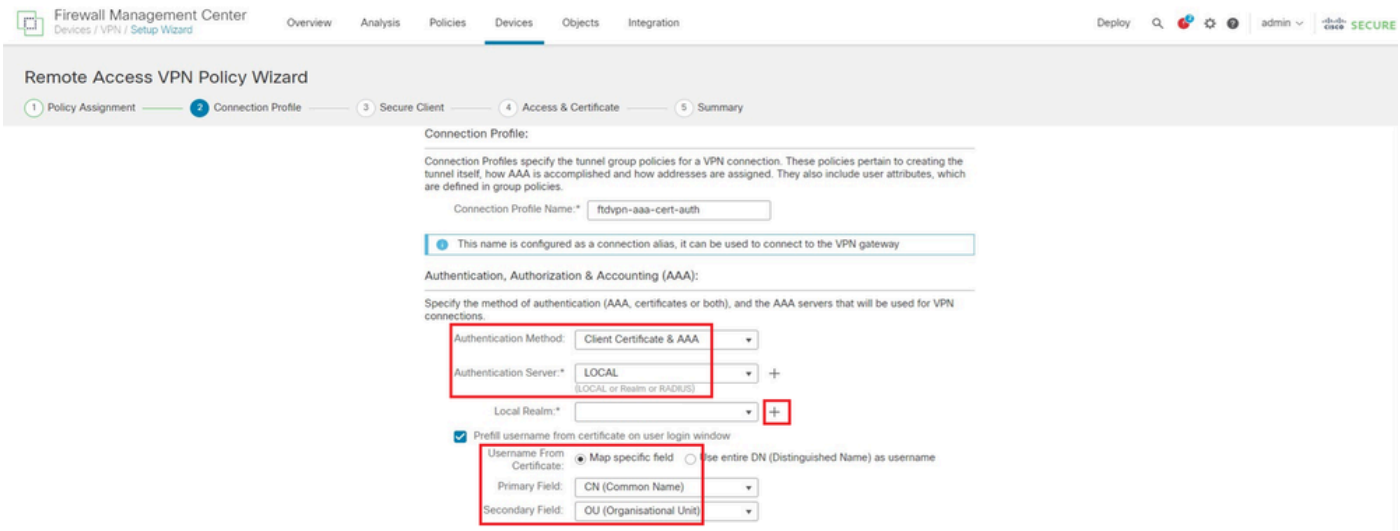


Beleidstoewijzing

Stap 4. Config-gegevens voor verbindingsprofiel

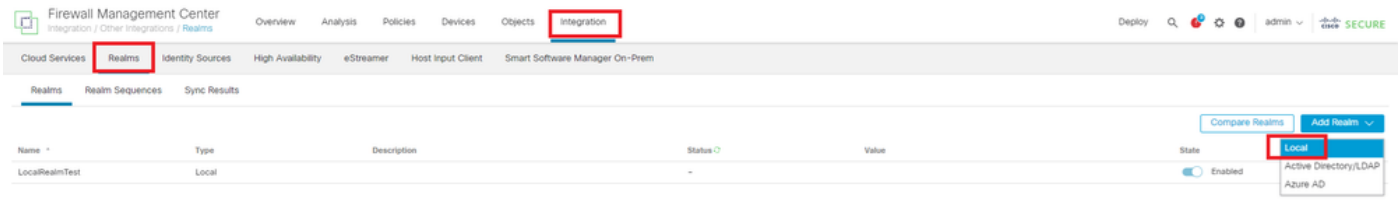
Voer de benodigde informatie voor het verbindingsprofiel in en klik op + knop naast de optie Lokaal gebied.

- Verificatiemethode: clientcertificaat en AAA
- Verificatieserver: LOKAAL
- Gebruikersnaam van certificaat: kaartspecifiek veld
- Primair veld : CN (algemene naam)
- Secundair veld : OU (organisatorische eenheid)



Details van verbindingsprofiel

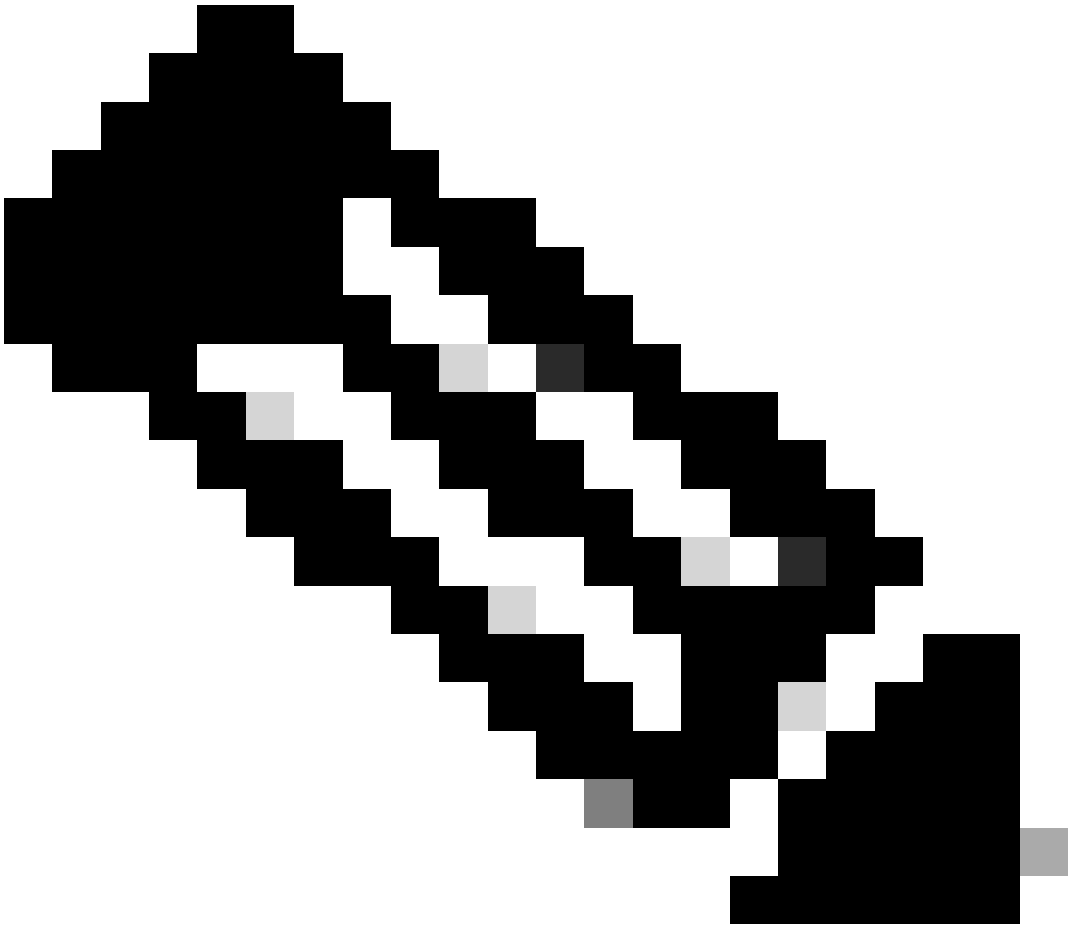
Klik op Lokaal vanuit de vervolgkeuzelijst Add Real om een nieuw lokaal domein toe te voegen.



