IPv6-compatibele RAVPN configureren met AAA-verificatie op FTD beheerd door FDM

Inhoud

Inleiding

In dit document worden de stappen beschreven voor het configureren van een voor IPv6 geschikte externe VPN-toegang met AAA-verificatie op FTD die wordt beheerd door FDM.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure FDM Virtual 7.6.0
- Cisco Secure FTD Virtual 7.6.0
- Cisco Secure Client 5.1.6.103

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.

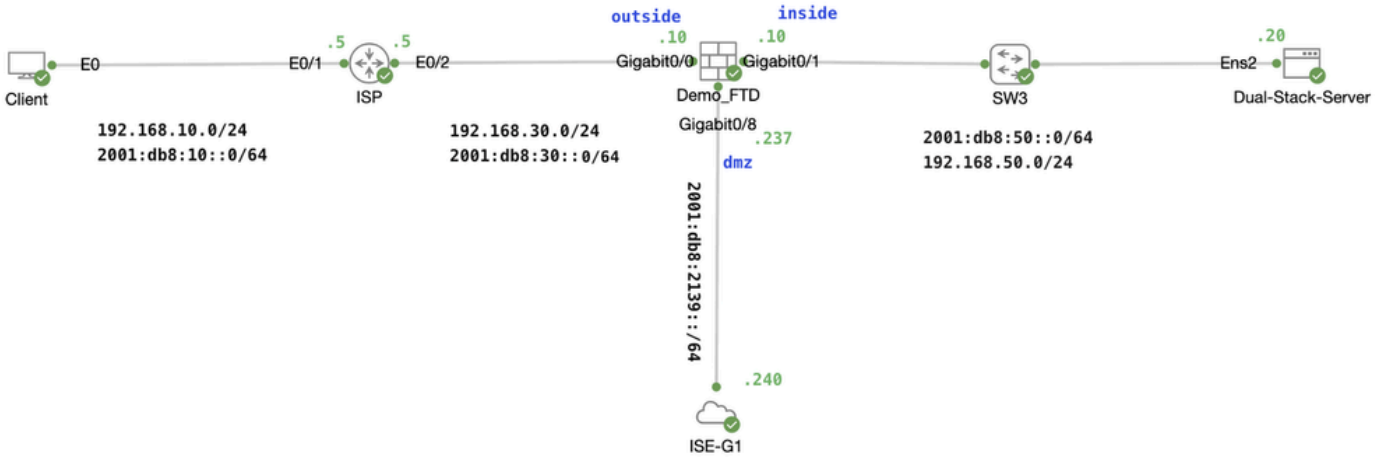
Achtergrondinformatie

IPv6 Remote Access VPN (RAVPN) wordt steeds belangrijker naarmate de wereld overgaat van IPv4 naar IPv6, omdat IPv4-adressen beperkt zijn en bijna uitgeput zijn, terwijl IPv6 een vrijwel onbeperkte adresruimte biedt, rekening houdend met het groeiende aantal met internet verbonden apparaten. Naarmate meer netwerken en services naar IPv6 gaan, zorgt de IPv6-mogelijkheid ervoor dat uw netwerk compatibel en toegankelijk blijft. IPv6 RAVPN helpt organisaties zich voor te bereiden op de toekomst van netwerken en zorgt voor veilige en schaalbare connectiviteit op afstand.

In dit voorbeeld communiceert de client met de VPN-gateway met behulp van een IPv6-adres dat door de serviceprovider is opgegeven, maar ontvangt zowel IPv4- als IPv6-adressen uit de VPN-pools, waarbij de Cisco Identity Service Engine (ISE) wordt gebruikt als bron voor de verificatie-identiteit. De ISE is alleen geconfigureerd met een IPv6-adres. De interne server is geconfigureerd met zowel IPv4- als IPv6-adressen, die hosts met twee stapels vertegenwoordigen. De client heeft toegang tot interne bronnen met het IPv4- of IPv6 VPN-adres, indien van toepassing.

Configureren

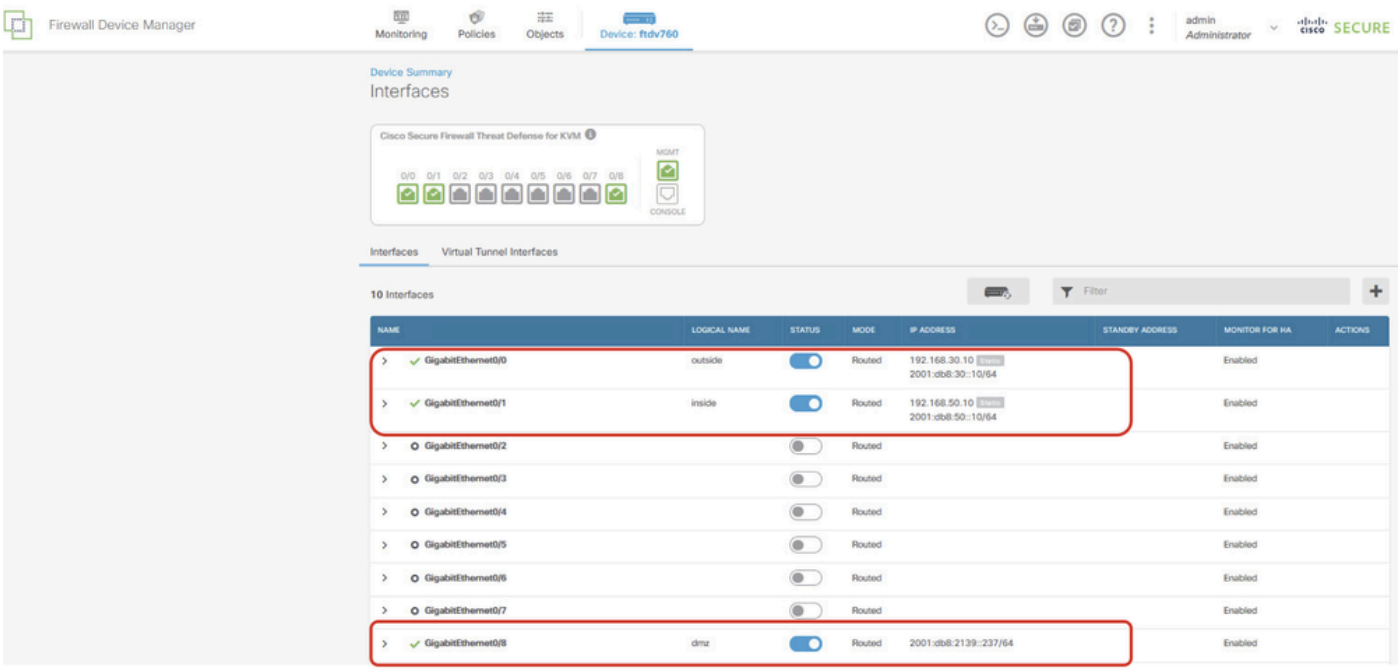
Netwerkdiagram



Topologie

Configuraties op FDM

Stap 1. Het is van essentieel belang ervoor te zorgen dat de voorlopige configuratie van IPv4- en IPv6-interconnectie tussen knooppunten naar behoren is voltooid. De gateway van client en FTD is een gerelateerd ISP-adres. De gateway van de server bevindt zich binnen het IP van FTD. De ISE bevindt zich in het DMZ-gebied van FTD.

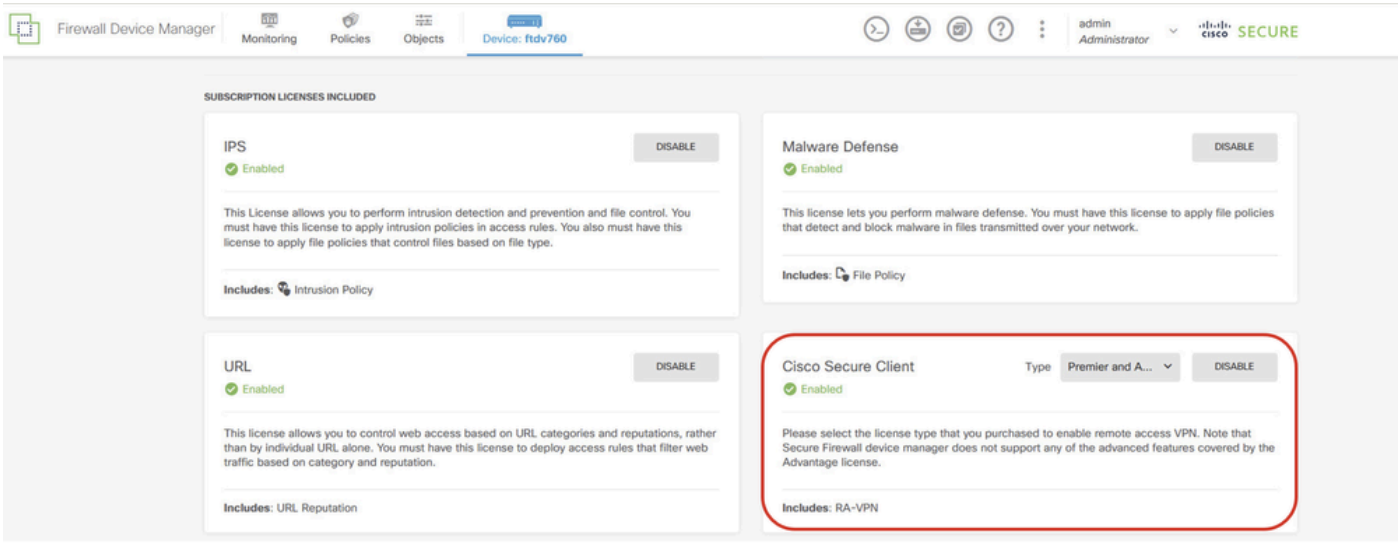


FTD_Interface_IP

FTD_Default_Route

Stap 2. Download het Cisco Secure Client-pakket namecisco-secure-client-win-5.1.6.103-webdeploy-k9.pkg van Cisco Software Download en zorg ervoor dat het bestand goed is na het downloaden door te bevestigen dat de md5 checksum van het gedownloade bestand hetzelfde is als de Cisco Software Download pagina.

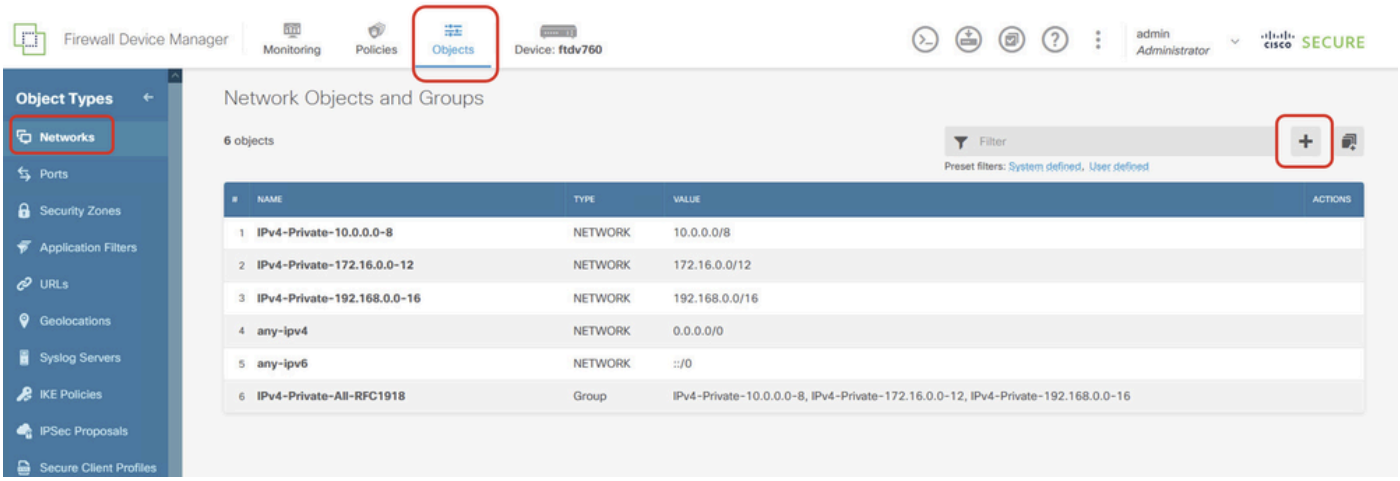
Stap 3. Controleer of RAVPN-gerelateerde licenties zijn ingeschakeld op FTD.



FDM_License

Stap 4. VPN-adresgroep maken.

Stap 4.1. IPv6- en IPv4-adresgroep maken door netwerkobjecten te maken. Navigeer naar Objecten > Netwerken en klik op de + knop.

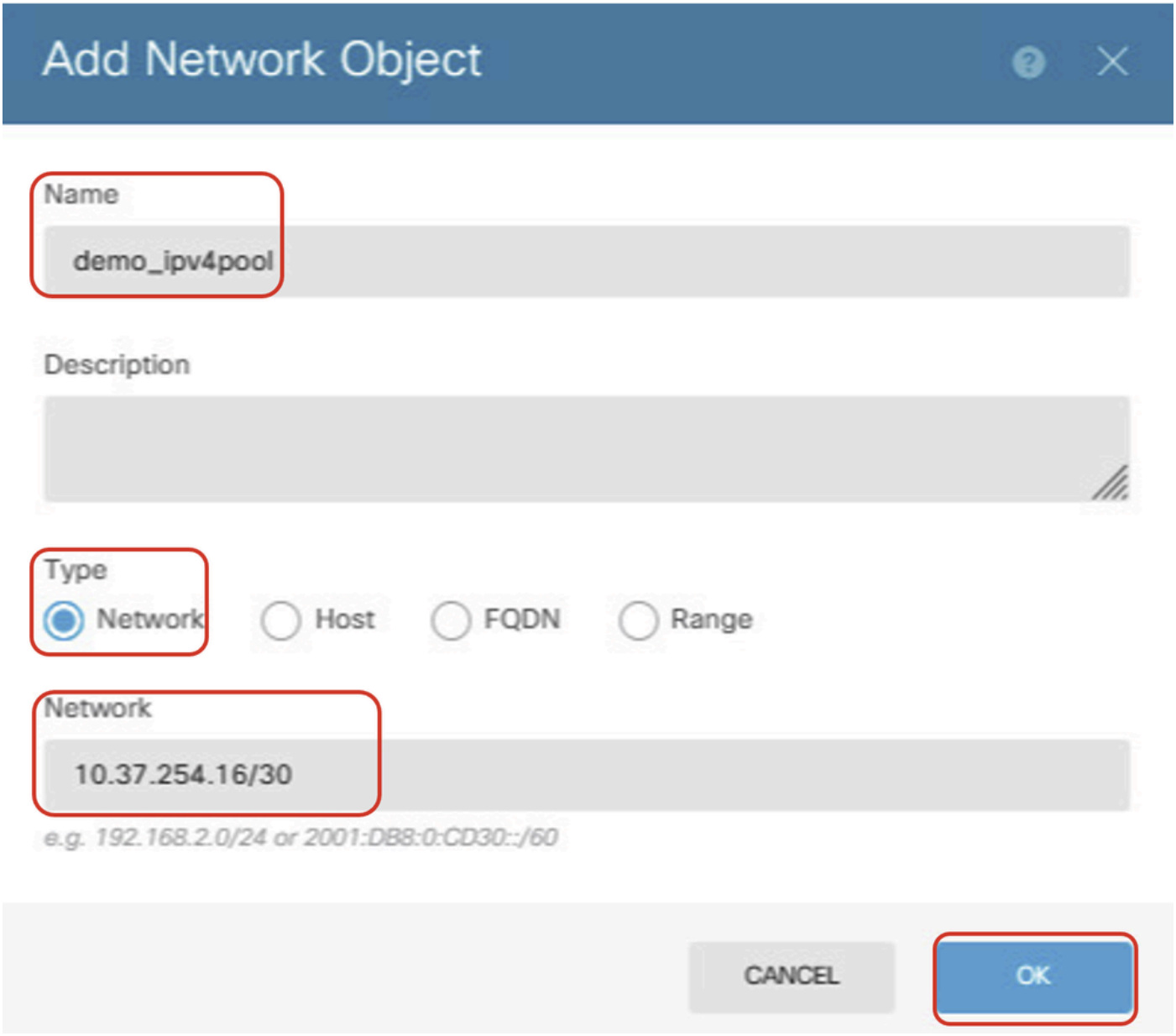


Create_VPN_Address_Pool_1

Stap 4.2. Verstrek de nodige informatie over elk netwerkobject. Klik op de knop OK.

Voor de IPv4-pool kan het objecttype worden gekozen met Netwerk of Bereik. In dit voorbeeld wordt het objecttype Network gekozen voor demodoeleinden.

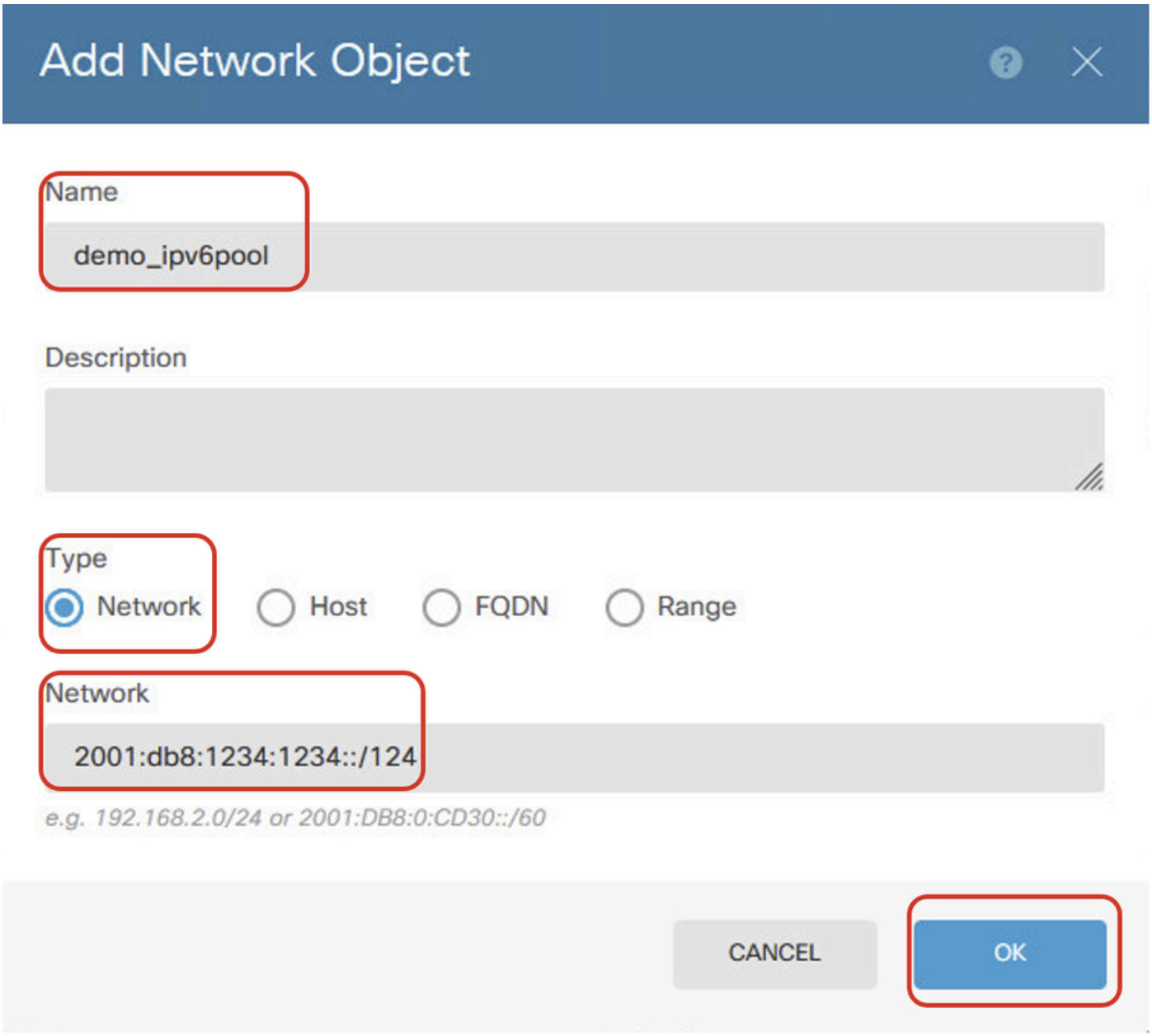
- Naam: demo_ipv4pool
- Type: netwerk
- Netwerk: 10.37.254.16/30



Create_VPN_Address_Pool_2_IPv4

Voor de IPv6-pool kan vanaf nu alleen het objecttype met Netwerk worden gekozen.

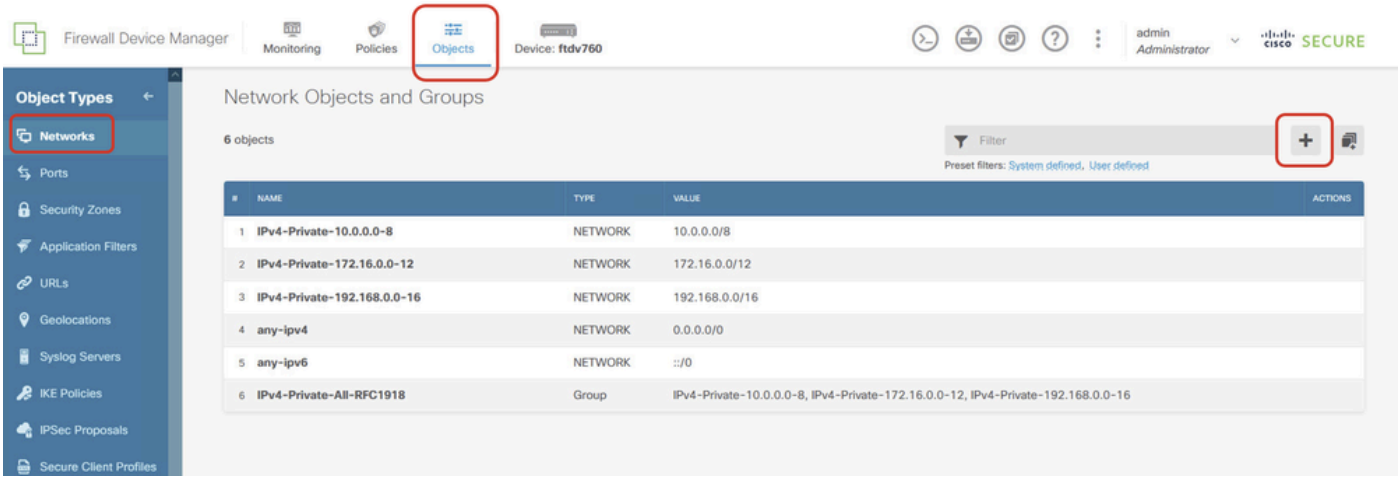
- Naam: demo_ipv6pool
- Type: netwerk
- Netwerk: 2001:db8:1234:1234::/124



Create_VPN_Address_Pool_2_IPv6

Stap 5. Maak het interne netwerk voor NAT-vrijstelling.

Stap 5.1. Navigeer naar Objecten > Netwerken en klik op de knop +.

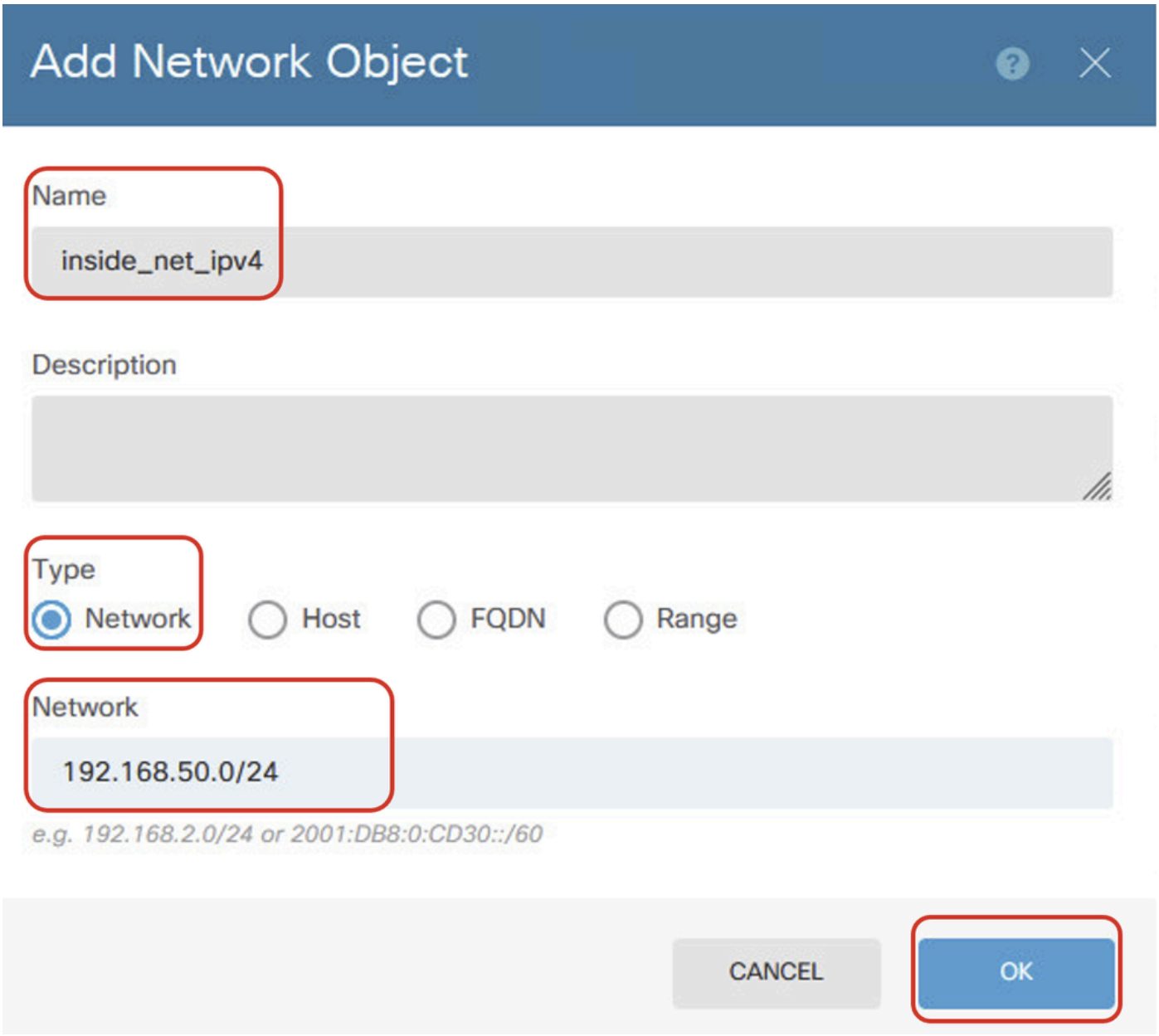


Create_NAT_Exempt_Network_1

Stap 5.2. Verstrek de benodigde informatie over elk netwerkobject. Klik op de knop OK.

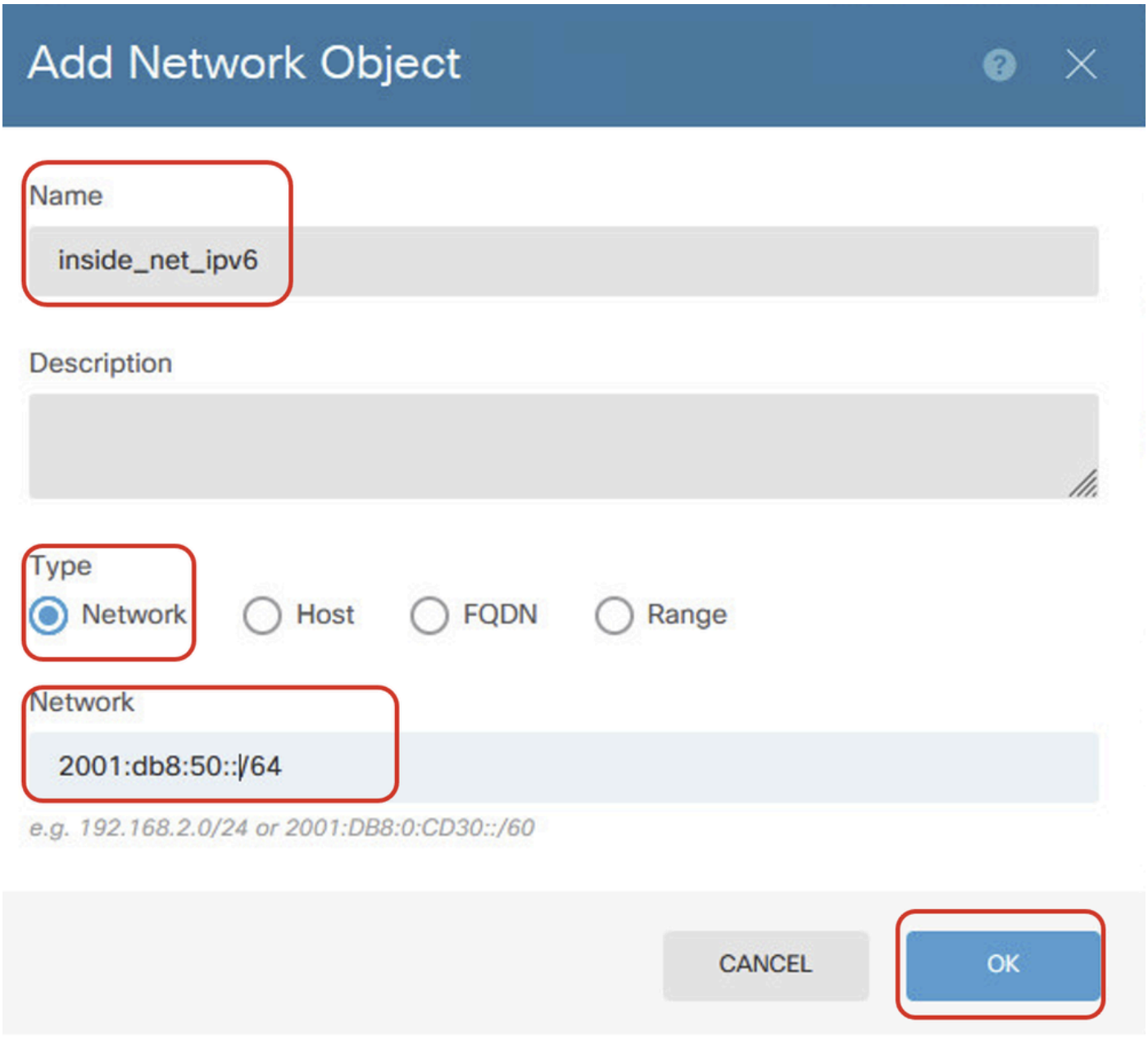
In dit voorbeeld worden zowel IPv4- als IPv6-netwerken geconfigureerd.