Lokaal gebied toevoegen

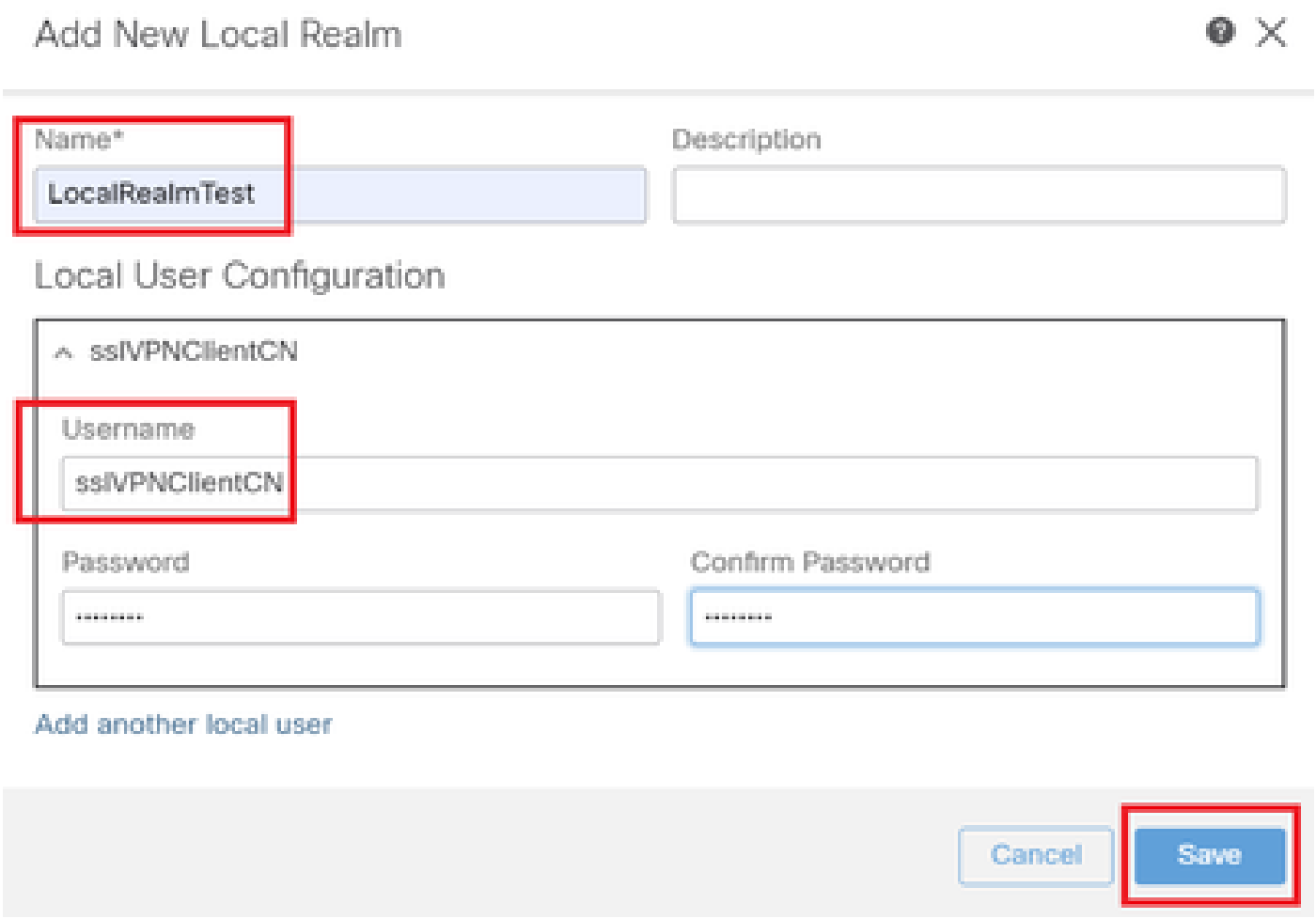
Voer de benodigde informatie voor de lokale omgeving in en klik op de knop Opslaan.

- Naam: LocalRealTest
- Gebruikersnaam: sslVPNClientCN



Opmerking: De gebruikersnaam is gelijk aan de algemene naam binnen het clientcertificaat

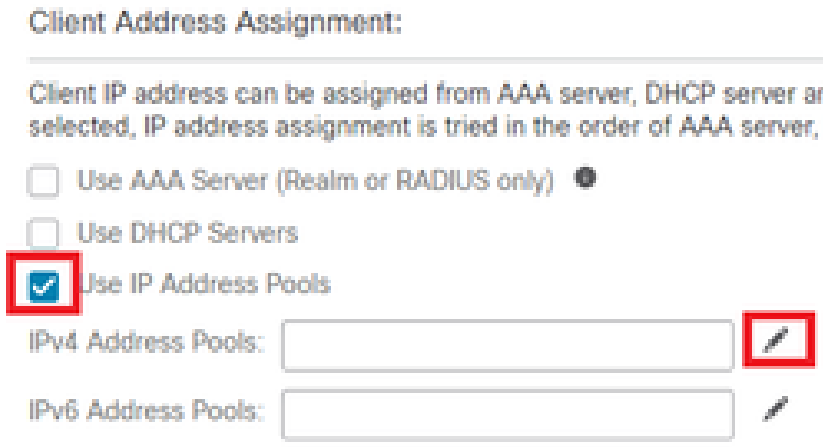
---



Details van Local Area

Stap 5. Adresgroep toevoegen voor verbindingsprofiel

Klik op de knop Bewerken naast het item IPv4-adrespools.

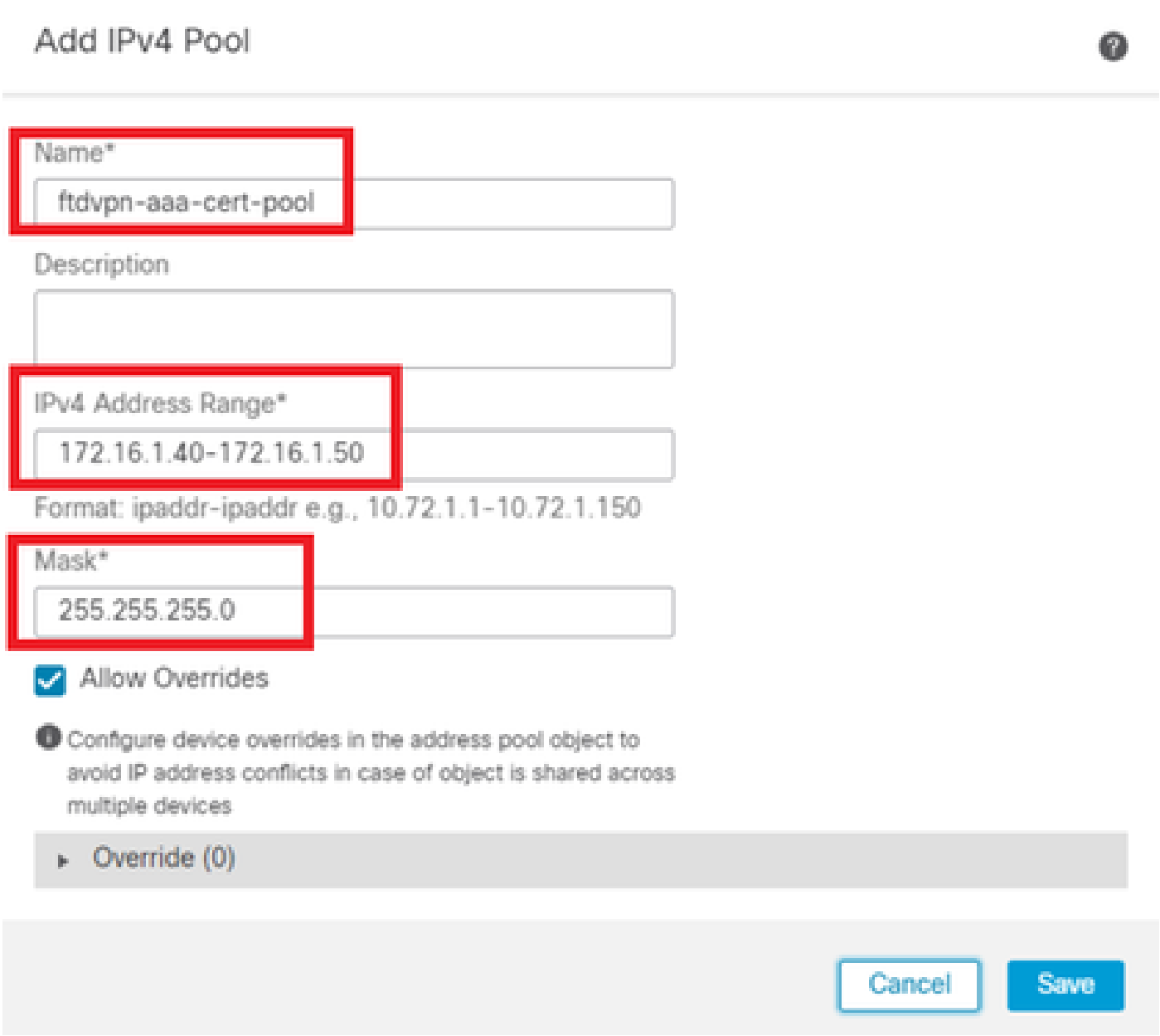


IPv4-adresgroep toevoegen

Voer de benodigde informatie in om een nieuwe IPv4-adresgroep toe te voegen. Selecteer de nieuwe IPv4-adresgroep voor het verbindingsprofiel.