- Naam: inside_net_ipv4
- Type: netwerk
- Netwerk: 192.168.50.0/24



Create_NAT_Exempt_Network_2_IPv4

- Naam: inside_net_ipv6
- Type: netwerk
- Netwerk: 2001:db8:50::/64

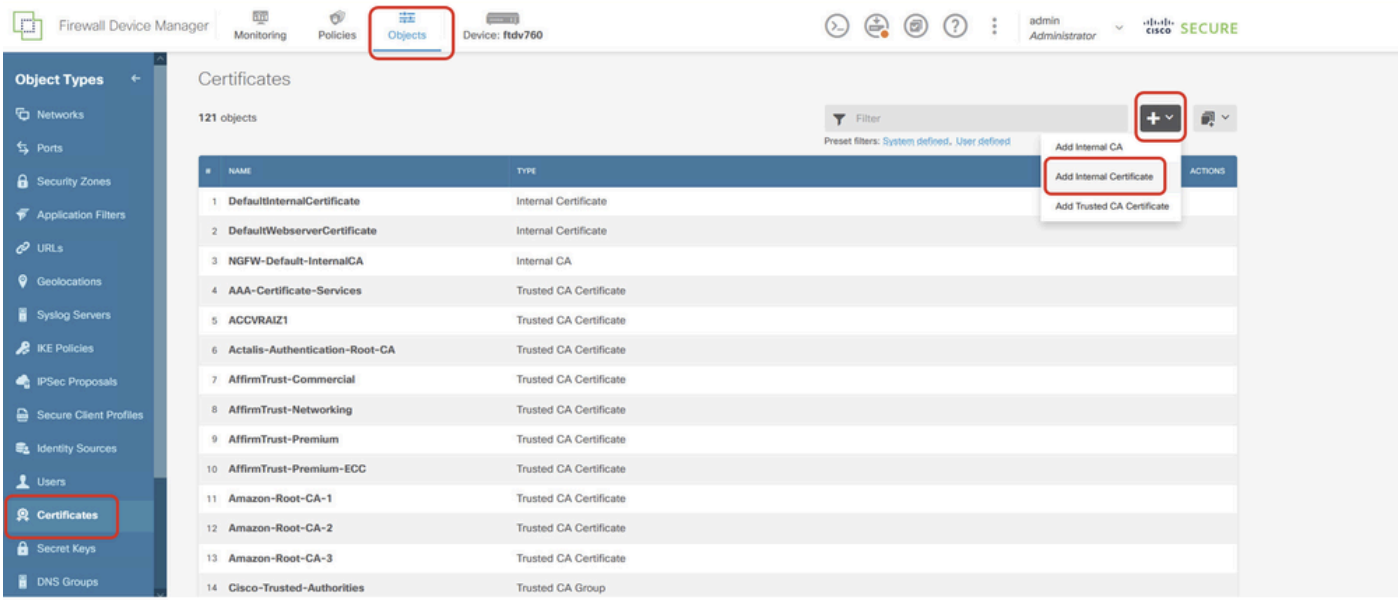


Create_NAT_Exempt_Network_2_IPv6

Stap 6. Maak een certificaat dat wordt gebruikt voor RAVPN. U hebt twee opties: u kunt een certificaat uploaden dat is ondertekend door een certificeringsinstantie van een derde partij of een nieuw zelf ondertekend certificaat genereren.

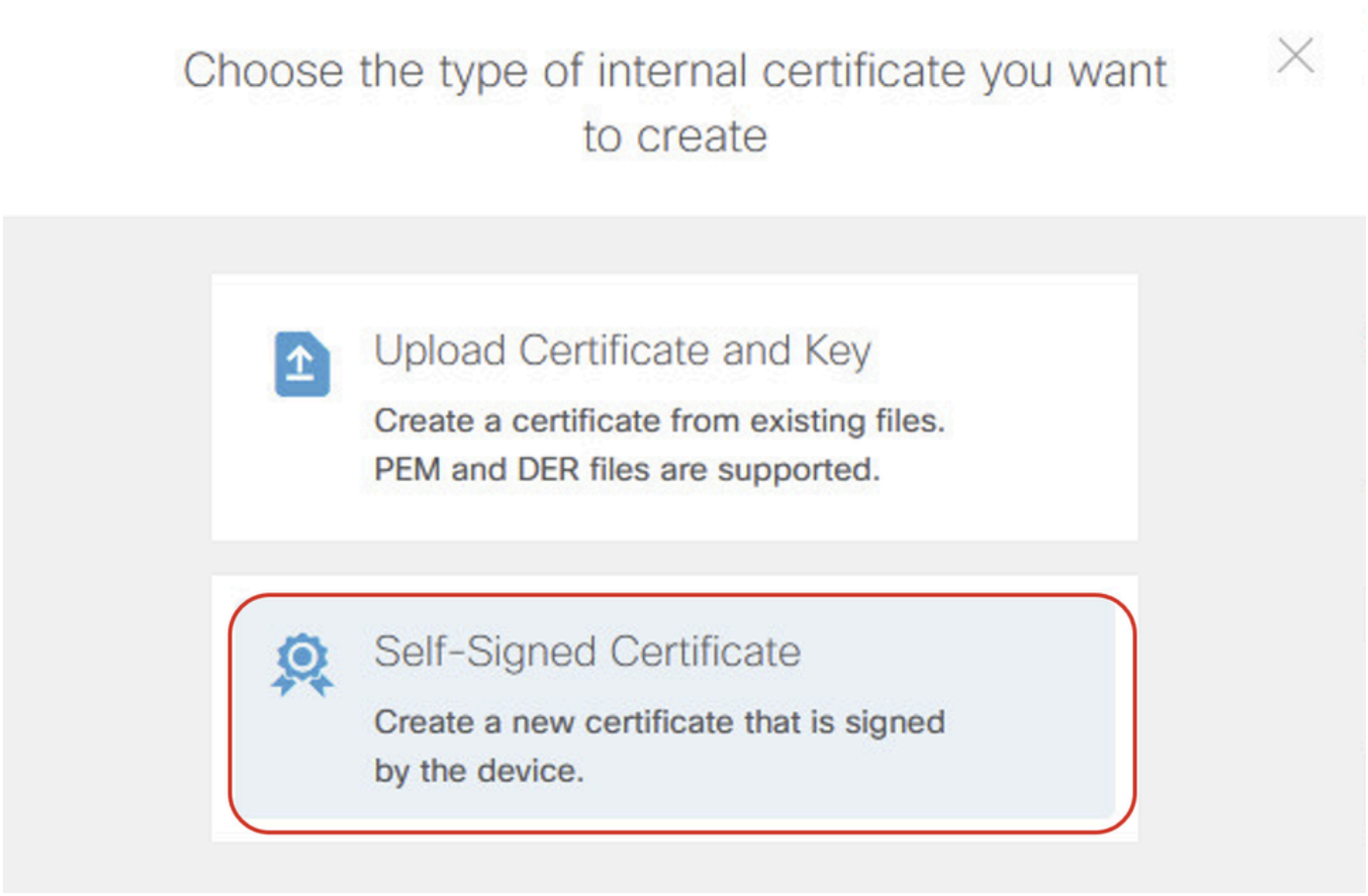
In dit voorbeeld wordt een nieuw zelf ondertekend certificaat gebruikt met aangepaste inhoud van het certificaat voor demodoeleinden.

Stap 6.1. Ga naar Objecten > Certificaten. Klik op de knop + en kies Intern certificaat toevoegen.



Create_Certificate_1

Stap 6.2. Klik op Certificaat met eigen handtekening.



Stap 6.3. Klik op het tabblad Algemeen en geef de benodigde informatie op.

Naam: demovpn

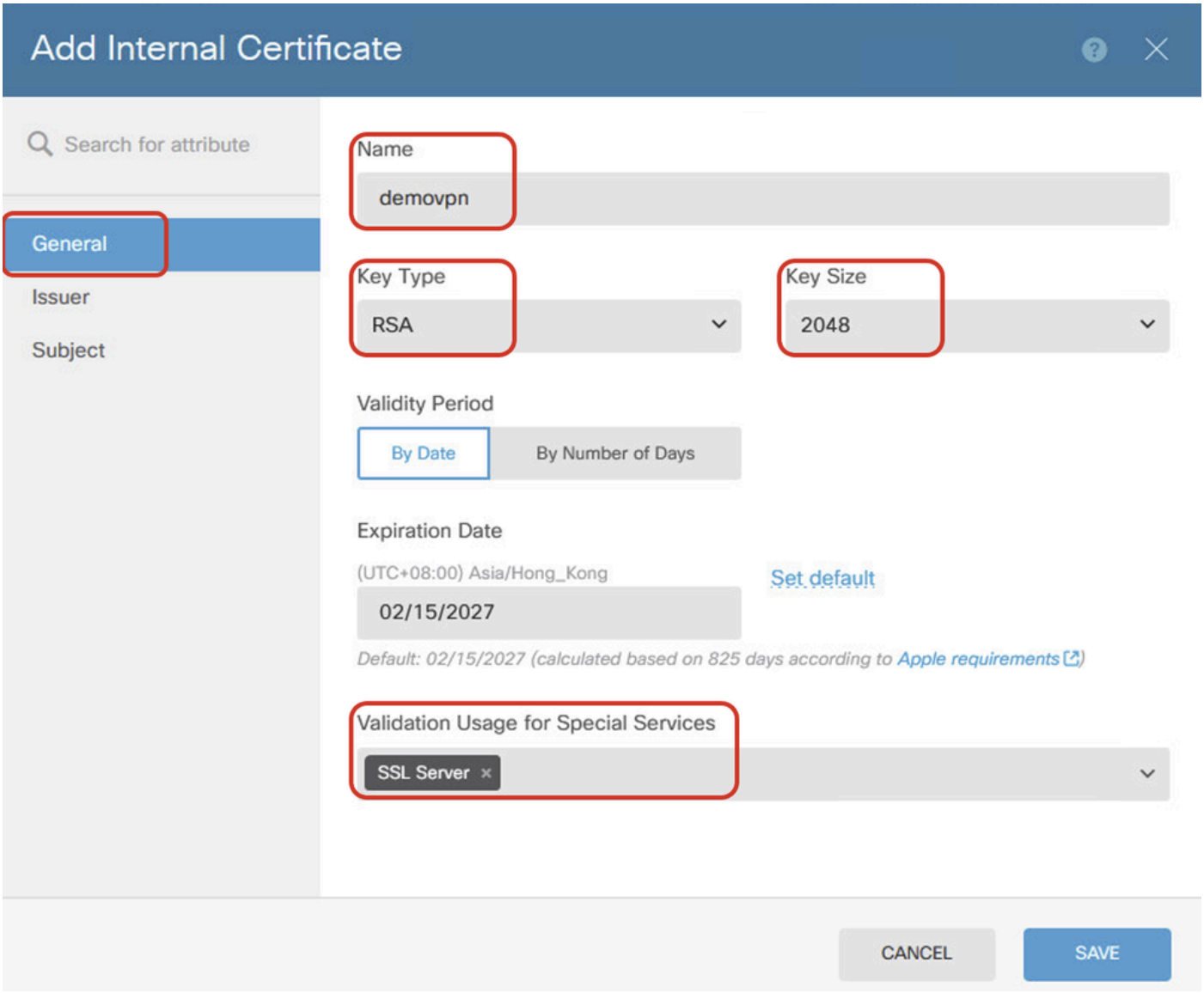
Soort sleutel: RSA

Sleutelgrootte: 2048

Geldigheidsduur: Standaard

Vervaldatum: standaard

Gebruik van validatie voor speciale services: SSL-server

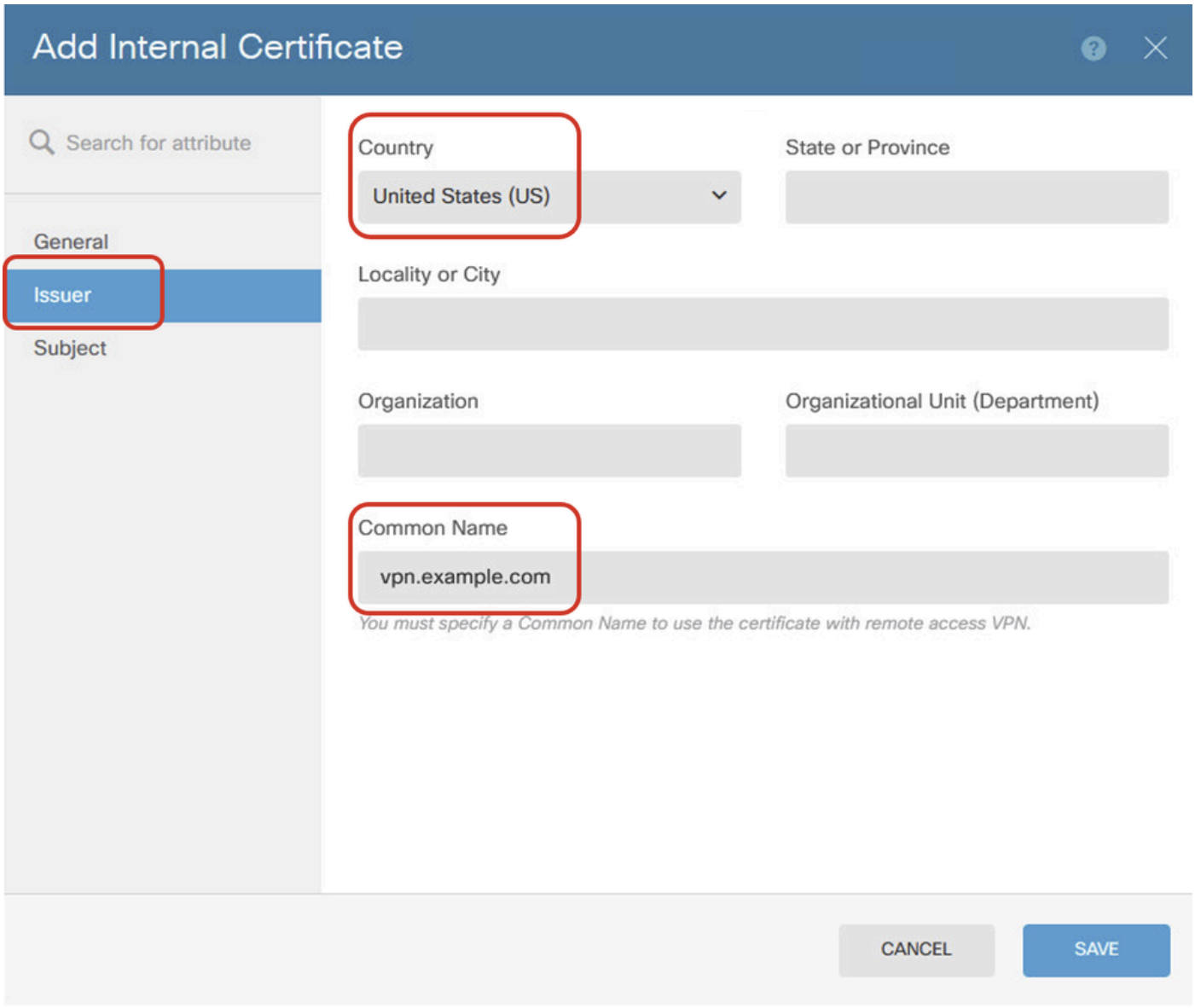


Create_Certificate_3

Stap 6.4. Klik op het tabblad Uitgever en geef de benodigde informatie op.

Land: Verenigde Staten (VS)

Algemene naam: vpn.example.com

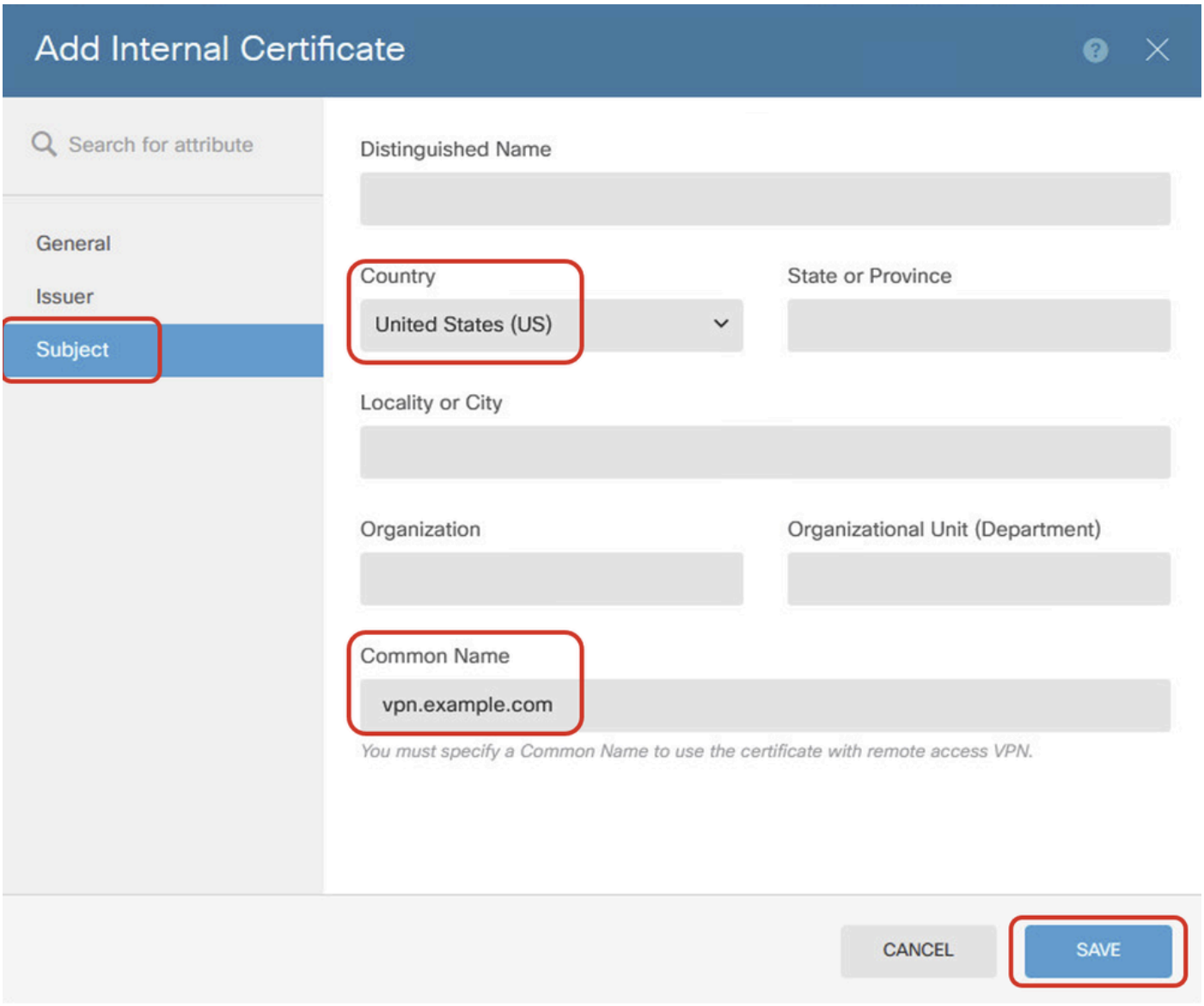


Create_Certificate_4

Stap 6.5. Klik op het tabblad Onderwerp, geef de benodigde informatie op en klik vervolgens op OPSLAAN.

Land: Verenigde Staten (VS)

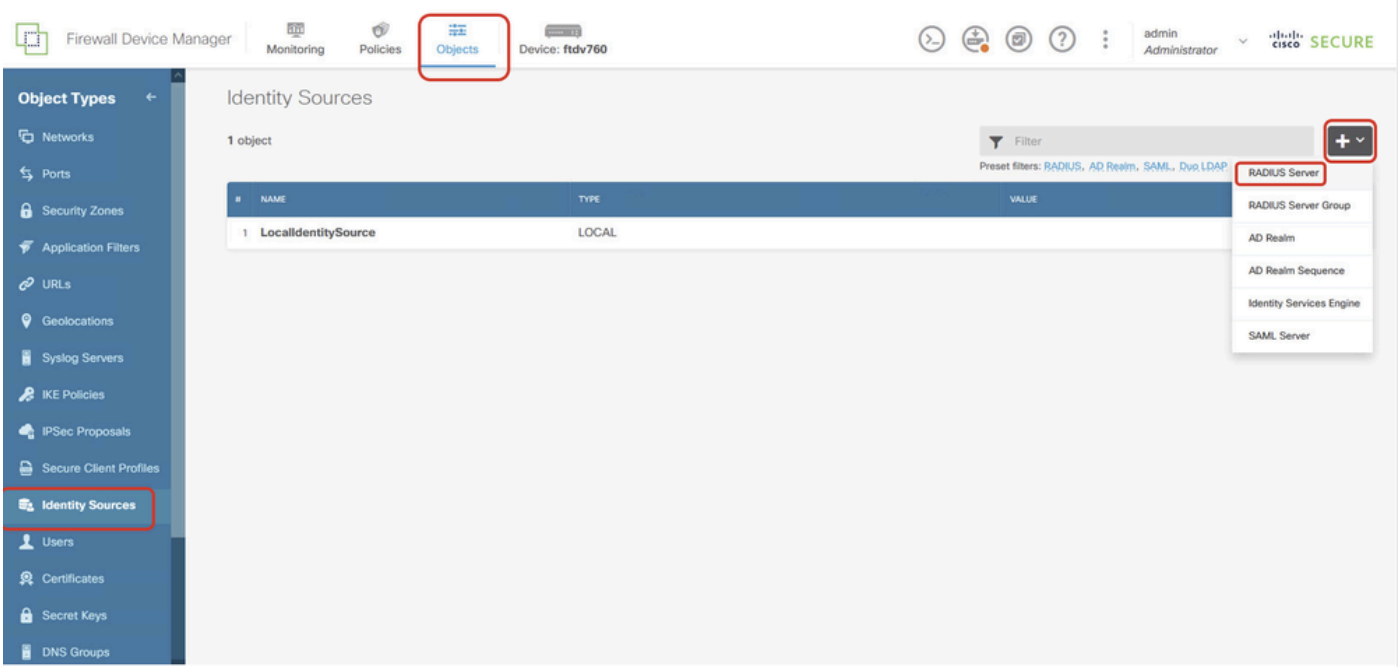
Algemene naam: vpn.example.com



Create_Certificate_5

Stap 7. Radius-server-identiteitsbron maken.

Stap 7.1. Navigeer naar Objecten > Identiteitsbronnen, klik op + en kies RADIUS Server.



Create_Radius_Source_1

Stap 7.2. Verstrek de nodige informatie over de radius-server. Klik op de knop OK.

Naam: demo_ise

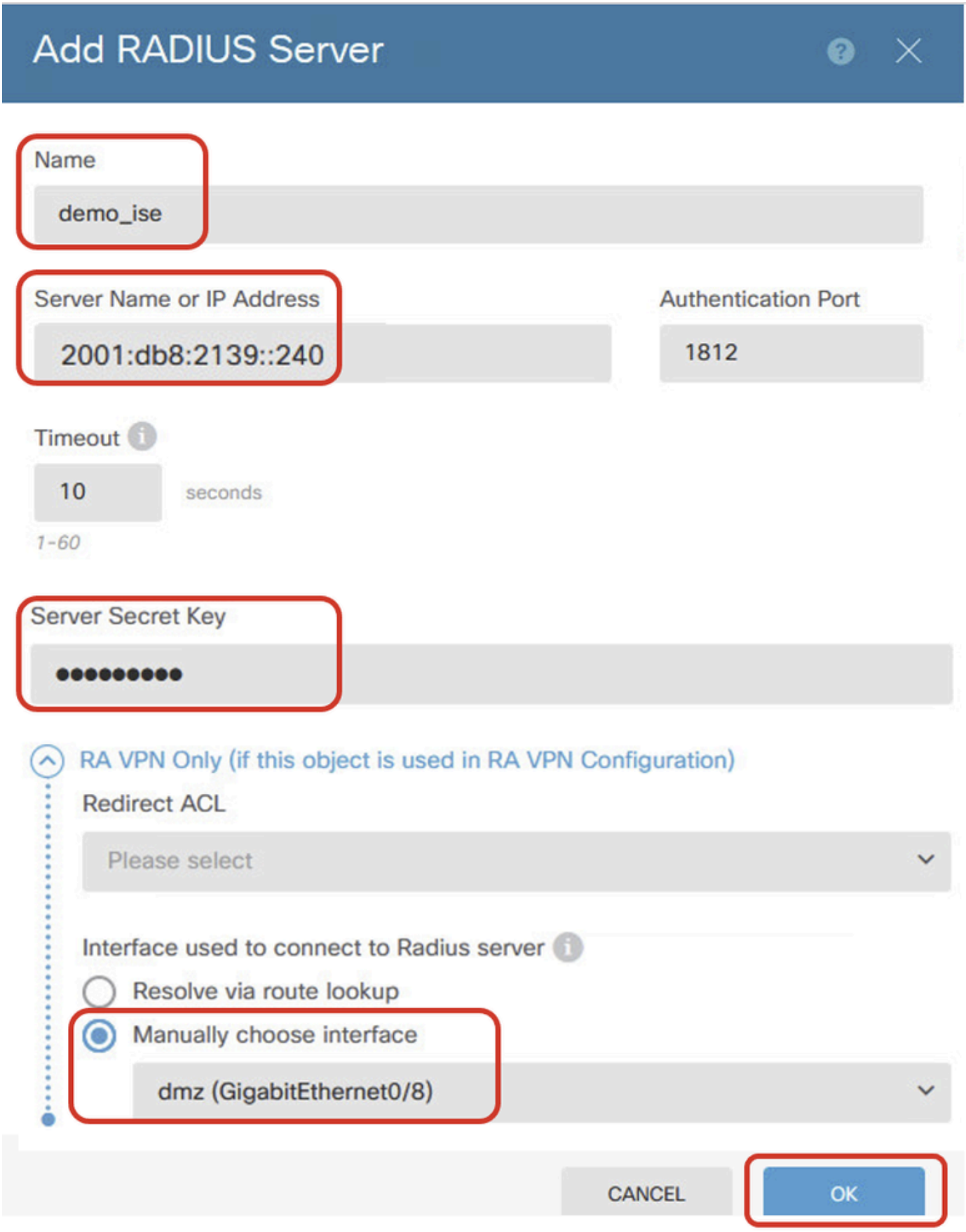
Servernaam of IP-adres: 2001:db8:2139:240

Verificatiepoort: 1812 (standaard)

Time-out: 10 (standaard)

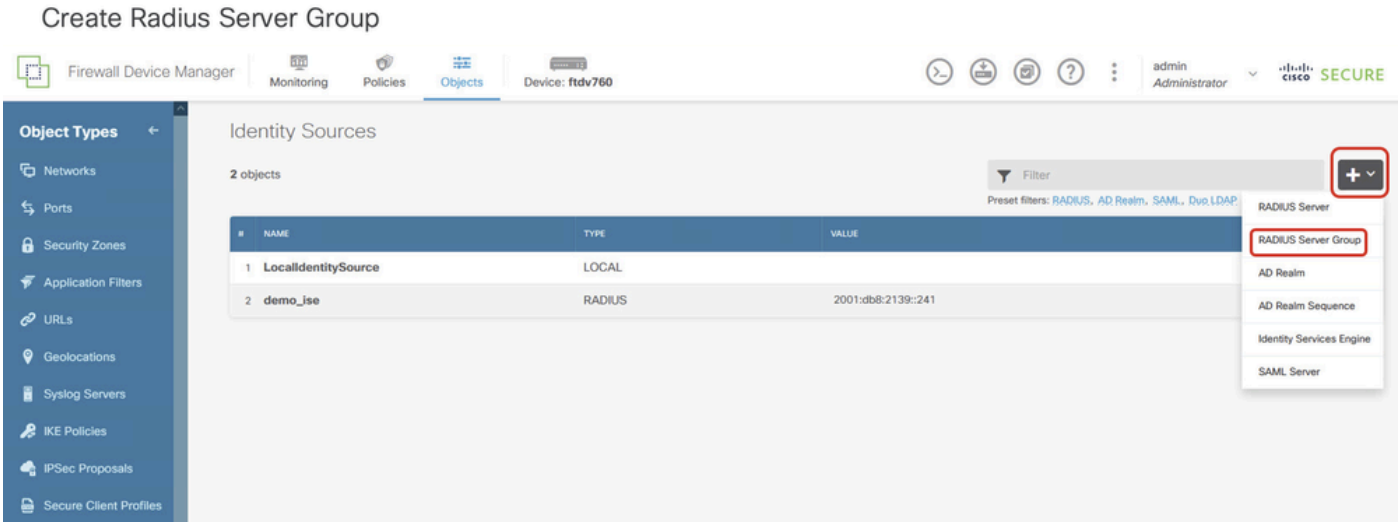
Server Secret-sleutel: cisco

Interface gebruikt om verbinding te maken met Radius-server: kies handmatig interface. Kies in dit voorbeeld dmz (Gigabit Ethernet0/8).



Create_Radius_Source_2

Stap 7.3. Ga naar Objecten > Identiteitsbronnen. Klik op de knop + en kies RADIUS-servergroep.



Create_Radius_Source_3

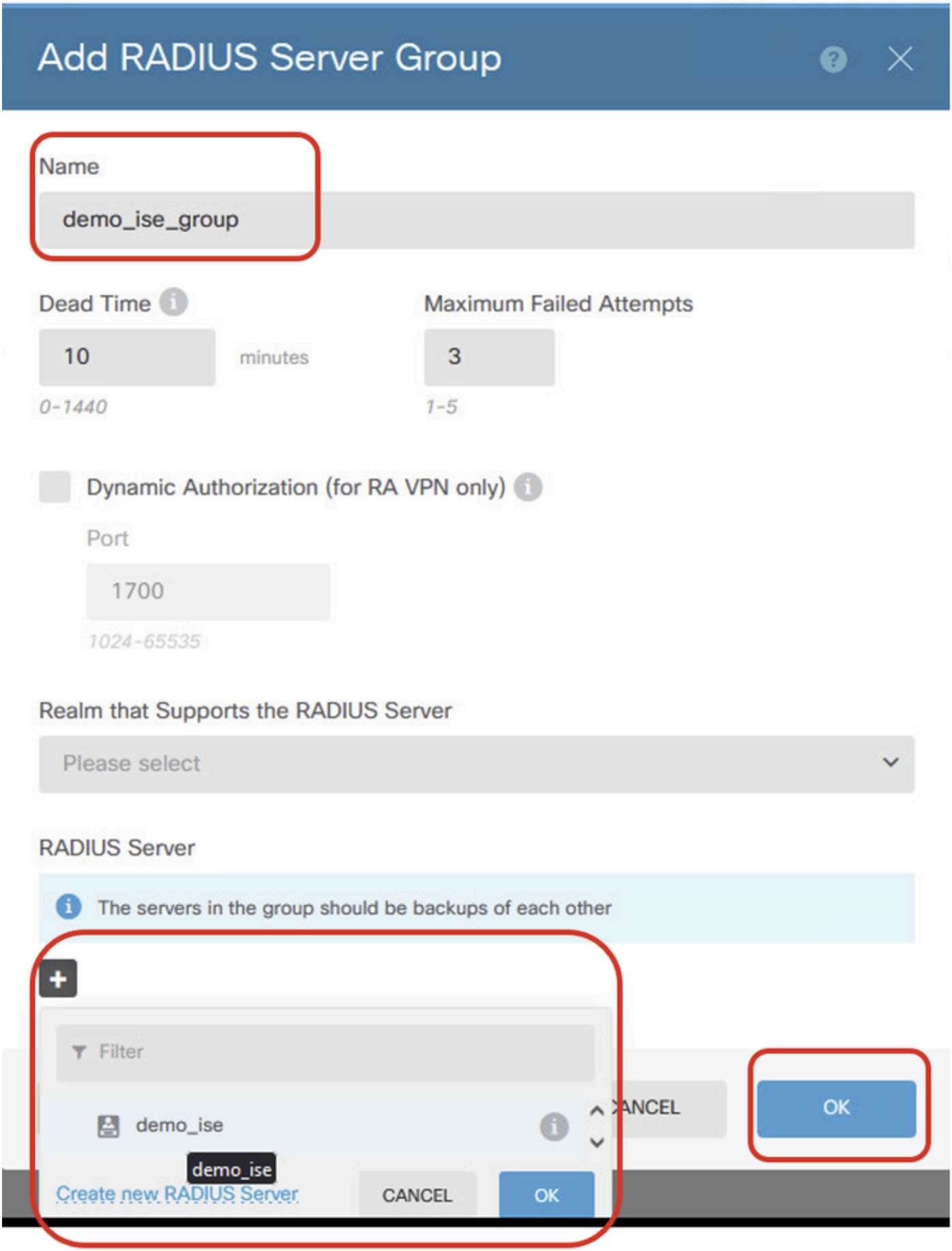
Stap 7.4. Geef de benodigde informatie over de radius-servergroep op. Klik op de knop OK.

Naam: demo_ise_group

Dode tijd: 10 (standaard)

Maximum aantal mislukte pogingen: 3 (standaard)

RADIUS-server: Klik op de knop +, selecteer de naam die is gemaakt in stap 6.2. In dit voorbeeld is het demo_ise.



Create_Radius_Source_4

Stap 8. Groepsbeleid maken dat voor RAVPN wordt gebruikt. In dit voorbeeld worden aangepaste banner- en time-outinstellingen geconfigureerd voor demodoeleinden. U kunt wijzigen op basis van uw werkelijke behoeften.