- Naam : ftdvpn-aaa-cert-pool
- IPv4-adresbereik: 172.16.1.40-172.16.1.50

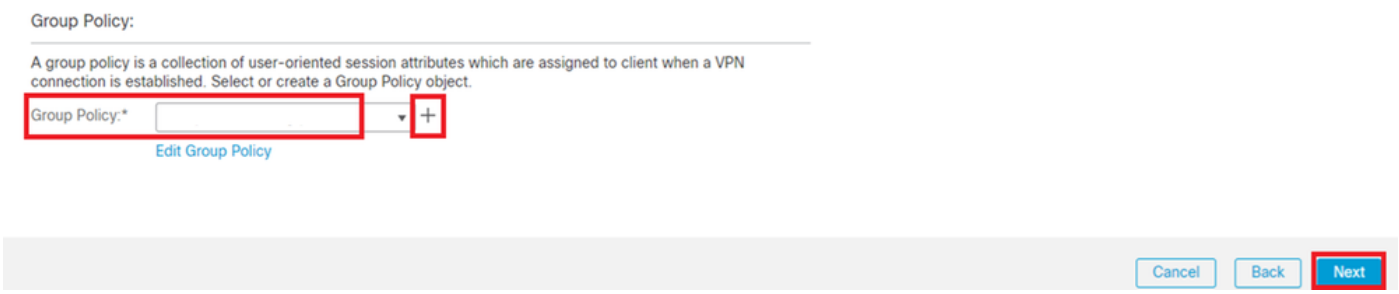
- Masker : 255 255 255,0



Details van IPv4-adresgroep

Stap 6. Groepsbeleid toevoegen voor verbindingsprofiel

Klik op + knop naast het item Groepsbeleid.

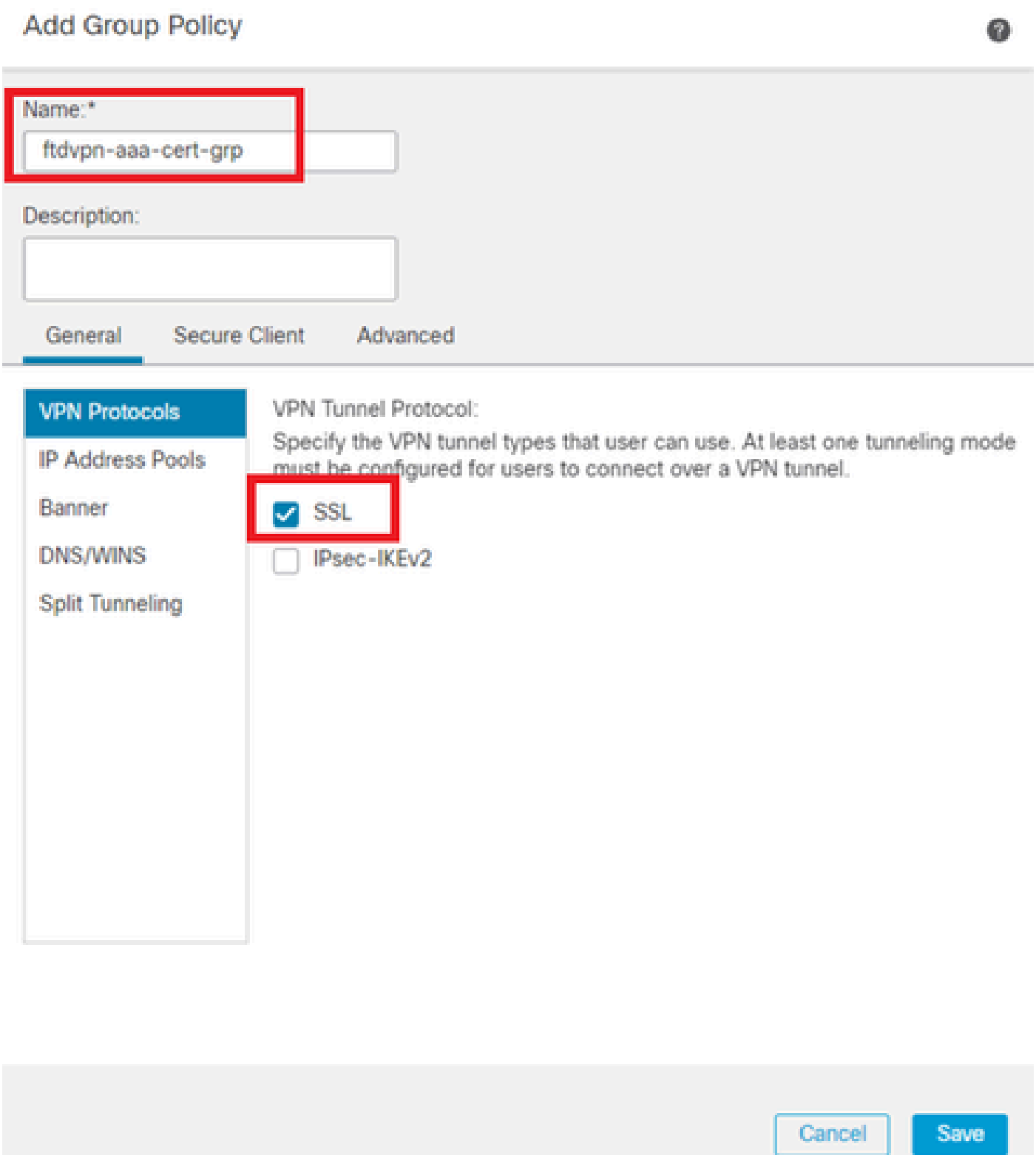


Groepsbeleid toevoegen

Voer de benodigde informatie in om een nieuw groepsbeleid toe te voegen. Selecteer het nieuwe

groepsbeleid voor het verbindingsprofiel.

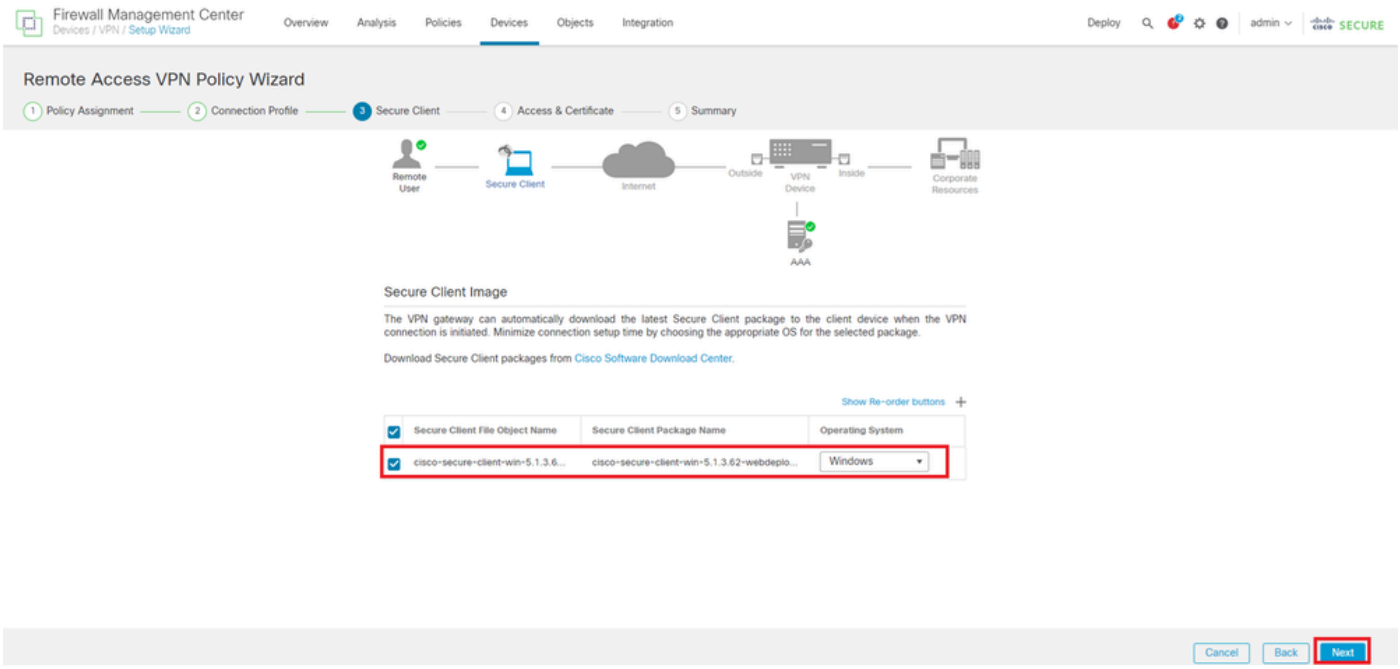
- Naam : ftdvpn-aaa-cert-grp
- VPN-protocollen: SSL