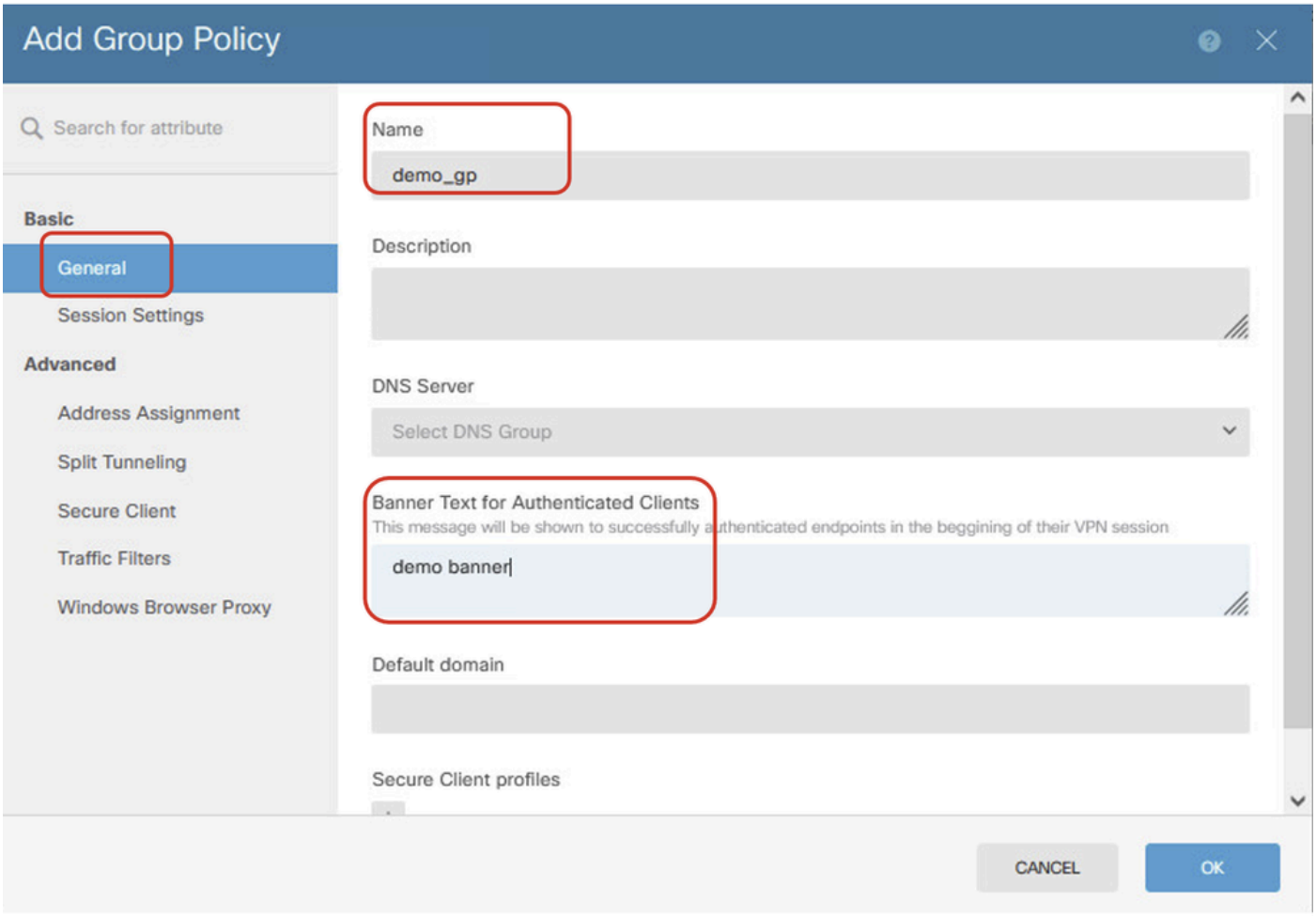
Stap 8.1. Navigeer naar Remote Access VPN > Configuratie bekijken. Klik op Groepsbeleid in de linkerzijbalk en klik op de knop +.

Create_Group_Policy_1

Stap 8.2. Klik op Algemeen en geef de benodigde informatie op.

Naam: demo_gp

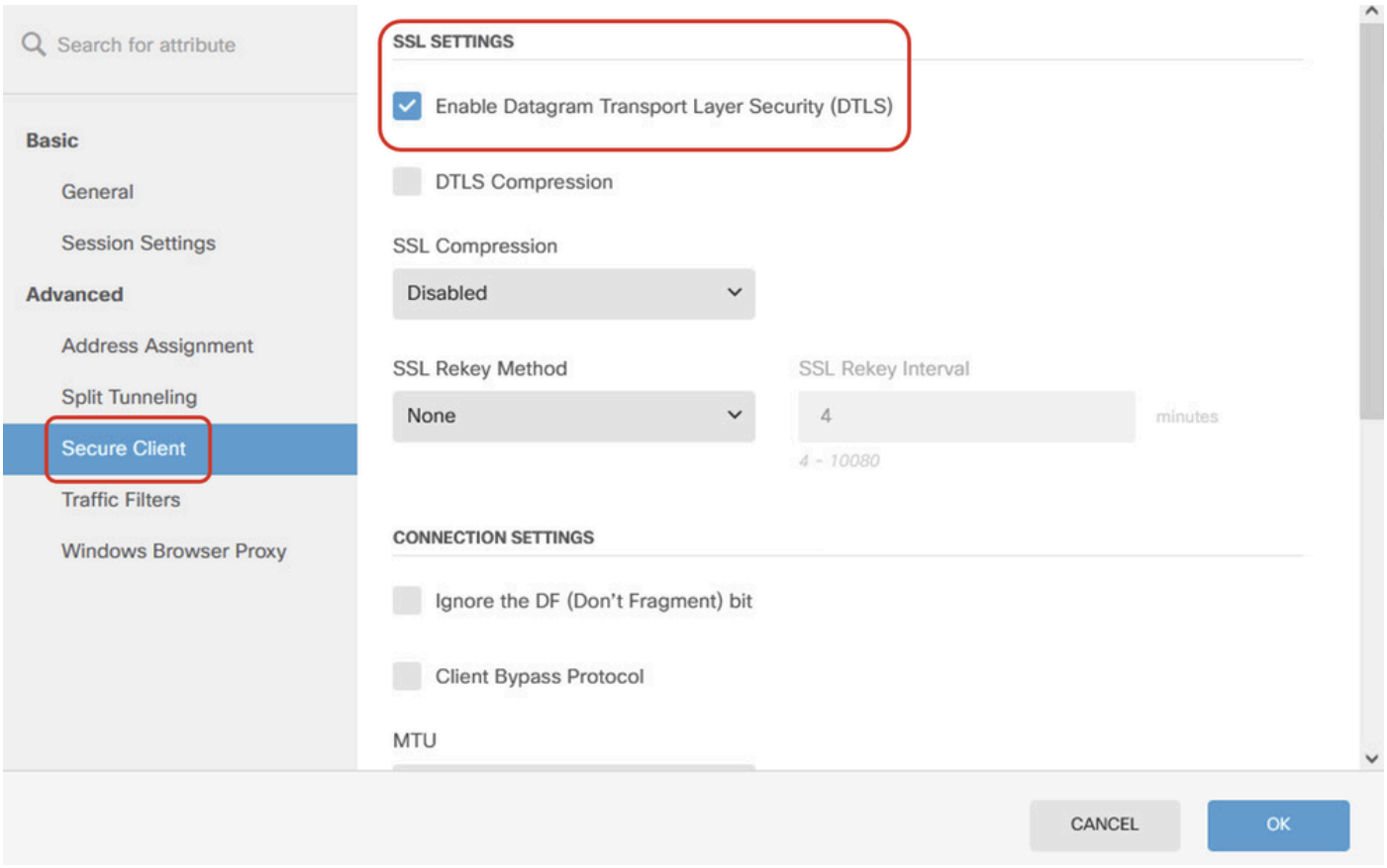
Bannertekst voor geverifieerde clients: demo-banner



Create_Group_Policy_2

Stap 8.3. Klik op Beveiligde client en geef de benodigde informatie op.

Schakel Datagram Transport Layer Security (DTLS) in.

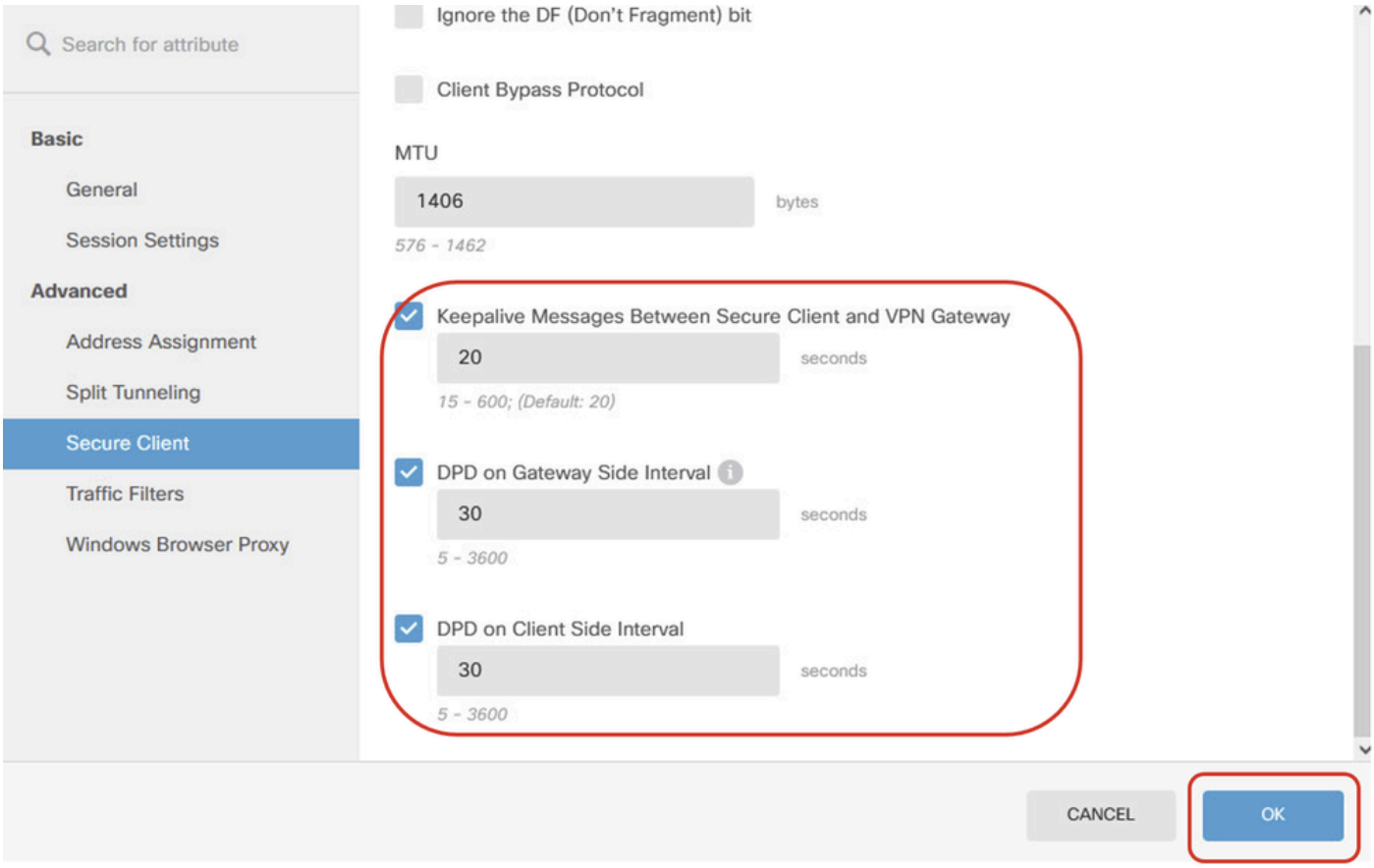


Create_Group_Policy_3

Controleer Keepalive Berichten tussen Secure Client en VPN Gateway (standaardwaarde).

Controleer DPD op Gateway Side Interval (standaardwaarde).

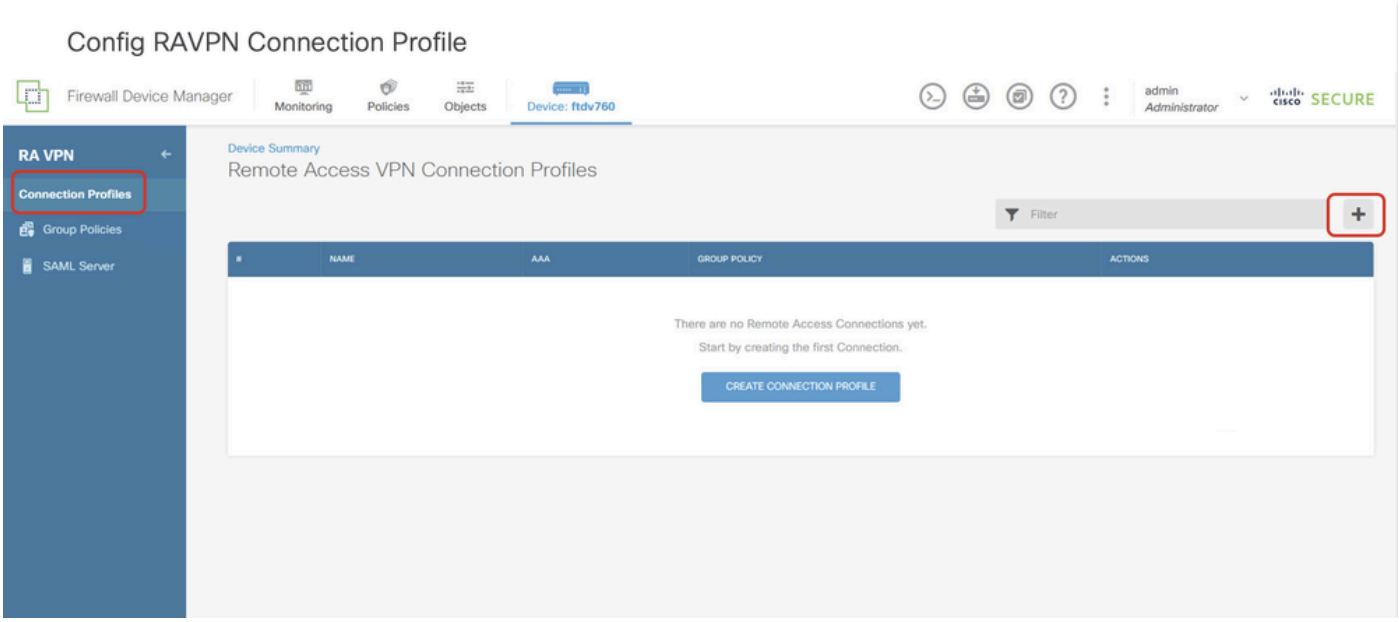
Controleer DPD op Client Side Interval (standaardwaarde).



Create_Group_Policy_3_CONT

Stap 9. Maak een RAVPN-verbindingsprofiel.

Stap 9.1. Navigeer naar Remote Access VPN > Configuratie bekijken. Klik op Verbindingsprofiel in de linkerzijbalk en klik op de + knop om de wizard te starten.