Details van groepsbeleid

Stap 7. Config Secure-clientafbeelding voor verbindingsprofiel

Selecteer een beveiligd clientbeeldbestand en klik op Volgende.

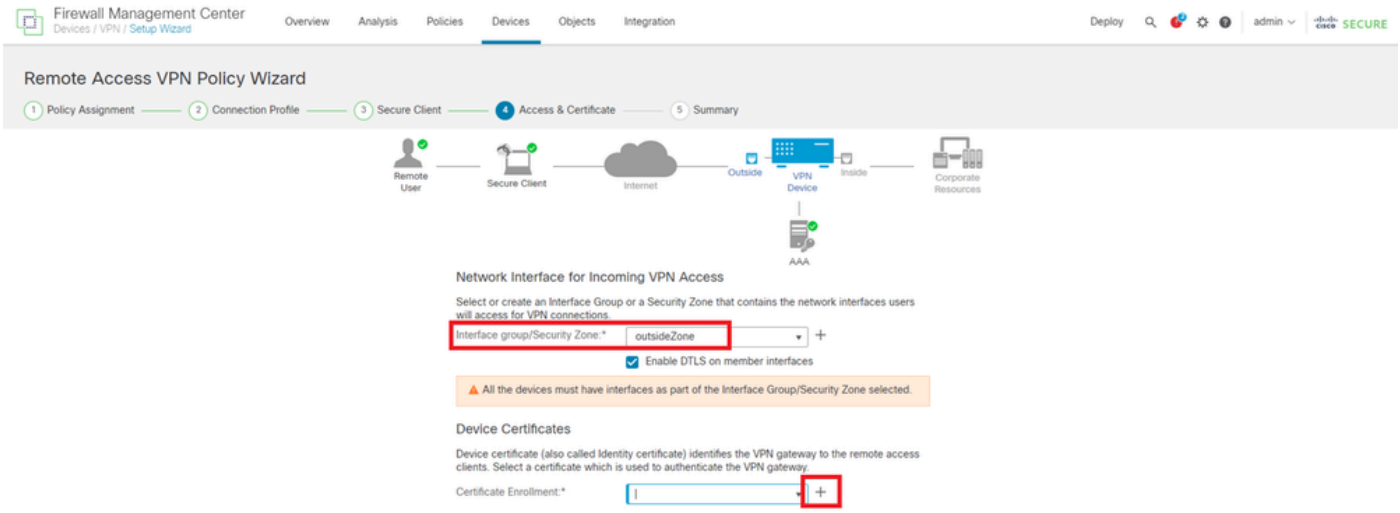


Selecteer een beveiligde clientafbeelding

Stap 8. Config-toegangs- en -certificaatprofiel voor verbindingen

Selecteer Security Zone voor VPN-verbinding en klik op + knop naast item Certificaatinschrijving.

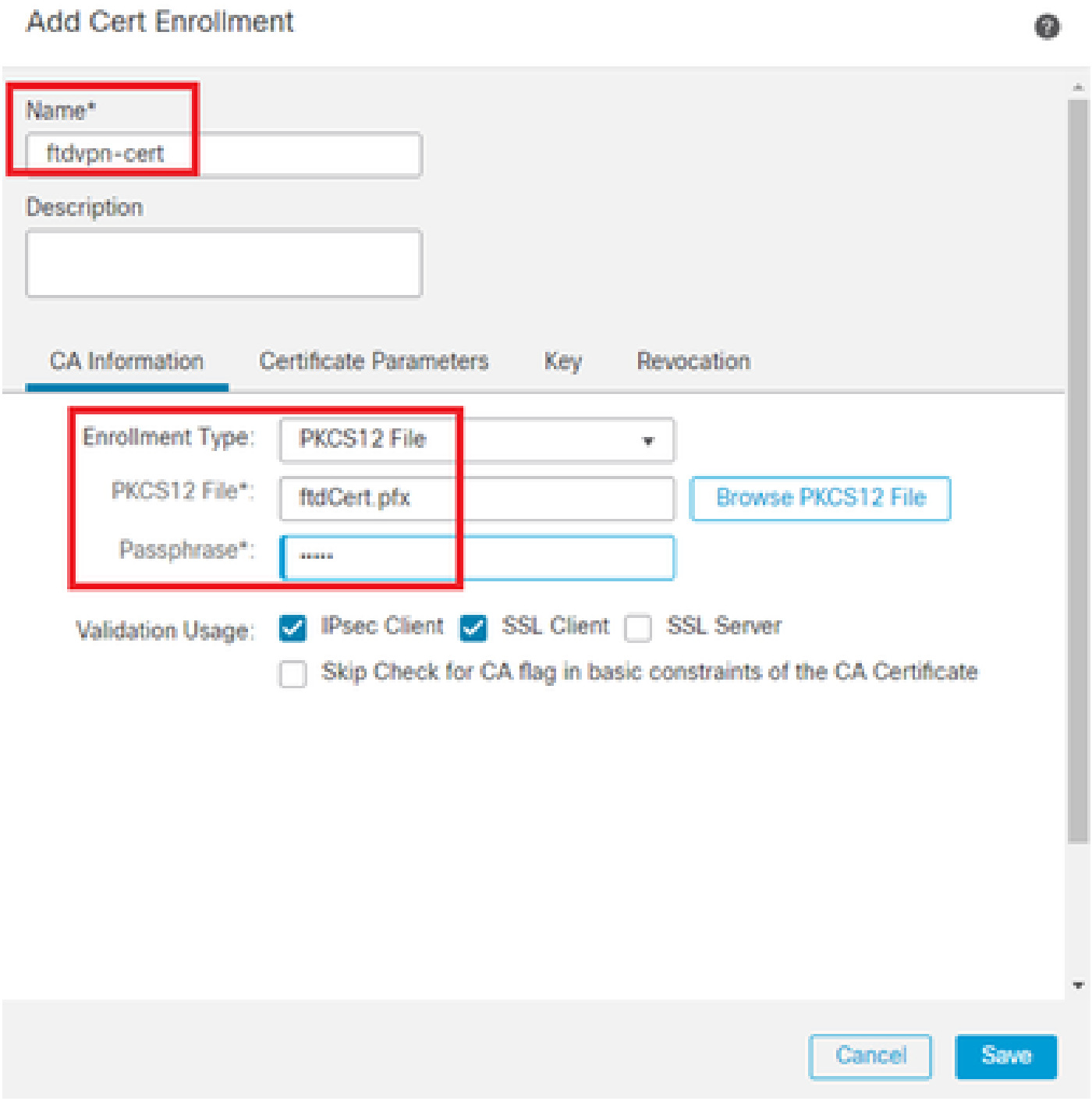
- Interfacegroep/Security Zone: buitenkantZone