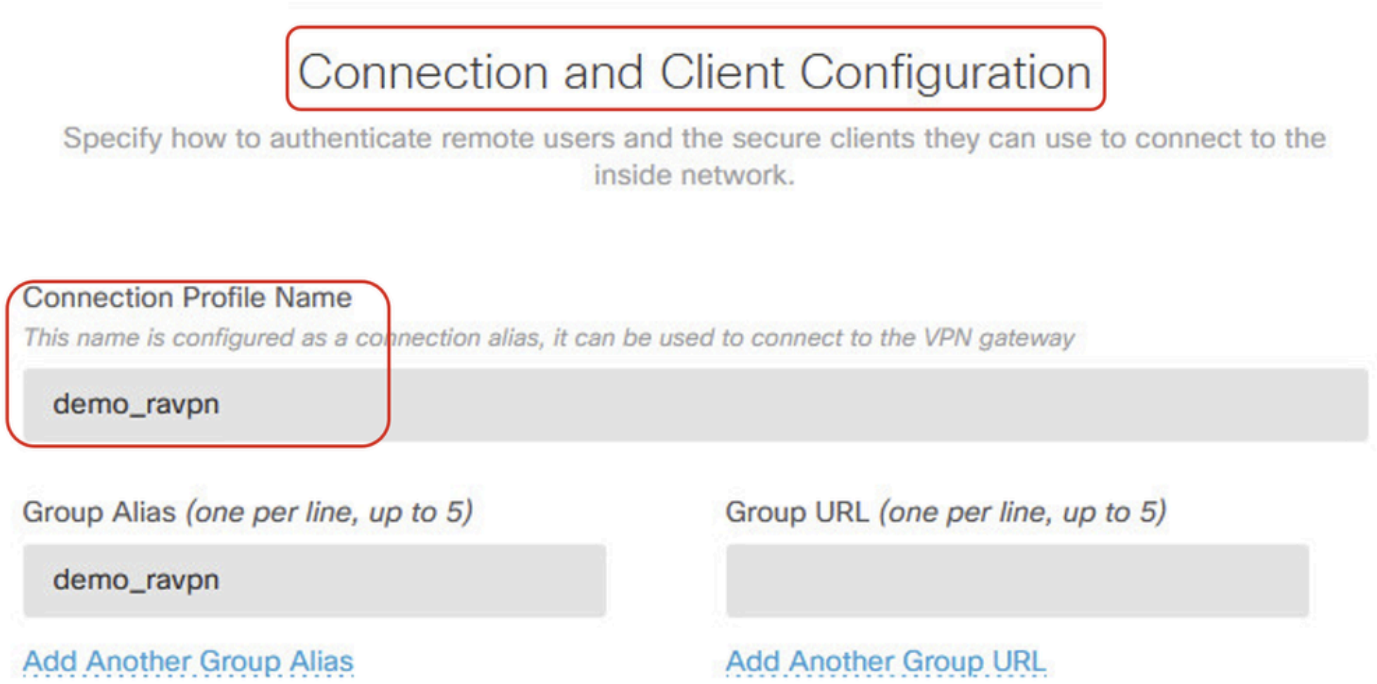


Create_RAVPN_Wizard_1

Stap 9.2. Geef de benodigde informatie op in de sectie Verbinding en clientconfiguratie en klik op de knop VOLGENDE.

Naam verbindingsprofiel: demo_ravpn

Groepsalias: demo_ravpn



Create_RAVPN_Wizard_2_Conn_Name

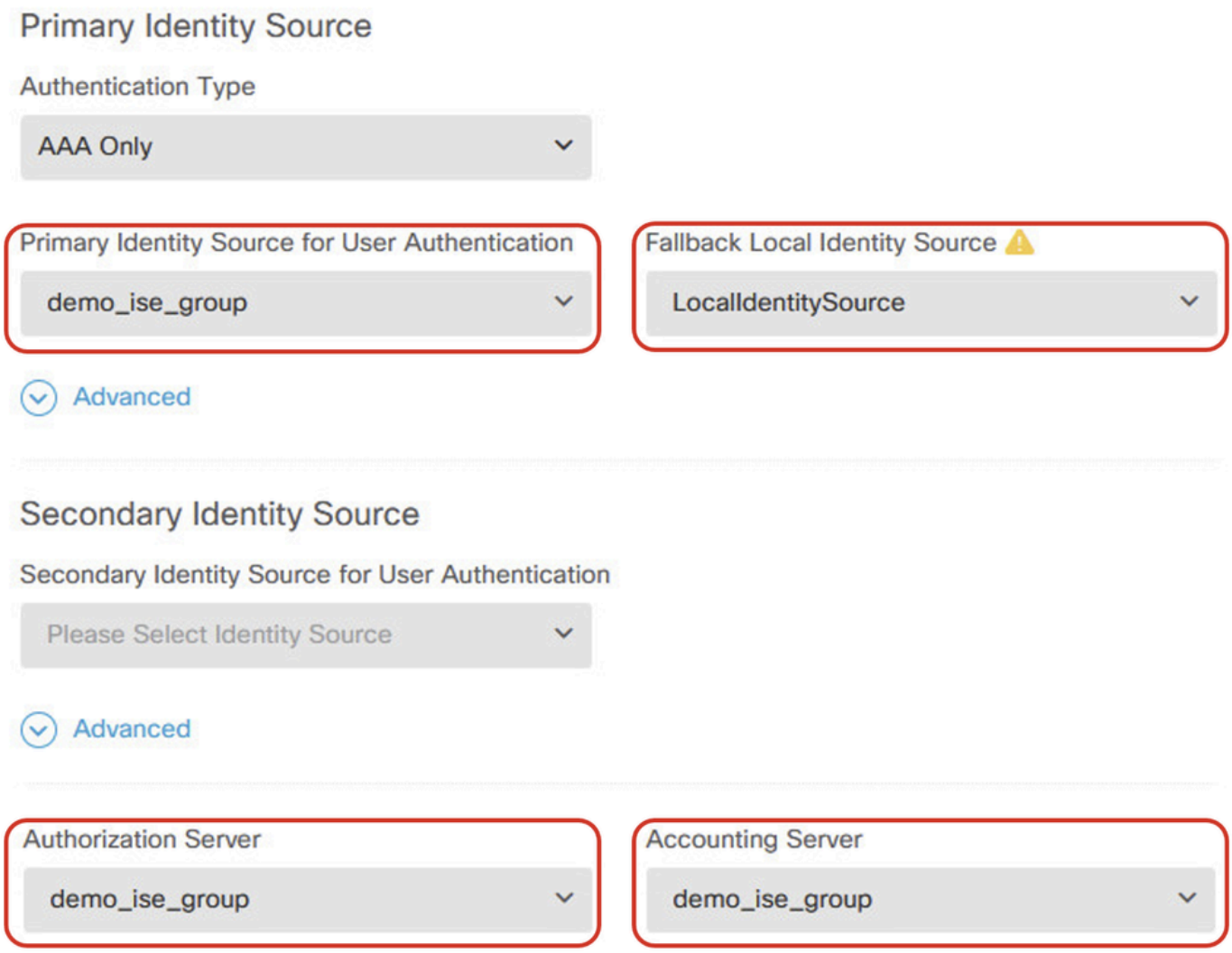
Primaire identiteitsbron > Verificatietype: alleen AAA

Primaire identiteitsbron > Primaire identiteitsbron: demo_ise_group (de naam die is geconfigureerd in stap 7.4.)

Bron lokale identiteit Fallback: LocalIdentitySource

Autorisatieserver: demo_ise_group (de naam die is geconfigureerd in stap 7.4.)

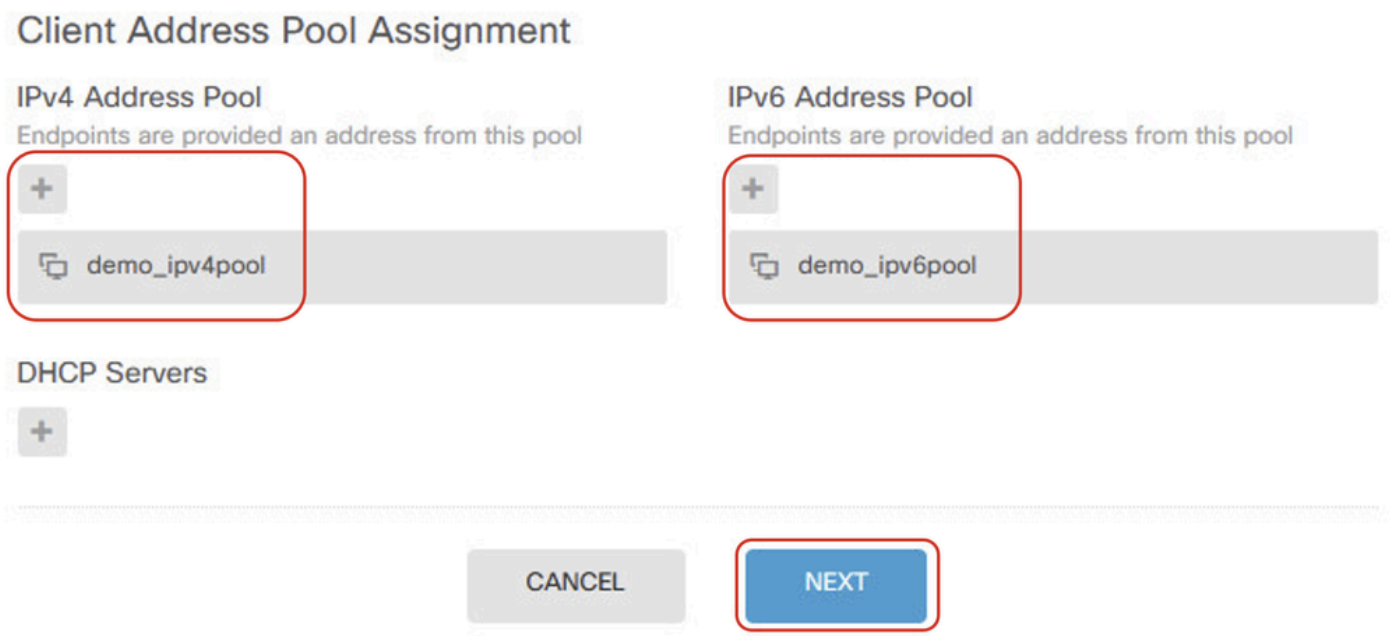
Accounting Server: demo_ise_group (de naam die is geconfigureerd in stap 7.4.)



Create_RAVPN_Wizard_2_Identity_Source

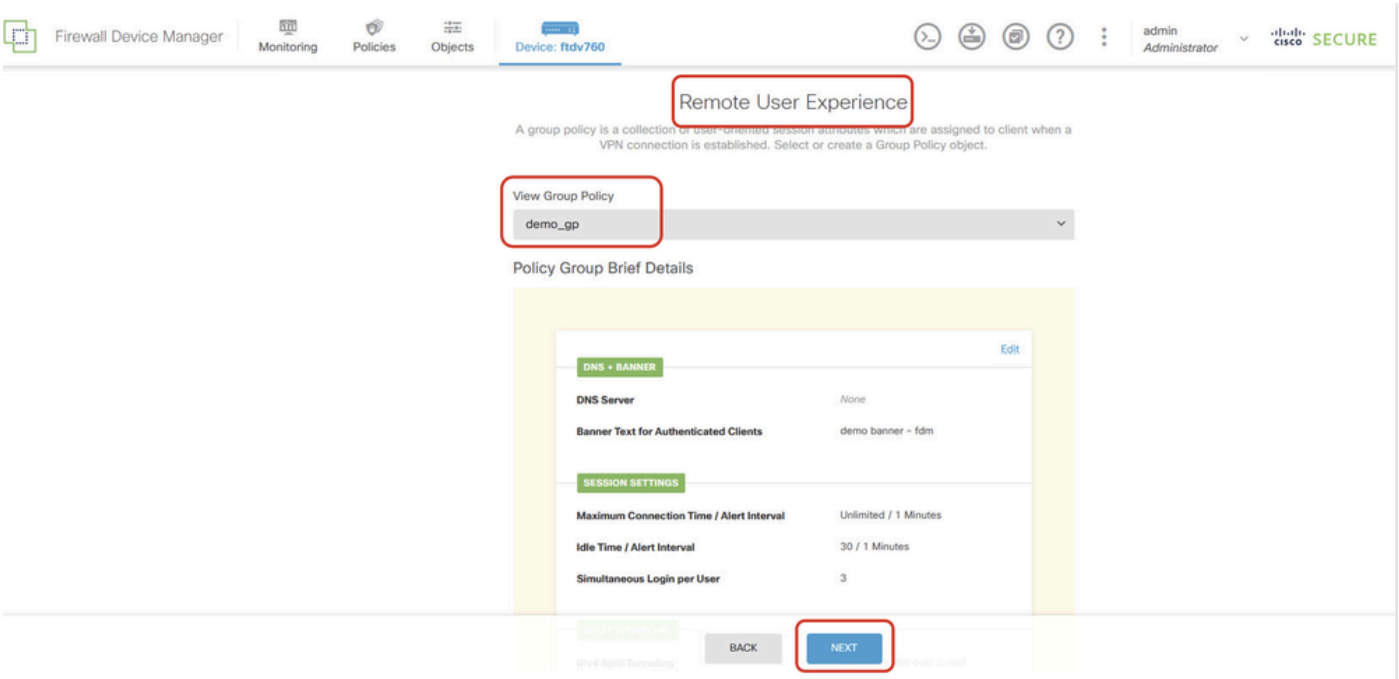
IPv4-adrespool: demo_ipv4pool (de naam geconfigureerd in stap 4.2.)

IPv6-adrespool: demo_ipv6pool (de naam die is geconfigureerd in stap 4.2.)



Create_RAVPN_Wizard_2_Address_Pool

Stap 9.3. Kies het groepsbeleid dat is geconfigureerd in stap 8.2. in het gedeelte Externe gebruikerservaring en klik op de knop VOLGENDE.

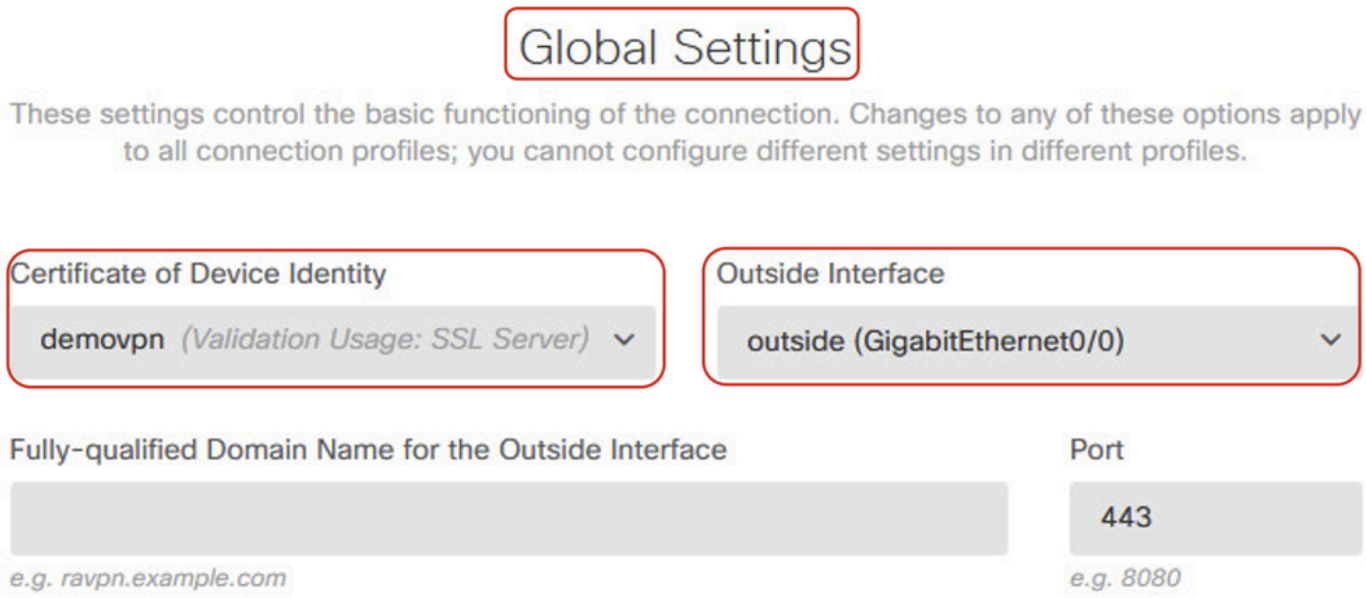


Create_RAVPN_Wizard_3

Stap 9.4. Geef de benodigde informatie op in het gedeelte Globale instellingen en klik op de knop VOLGENDE.

Certificaat van apparaatidentiteit: demovpn (de naam die is geconfigureerd in stap 6.3)

Buitenkant interface: buitenkant



Create_RAVPN_Wizard_4

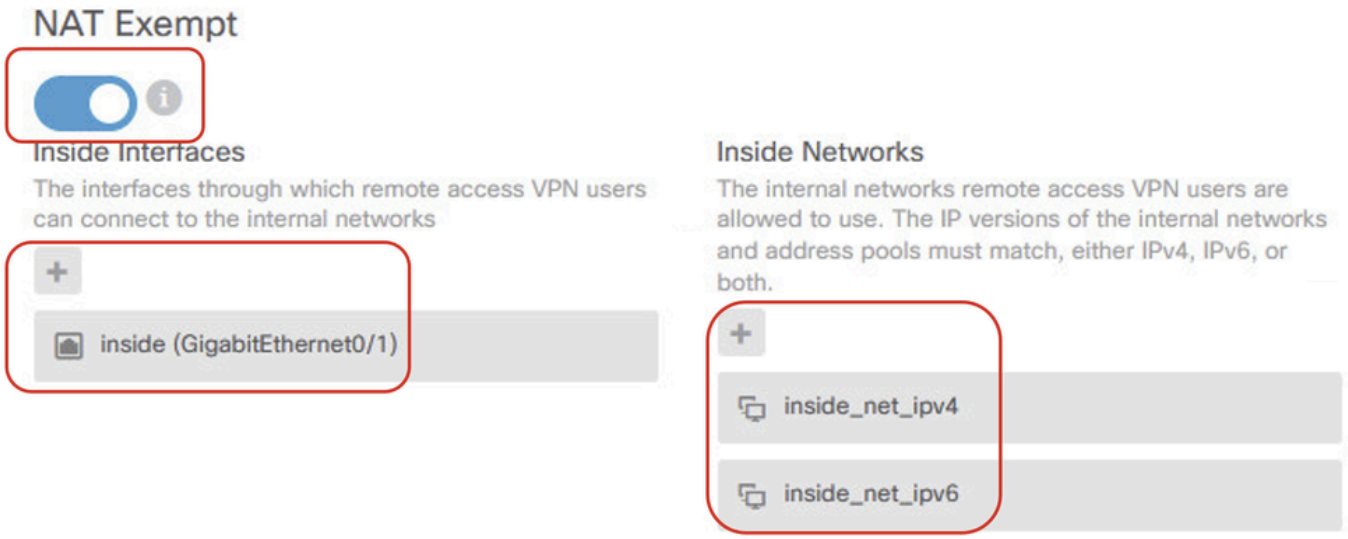
Toegangscontrole voor VPN-verkeer: Controleer het beleid voor toegangscontrole voor omzeilen voor gedecodeerd verkeer (sysopt permit-vpn).

Create_RAVPN_Wizard_4_VPN_ACP

NAT-vrijstelling: klik op de schuifregelaar naar de positie Ingeschakeld

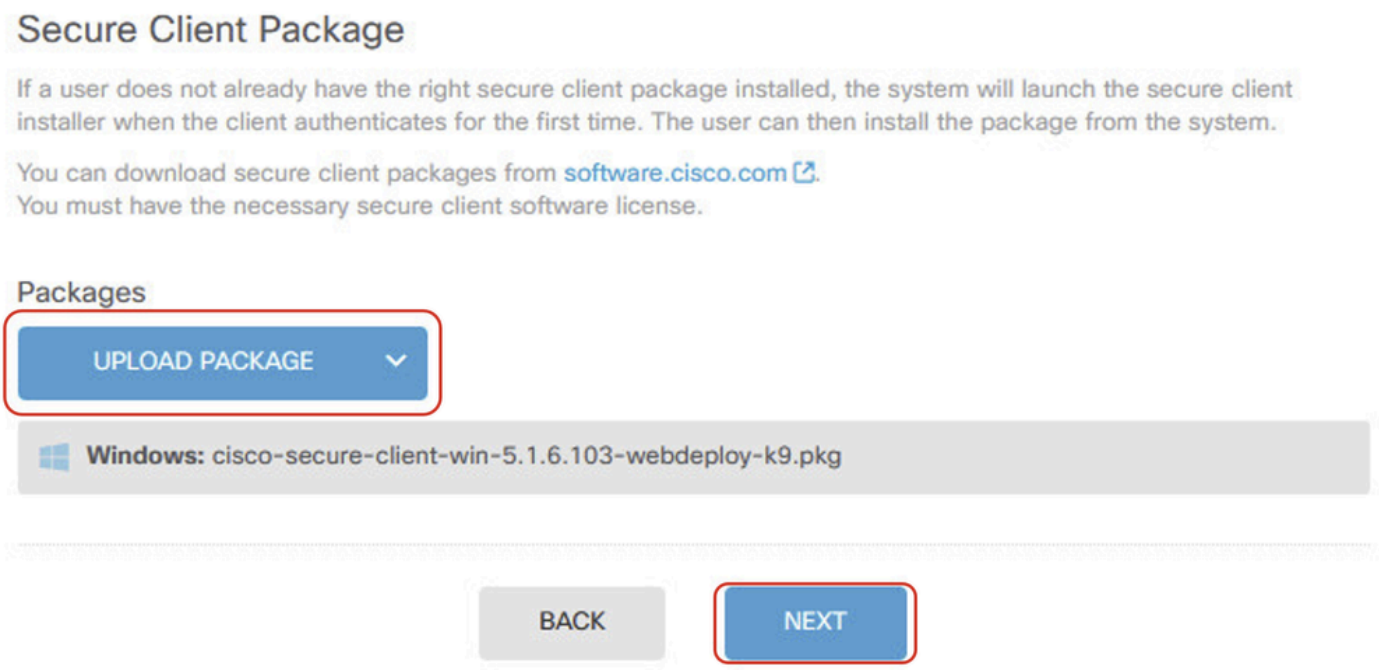
Bnneninterfaces: binnenzijde

Binnen netwerken: inside_net_ipv4, inside_net_ipv6 (de naam geconfigureerd in stap 5.2.)



Create_RAVPN_Wizard_4_VPN_NATExempt

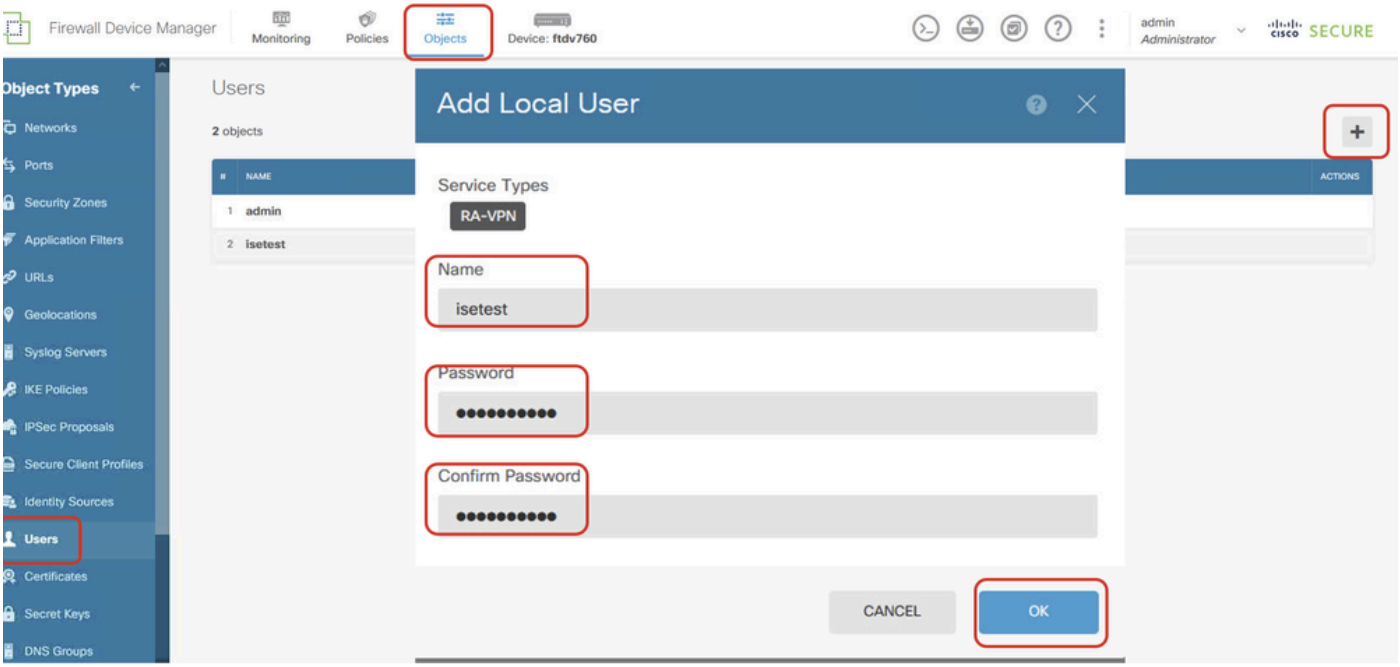
Beveiligd clientpakket: klik op PAKKET UPLOADEN en upload het pakket dienovereenkomstig. In dit voorbeeld wordt het Windows-pakket geüpload.



Create_RAVPN_Wizard_4_Image

Stap 9.5. Bekijk de samenvatting. Als er iets moet worden gewijzigd, klikt u op de knop TERUG. Als alles goed is, klikt u op de knop FINISH.

Stap 10. Maak een lokale gebruiker aan als Fallback Local Identity Source is gekozen met LocalIdentitySource in stap 9.2. Het wachtwoord van de lokale gebruiker moet hetzelfde zijn als het wachtwoord dat op ISE is geconfigureerd.



Create_Local_User

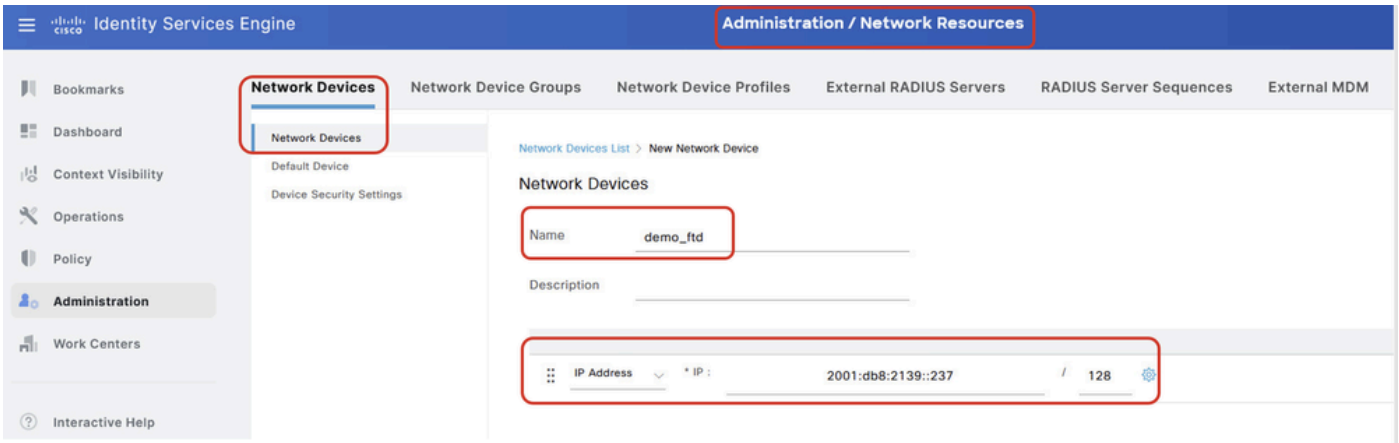
Stap 11. Implementeer de configuratiewijzigingen.

Implementeren_Wijzigingen

Configuraties op ISE

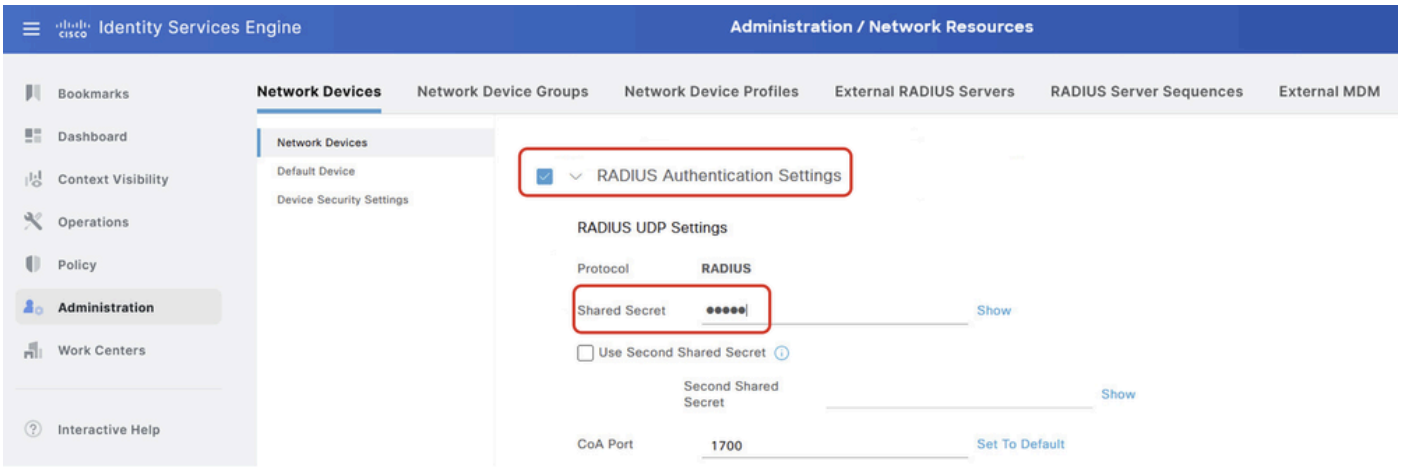
Stap 12. Netwerkapparaten maken.

Stap 12.1. Navigeer naar Beheer > Netwerkbronnen > Netwerkapparaten, klik op Toevoegen, geef de naam, het IP-adres op en blader naar beneden op de pagina.



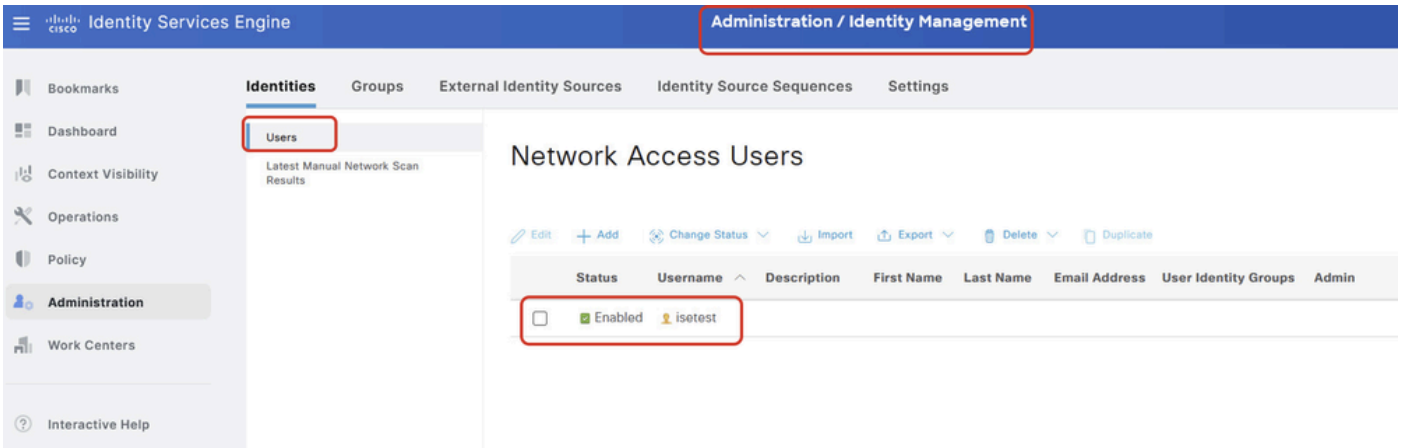
Create_Network_Devices

Stap 12.2. Schakel het selectievakje RADIUS-verificatie-instellingen in. Geef het gedeelde geheim op en klik op Indienen.