Selecteer Security Zone

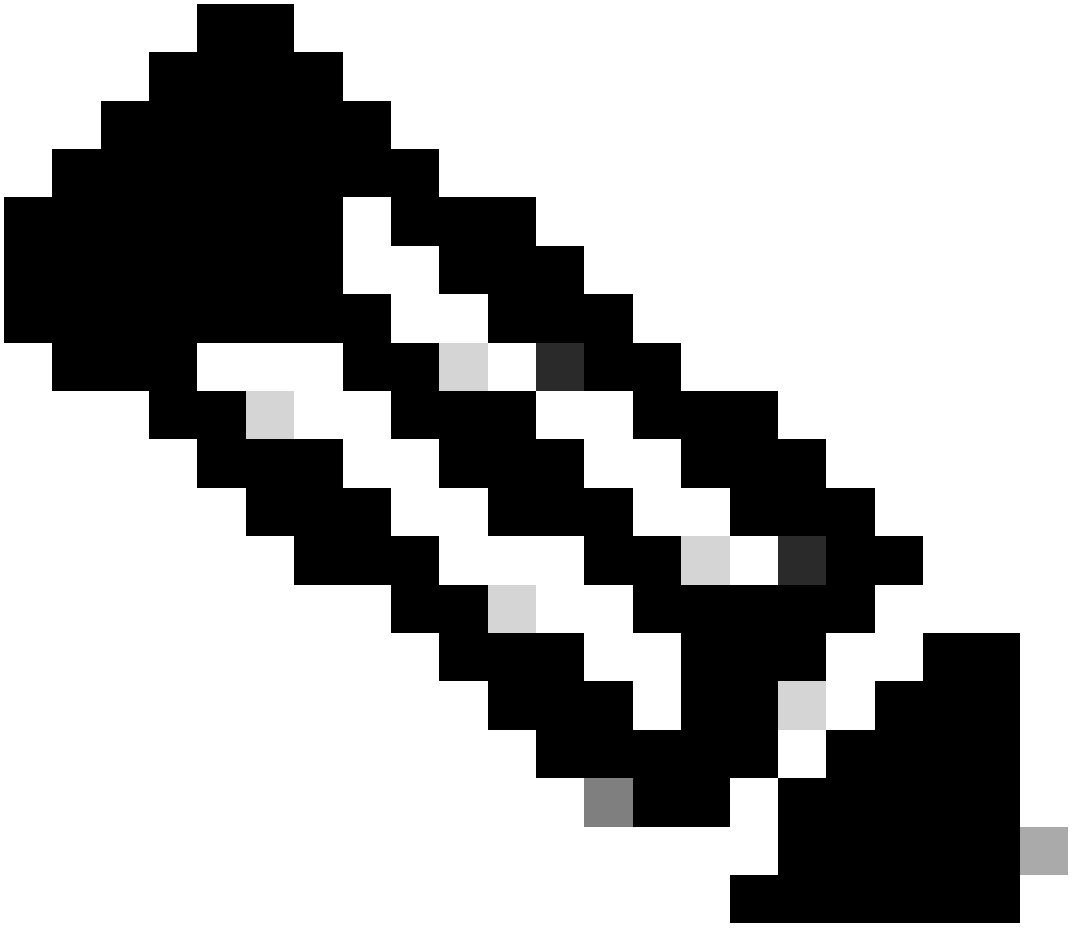
Voer de benodigde informatie voor FTD-certificaat in en importeer een PKCS12-bestand van een lokale computer.

- Naam: ftdvpn-cert
- Type inschrijving: PKCS12-bestand

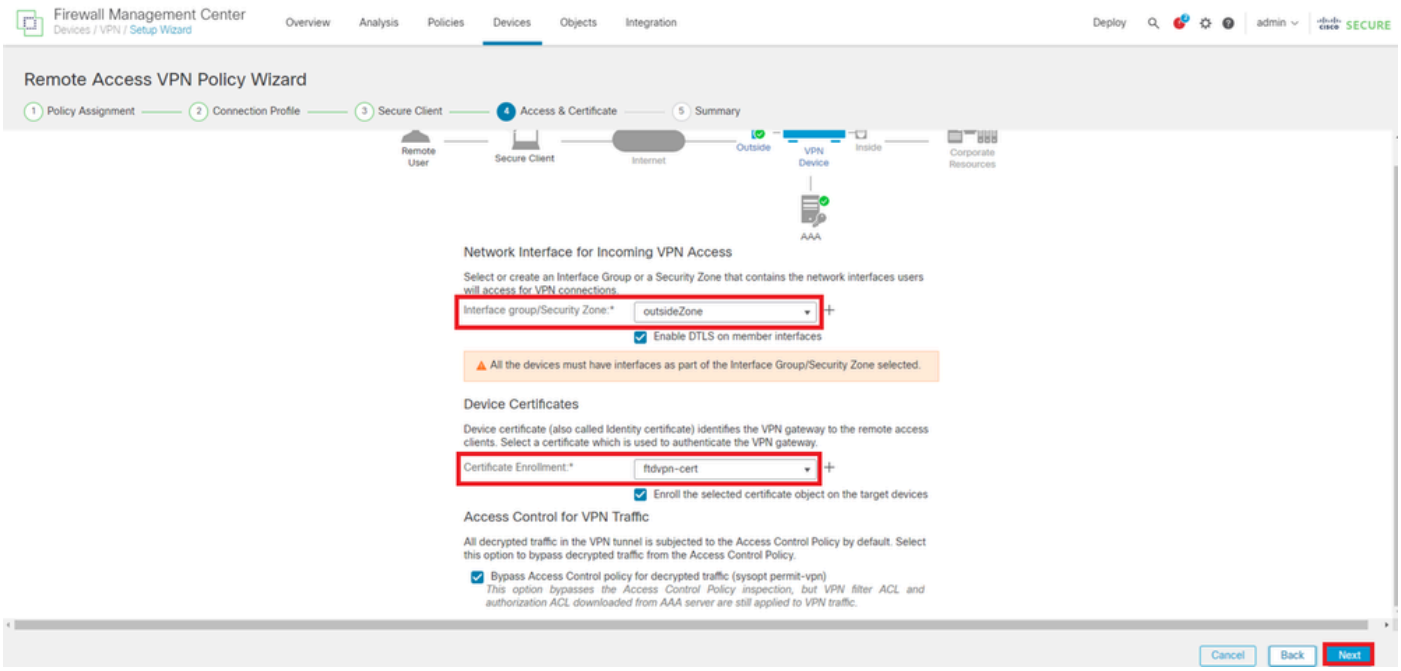


FTD-certificaat toevoegen

Bevestig de informatie die u in de wizard Toegang en certificaat hebt ingevoerd en klik op Volgende.



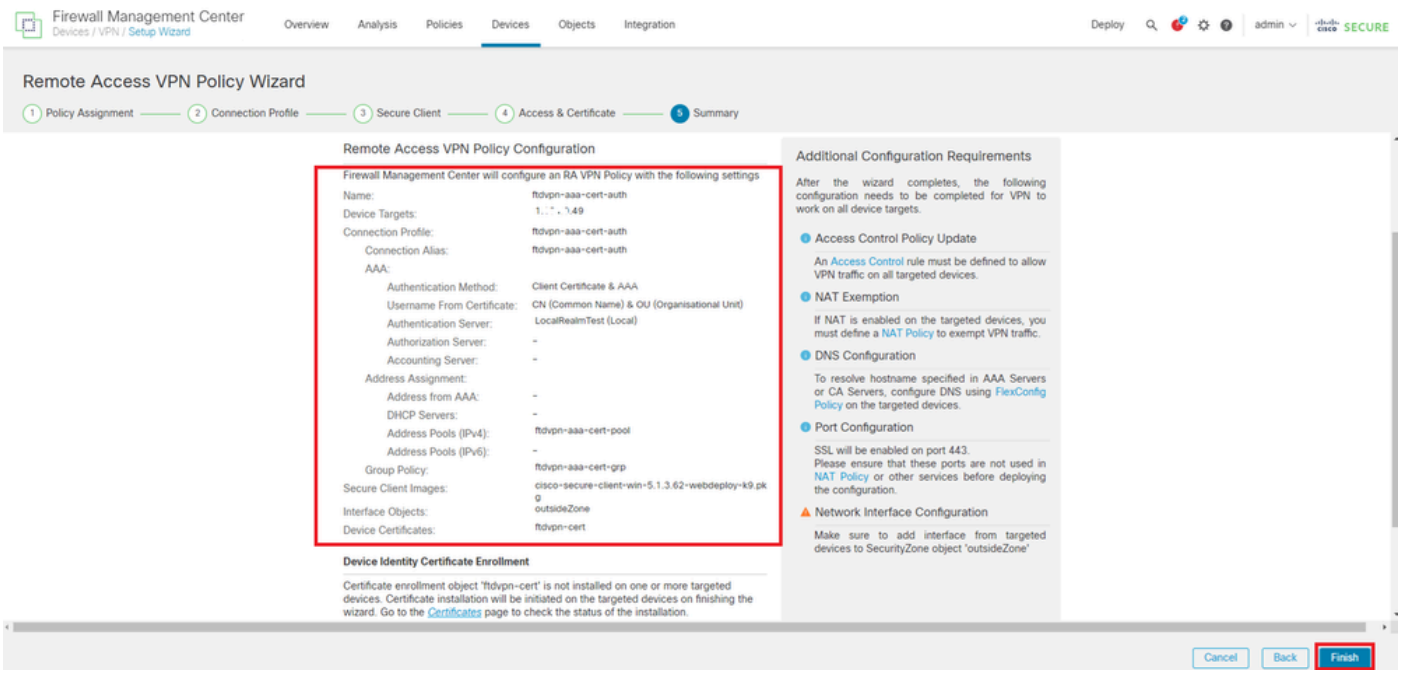
Opmerking: Omzeilen van toegangscontrolebeleid voor gedecrypteerd verkeer inschakelen (sysopt license-vpn), zodat gedecrypteerd VPN-verkeer niet wordt onderworpen aan controle van het toegangscontrolebeleid.



Instellingen in toegang en certificaat bevestigen

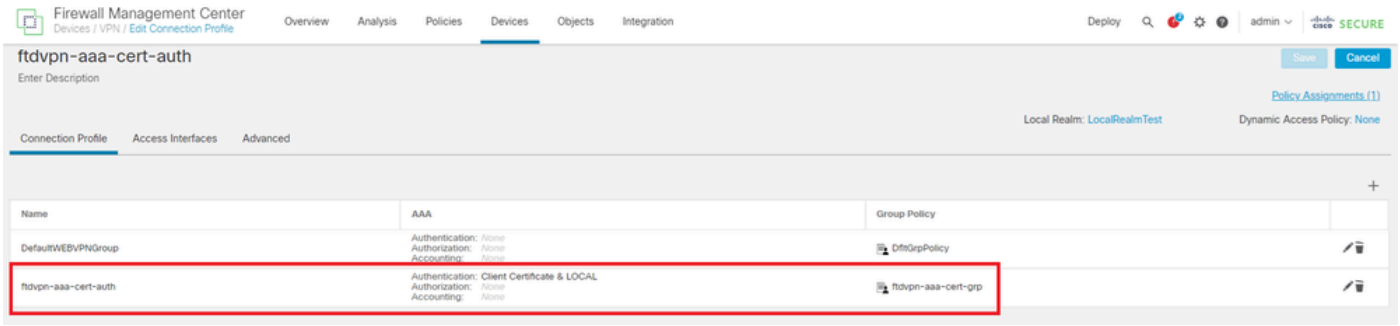
Stap 9. Samenvatting voor verbindingsprofiel bevestigen

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



Instellingen voor VPN-verbinding bevestigen

Bevestig de samenvatting van het VPN-beleid voor externe toegang en implementeer de instellingen voor FTD.



Samenvatting van VPN-beleid voor externe toegang

Bevestigen in FTD CLI

Bevestig de instellingen van de VPN-verbinding in de FTD CLI na implementatie vanuit het FMC.

```
// Defines IP of interface
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 192.168.1.200 255.255.255.0
interface GigabitEthernet0/1
nameif inside
security-level 0
ip address 192.168.10.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftdvpn-aaa-cert-pool 172.16.1.40-172.16.1.50 mask 255.255.255.0

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

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftdvpn-cert
keypair ftdvpn-cert
crl configure

// Server Certificate Chain
crypto ca certificate chain ftdvpn-cert
certificate 22413df584b6726c
3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7
......
quit
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
......
quit

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

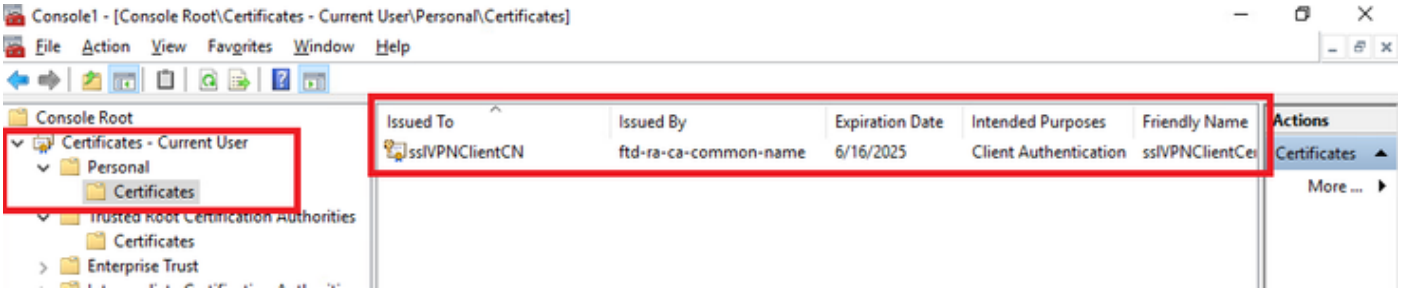
```
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Bypass Access Control policy for decrypted traffic
// This setting is displayed in the 'show run all' command output
sysopt connection permit-vpn

// Configures the group-policy to allow SSL connections
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-grp attributes
banner none
wins-server none
dns-server none
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools none
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
anyconnect ssl keepalive 20
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable

// Configures the tunnel-group to use the aaa & certificate authentication
tunnel-group ftdvpn-aaa-cert-auth type remote-access
tunnel-group ftdvpn-aaa-cert-auth general-attributes
address-pool ftdvpn-aaa-cert-pool
default-group-policy ftdvpn-aaa-cert-grp
// These settings are displayed in the 'show run all' command output. Start
authentication-server-group LOCAL
secondary-authentication-server-group none
```