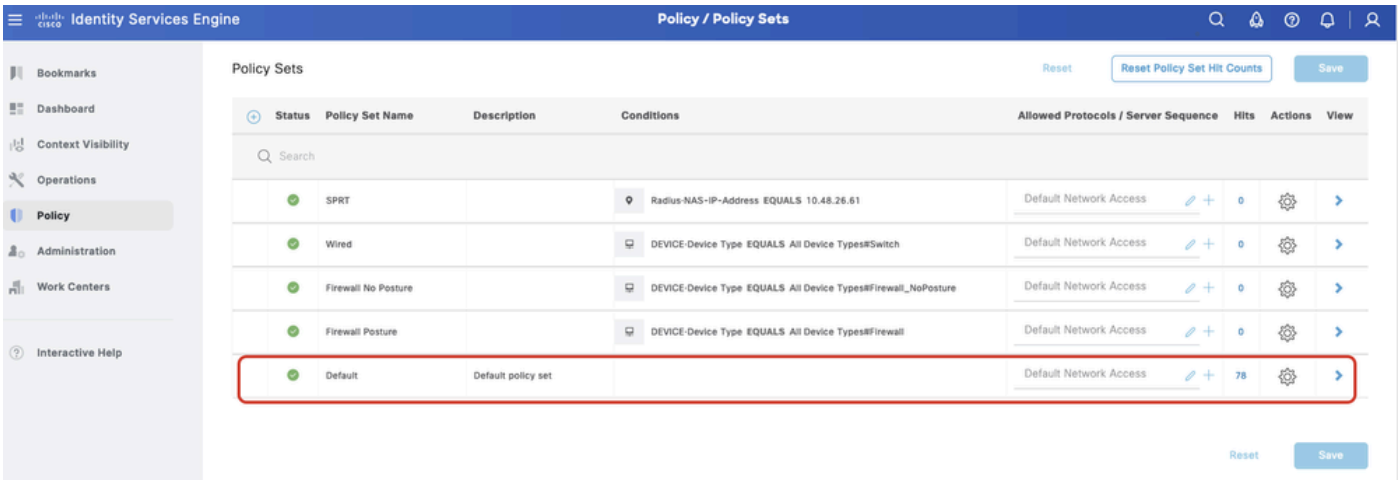
Create_Network_Devices_Cont

Stap 13. Netwerktoeganggebruikers maken. Navigeer naar Beheer > Identiteitsbeheer > Identiteiten. Klik op Toevoegen om een nieuwe gebruiker aan te maken. Het wachtwoord is hetzelfde als bij de lokale FDM-gebruiker die is gemaakt in stap 10. om ervoor te zorgen dat de terugvalfunctie werkt.



Create_ISE_User

Stap 14. (Optioneel) Maak een nieuwe beleidsset met aangepaste verificatieregel en autorisatieregel. In dit voorbeeld wordt de standaardbeleidsset gebruikt voor demodoeleinden.

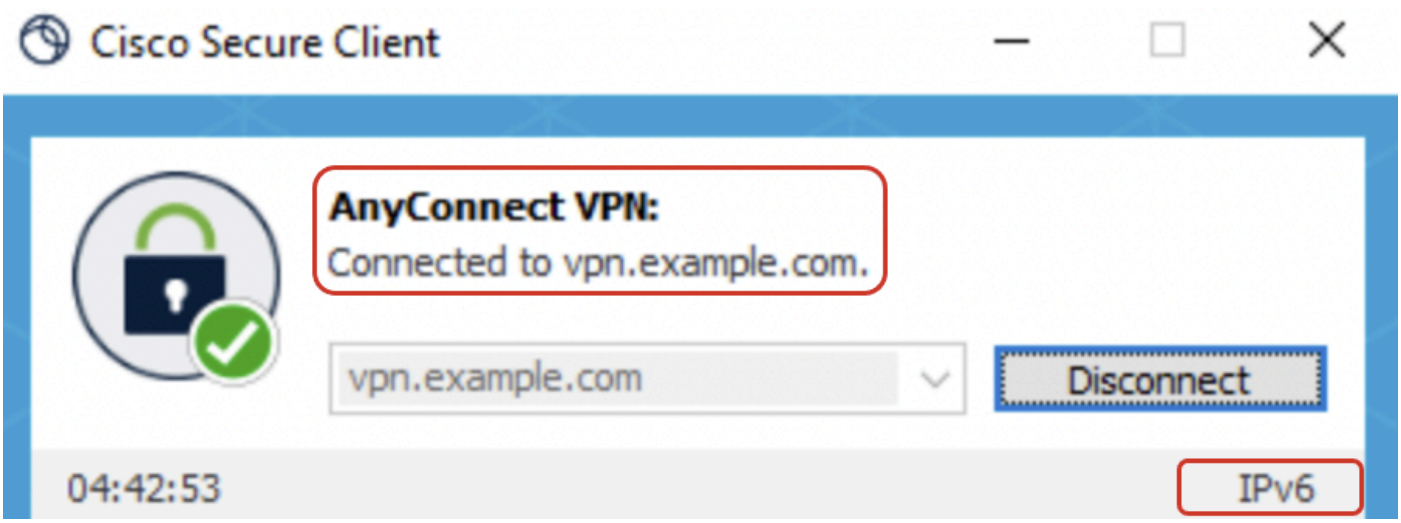


ISE_Default_Policy_Set

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Stap 15. Verbind de VPN-gateway via het IPv6-adres op de client. De VPN verbinding is succesvol.



Verify_Connection_Succesvol

Stap 16. Navigeer naar de CLI van FTD via SSH of console. Run command show vpn-sessiondb detail any connect in FTD (Lina) CLI om de VPN-sessiedetails te controleren.

<#root>

```
ftdv760# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed
```

Username : isetest

Index : 2

Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

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 : 15402 Bytes Rx : 14883
Pkts Tx : 10 Pkts Rx : 78
Pkts Tx Drop : 0 Pkts Rx Drop : 10
Group Policy : demo_gp Tunnel Group : demo_ravpn
Login Time : 05:22:30 UTC Mon Dec 23 2024
Duration : 0h:05m:05s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : c0a81e0a000020006768f396
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 2.1

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Encryption : none Hashing : none
TCP Src Port : 58339 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 24 Minutes
Client OS : win
Client OS Ver: 10.0.19042
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 7421 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 2.2

Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

```
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 58352
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 25 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 7421 Bytes Rx : 152
Pkts Tx : 1 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 2.3
```

Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

```
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 58191
UDP Dst Port : 443 Auth Mode : 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 5.1.6.103
Bytes Tx : 560 Bytes Rx : 14731
Pkts Tx : 8 Pkts Rx : 76
Pkts Tx Drop : 0 Pkts Rx Drop : 10
```

Stap 17. Pingtest bij de klant. In dit voorbeeld pingt de client zowel het IPv4- als het IPv6-adres van de server.

Command Prompt

```
C:\Users\admin>
C:\Users\admin>ping 2001:db8:50::20

Pinging 2001:db8:50::20 with 32 bytes of data:
Request timed out.
Reply from 2001:db8:50::20: time=4ms
Reply from 2001:db8:50::20: time=4ms
Reply from 2001:db8:50::20: time=3ms

Ping statistics for 2001:db8:50::20:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

Select Command Prompt

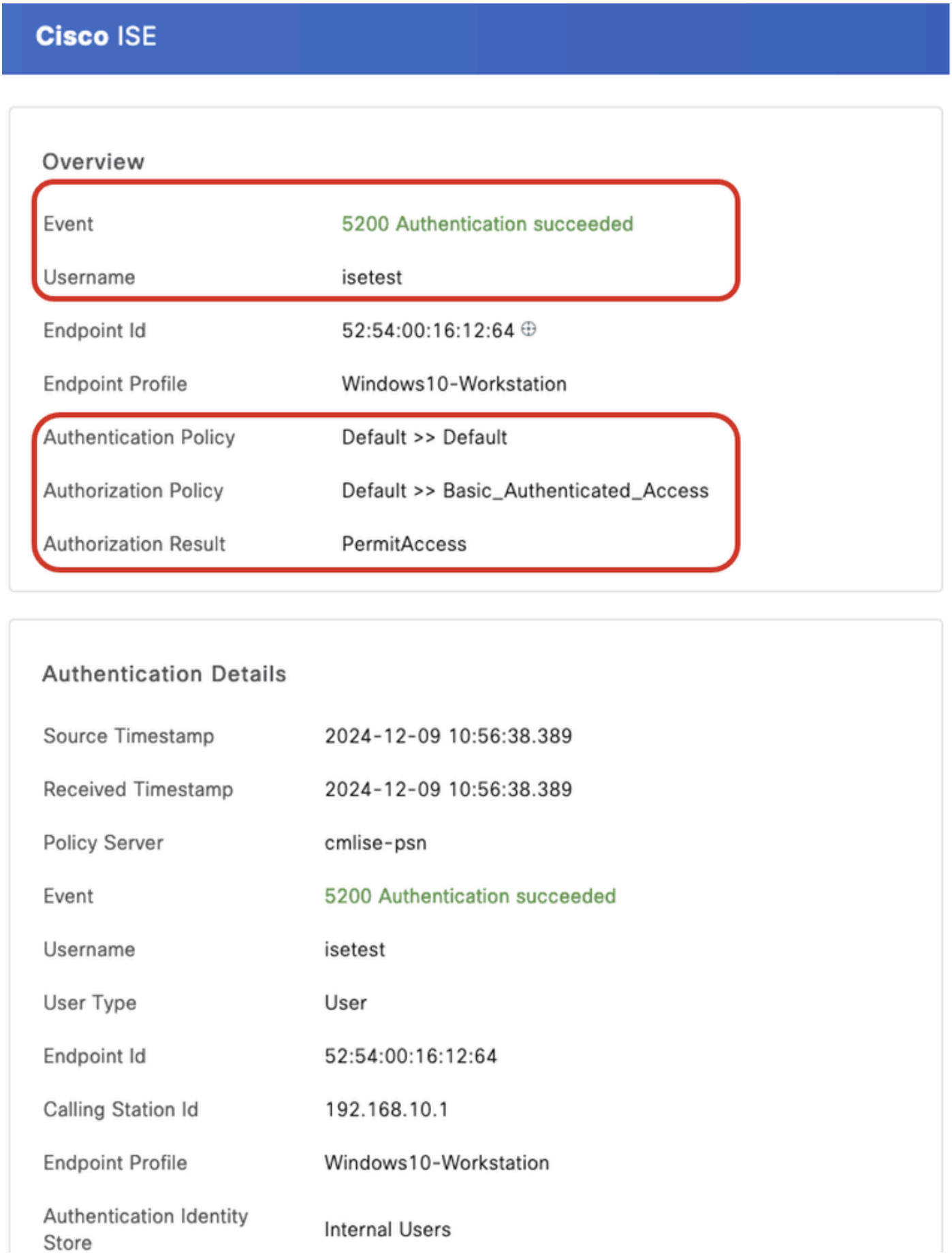
```
C:\Users\admin>
C:\Users\admin>ping 192.168.50.20

Pinging 192.168.50.20 with 32 bytes of data:
Reply from 192.168.50.20: bytes=32 time=3ms TTL=64
Reply from 192.168.50.20: bytes=32 time=3ms TTL=64
Reply from 192.168.50.20: bytes=32 time=3ms TTL=64
Reply from 192.168.50.20: bytes=32 time=4ms TTL=64

Ping statistics for 192.168.50.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

Verify_Cisco_Secure_Client_Ping

Stap 18. ISE radius live log toont succesvolle authenticatie.



ISE_Authentication_Success_Log

Stap 19. Test FTD-verificatie gaat naar LOKAAL wanneer FTD ISE niet kan bereiken.

Stap 19.1. Wanneer FTD-verificatie naar ISE gaat, voert u de opdracht show aaa-server in FTD (Lina) CLI uit om de statistieken te controleren.

In dit voorbeeld zijn er geen tellers voor LOKAAL en wordt de verificatie naar de RADIUS-server geleid.

<#root>

```
ftdv760# show aaa-server

Server Group:    LOCAL
Server Protocol: Local database
Server Address:  None
Server port:     None
Server status:   ACTIVE, Last transaction at 08:18:11 UTC Fri Dec 6 2024
Number of pending requests              0
Average round trip time                 0ms
Number of authentication requests       0
Number of authorization requests        0
Number of accounting requests           0
Number of retransmissions               0
Number of accepts                       0
Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0
Server Group:    demo_ise_group
Server Protocol: radius


Server Address:  2001:db8:2139::240


Server port:     1812(authentication), 1646(accounting)
Server status:   ACTIVE, Last transaction at 02:56:41 UTC Mon Dec 9 2024
Number of pending requests              0
Average round trip time                 100ms

Number of authentication requests       1  <== Increased


Number of authorization requests        1  <== Increased


Number of accounting requests           1  <== Increased


Number of retransmissions               0

Number of accepts                       2  <== Increased


Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0
```

Stap 19.2. Sluit de ISE-interface af om te simuleren dat FTD geen respons van ISE kan ontvangen.

<#root>

```
ftdv760# ping 2001:db8:2139::240

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:2139::240, timeout is 2 seconds:
???
Success rate is 0 percent (0/3)
```

Stap 19.3. De client start de VPN-verbinding en voert hetzelfde wachtwoord voor de gebruikersnaam in dat is gemaakt in stap 10. De VPN-verbinding is nog steeds succesvol.

Opdracht uitvoeren toont aaa-server in FTD (Lina) CLI opnieuw om de statistiek te controleren, de authenticatie, autorisatie en acceptaties tellers voor LOKAAL zijn nu verhoogd. De acceptatieteller voor de RADIUS-server is niet verhoogd.

<#root>

```
ftdv760# show aaa-server
Server Group:    LOCAL
Server Protocol: Local database
Server Address:  None
Server port:     None
Server status:   ACTIVE, Last transaction at 03:36:26 UTC Mon Dec 9 2024
Number of pending requests              0
Average round trip time                 0ms

Number of authentication requests       1  <== Increased

Number of authorization requests        1  <== Increased

Number of accounting requests           0
Number of retransmissions               0

Number of accepts                       2  <== Increased

Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0
Server Group:    demo_ise_group
Server Protocol: radius

Server Address:  2001:db8:2139::240
Server port:     1812(authentication), 1646(accounting)
Server status:   ACTIVE, Last transaction at 03:36:41 UTC Mon Dec 9 2024
Number of pending requests              0
Average round trip time                 100ms
```

```
Number of authentication requests       2
Number of authorization requests        1
Number of accounting requests           6
Number of retransmissions               0

Number of accepts                       2  <== Not increased


Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      6
Number of unrecognized responses        0
```

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

U kunt deze opdrachten uitvoeren op FTD Lina om problemen met de VPN-sectie op te lossen.

debug webvpn 255
debug webvpn anyconnect 255

U kunt een DART-bestand van de client verzamelen voor VPN-probleemoplossing om te bepalen of het probleem zich voordoet met de beveiligde client. Raadpleeg voor meer informatie het relevante CCO-document Collect DART Bundle for Secure Client.

U kunt deze opdrachten uitvoeren op FTD Lina om problemen op te lossen in het gedeelte Radius.

```
ftdv760# debug radius ?

all      All debug options
decode   Decode debug option
dynamic-authorization CoA listener debug option
session  Session debug option
user     User debug option
<cr>
```

```
ftdv760# debug aaa ?

accounting
authentication
authorization
common
```

```
condition
internal
shim
url-redirect
<cr>
```

U kunt deze bekijken om het verkeersgerelateerde probleem op te lossen nadat de VPN-verbinding succesvol is verlopen.

1. Leg verkeer vast op FTD Lina om te zien of Lina het verkeer laat vallen, verwijzend naar dit CCO-document; Gebruik Firepower Threat Defense Captures en Packet Tracer - Cisco.
2. Controleer het toegangscontrolebeleid om ervoor te zorgen dat het gerelateerde VPN-verkeer mag worden doorgegeven als het beleid voor toegangscontrole voor gedecodeerd verkeer is uitgeschakeld.
3. De NAT-vrijstelling herzien om ervoor te zorgen dat VPN-verkeer wordt uitgesloten van NAT.

Gerelateerde informatie

- FDM Configuratiegids van RAVPN - Cisco
- Verzamel DART-bundel voor beveiligde client - Cisco
- Firepower Threat Defense Captures en Packet Tracer gebruiken - Cisco
- Problemen oplossen met Cisco Secure Client - Cisco
- Cisco Technical Support en downloads

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.