```
no accounting-server-group
default-group-policy ftdvpn-aaa-cert-grp
username-from-certificate CN OU
secondary-username-from-certificate CN OU
authentication-attr-from-server primary
authenticated-session-username primary
username-from-certificate-choice second-certificate
secondary-username-from-certificate-choice second-certificate
// These settings are displayed in the 'show run all' command output. End
tunnel-group ftdvpn-aaa-cert-auth webvpn-attributes
authentication aaa certificate
pre-fill-username client
group-alias ftdvpn-aaa-cert-auth enable
```

Bevestigen in VPN-client

Stap 1. Clientcertificaat bevestigen

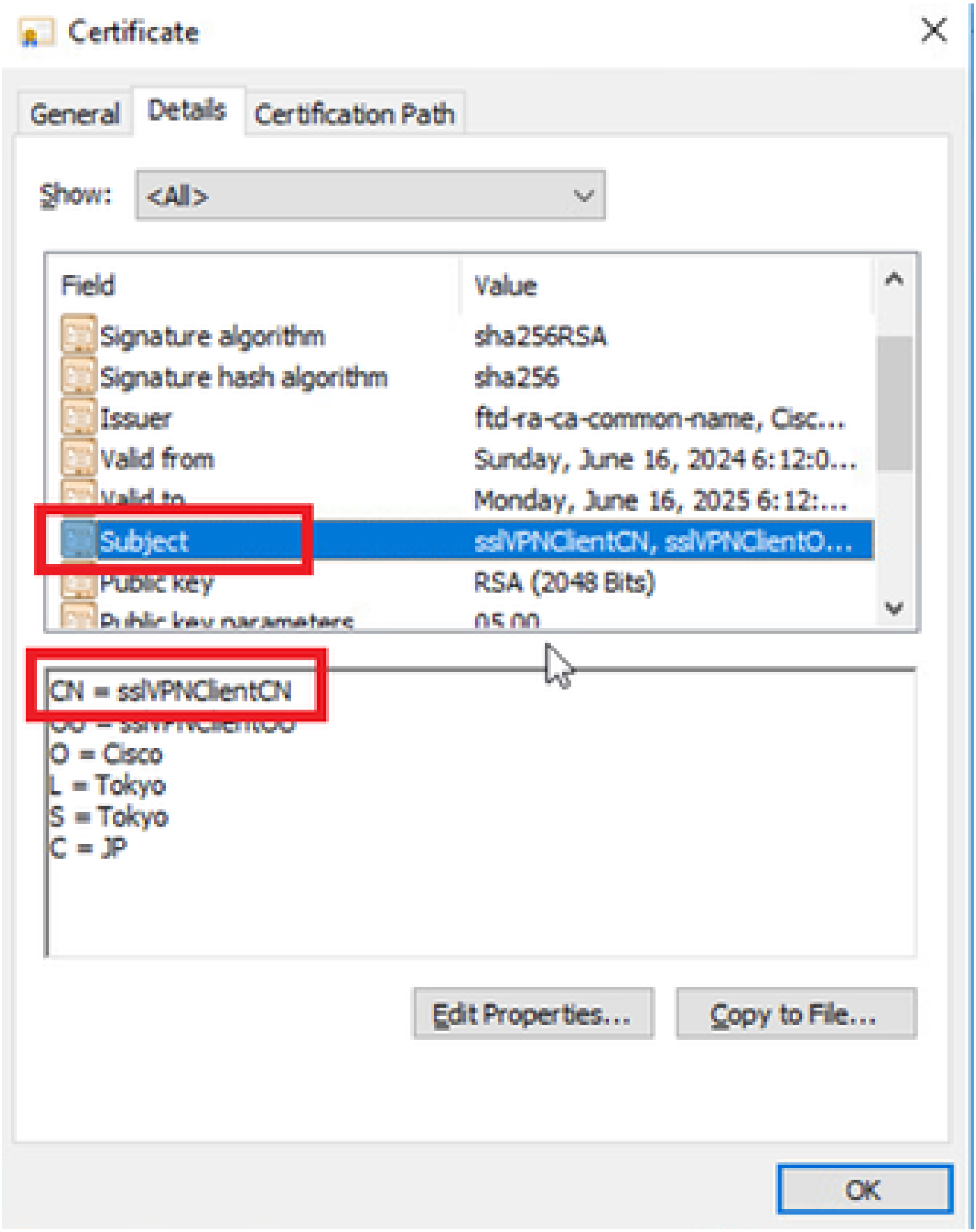
Navigeer naar Certificaten - Huidige gebruiker > Persoonlijk > Certificaten, controleer het clientcertificaat dat wordt gebruikt voor verificatie.



Clientcertificaat bevestigen

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

- Betreft: CN = sslVPNClientCN



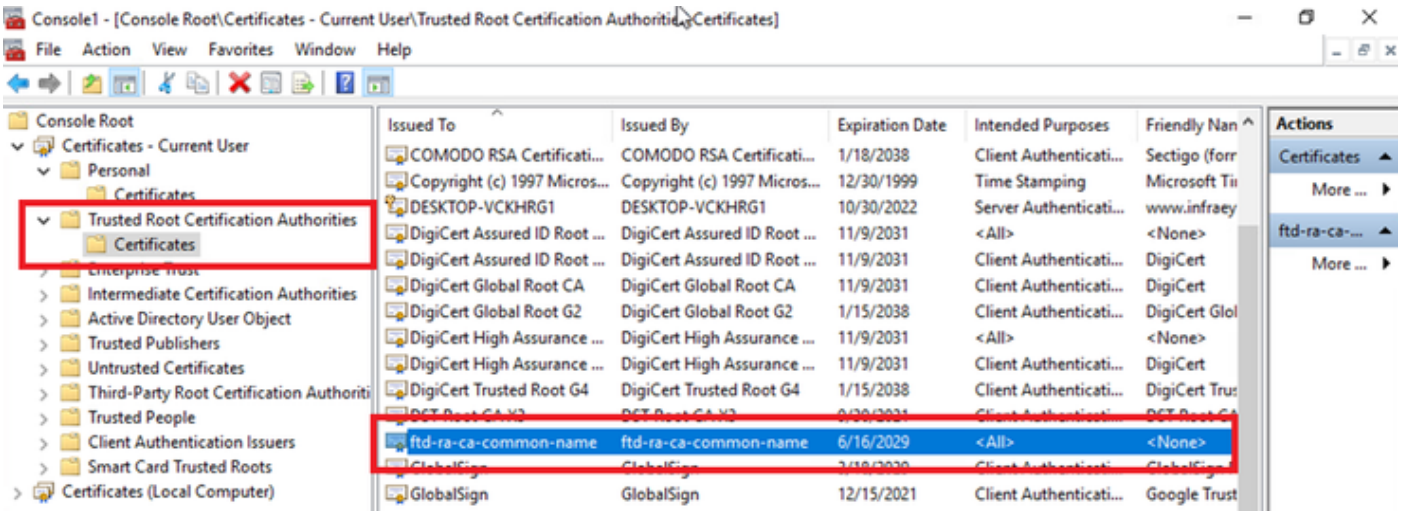
Details van clientcertificaat

Stap 2. Bevestig CA

Ga naar Certificaten - Huidige gebruiker > Trusted Root Certification Authorities > Certificates,

controleer de CA die gebruikt wordt voor verificatie.

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

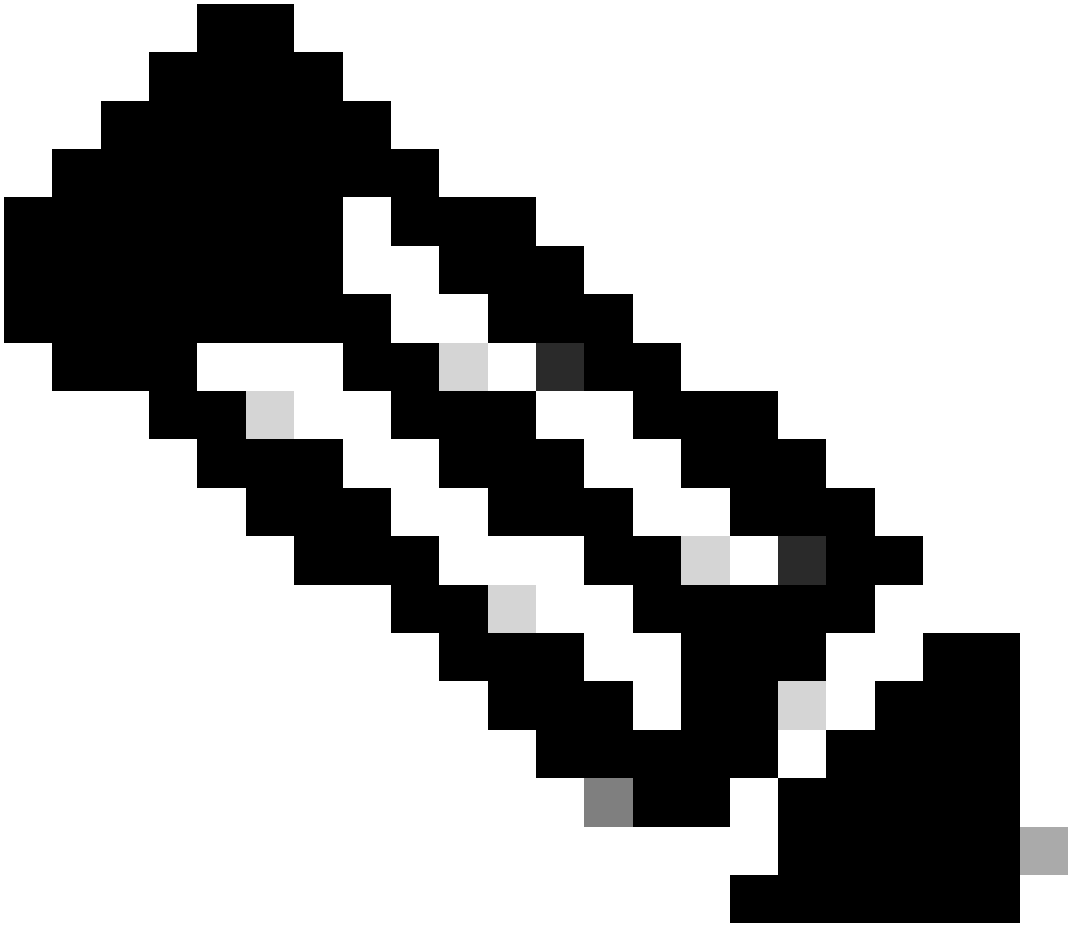


Bevestig CA

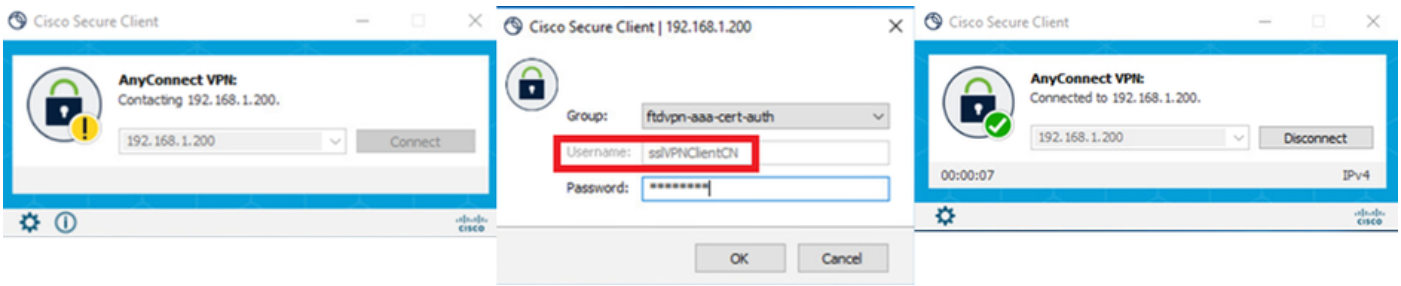
Verifiëren

Stap 1. VPN-verbinding starten

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



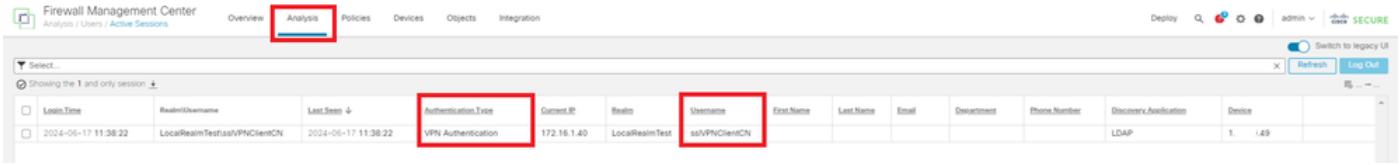
Opmerking: De gebruikersnaam is afgeleid uit het veld CN (Common Name) van het clientcertificaat in dit document.



VPN-verbinding starten

Stap 2. Bevestig actieve sessies in VCC

Navigeer naar Analyse > Gebruikers > Actieve sessies en controleer de actieve sessie op VPN-verificatie.



Bevestig actieve sessie

Stap 3. VPN-sessie in FTD CLI bevestigen

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

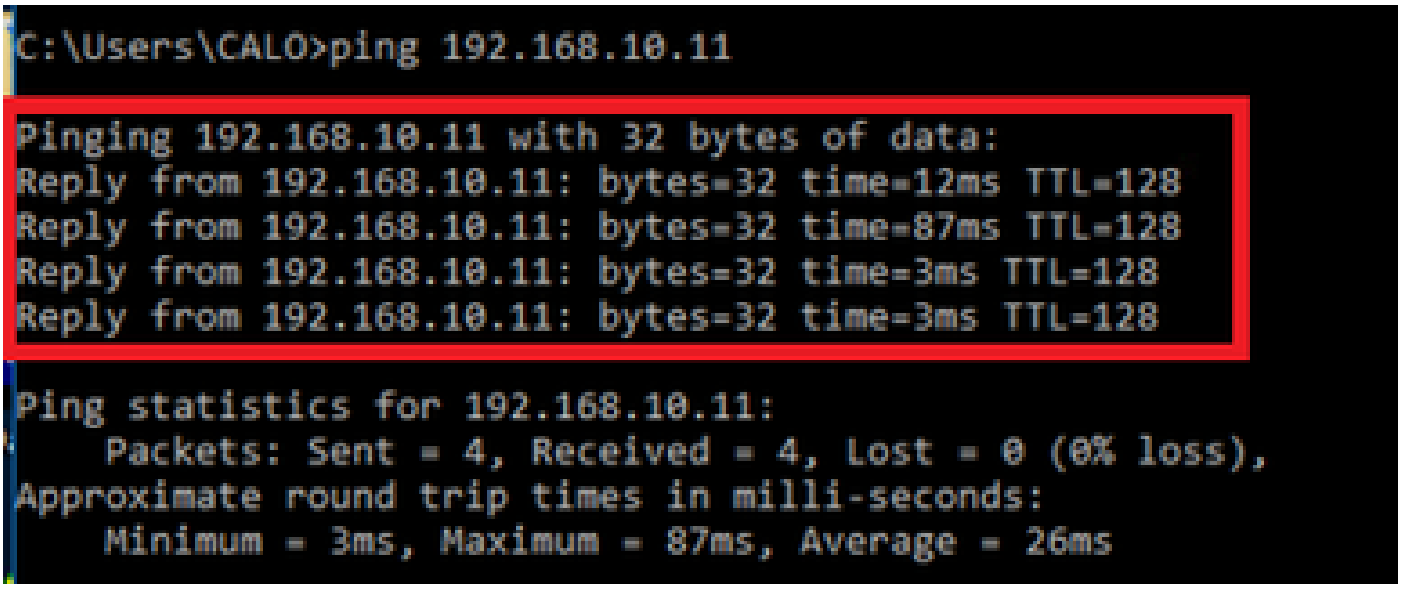
```
ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 7
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 14780 Bytes Rx : 15386
Pkts Tx : 2 Pkts Rx : 37
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth
Login Time : 02:38:22 UTC Mon Jun 17 2024
Duration : 0h:01m:22s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb00718200007000666fa19e
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 7.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50035 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7390 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 7.2
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-128 Hashing : SHA256
```

Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 50042
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7390 Bytes Rx : 2292
Pkts Tx : 1 Pkts Rx : 3
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 7.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 56382
UDP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 0 Bytes Rx : 13094
Pkts Tx : 0 Pkts Rx : 34
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Stap 4. Communicatie met server bevestigen

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



Ping gelukt

capture in interface inside real-time Start de opdracht in FTD (Lina) CLI om pakketopname te bevestigen.

ftd702#

```
capture in interface inside real-time


Use ctrl-c to terminate real-time capture

1: 03:39:25.729881 172.16.1.40 > 192.168.10.11 icmp: echo request
2: 03:39:25.730766 192.168.10.11 > 172.16.1.40 icmp: echo reply
3: 03:39:26.816211 172.16.1.40 > 192.168.10.11 icmp: echo request
4: 03:39:26.818683 192.168.10.11 > 172.16.1.40 icmp: echo reply
5: 03:39:27.791676 172.16.1.40 > 192.168.10.11 icmp: echo request
6: 03:39:27.792195 192.168.10.11 > 172.16.1.40 icmp: echo reply
7: 03:39:28.807789 172.16.1.40 > 192.168.10.11 icmp: echo request
8: 03:39:28.808399 192.168.10.11 > 172.16.1.40 icmp: echo reply
```

Problemen oplossen

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

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

```
// Certificate Authentication
Jun 17 2024 02:38:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=sslV
Jun 17 2024 02:38:03: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked.
Jun 17 2024 02:38:03: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name:  CN=sslVPNClientCl

// Extract username from the CN (Common Name) field
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has been requested.  [Request 5]
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has completed.  [Request 5]

// AAA Authentication
Jun 17 2024 02:38:22: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN
Jun 17 2024 02:38:22: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN
Jun 17 2024 02:38:22: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN
```

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

Referentie

AnyConnect Remote Access VPN configureren op FTD

AnyConnect-certificaatgebaseerde verificatie voor mobiele toegang configureren

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.