

# Configureer de routegebaseerde site-to-site VPN-tunnel op FTD die door FMC wordt beheerd

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Beperkingen en beperkingen](#)

[Configuratiestappen op FMC](#)

[Verifiëren](#)

[Van FMC GUI](#)

[Van FTD CLI](#)

## Inleiding

Dit document beschrijft hoe u een routegebaseerde site-to-site VPN-tunnel kunt configureren op basis van een Firepower Threat Defence (FTD) die wordt beheerd door een Firepower Management Center (FMC).

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basis begrip van hoe een VPN-tunnel werkt.
- Begrijp hoe je door het VCC moet navigeren.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Cisco Firepower Management Center (FMC) versie 6.7.0
- Cisco Firepower Threat Defence (FTD) versie 6.7.0

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

Op route gebaseerde VPN maakt het mogelijk om interessant verkeer te versleutelen of te verzenden via een VPN-tunnel en verkeer te routeren in plaats van beleid/toeganglijst zoals in op beleid gebaseerde of op Crypto-kaart gebaseerde VPN. Het coderingsdomein is ingesteld om verkeer dat de IPsec-tunnel binnenkomt, toe te staan. IPsec Local en Remote Traffic Selectors zijn ingesteld op 0.0.0.0/0.0.0.0. Dit betekent dat elk verkeer dat in de IPsec-tunnel wordt gerouteerd, wordt versleuteld ongeacht het bron-/doelsubstelsysteem.

## Beperkingen en beperkingen

Dit zijn bekende beperkingen en beperkingen voor routegebaseerde tunnels op FTD:

- Ondersteunt alleen IPsec. GRE wordt niet ondersteund.
- Geen ondersteuning voor Dynamic VTI.
- Ondersteunt alleen IPv4 interfaces, evenals IPv4, beschermde netwerken of VPN-payload (geen ondersteuning voor IPv6).
- Statische routing en alleen BGP Dynamic Routing Protocol worden ondersteund voor VTI-interfaces die verkeer voor VPN classificeren (geen ondersteuning voor andere protocollen zoals OSPF, RIP, enzovoort).
- Slechts 100 VTIs worden ondersteund per interface.
- VTI wordt niet ondersteund op een FTD-cluster.
- VTI wordt niet ondersteund in dit beleid:

·QoS

NAT

·Platforminstellingen

Deze algoritmen worden niet langer ondersteund door FMC/FTD versie 6.7.0 voor nieuwe VPN-tunnels (FMC ondersteunt alle verwijderde algoritmen voor het beheer van FTD < 6.7):

- 3DES, DES en NULL-encryptie worden niet ondersteund in IKE-beleid.
- DH-groepen 1, 2 en 24 worden niet ondersteund in IKE-beleid en IPsec-voorstel.
- MD5-integriteit wordt niet ondersteund in IKE-beleid.
- PRF MD5 wordt niet ondersteund in IKE-beleid.
- DES, 3DES, AES-GMAC, AES-GMAC-192 en AES-GMAC-256 versleutelingsalgoritmen worden niet ondersteund in IPsec-voorstel.

**Opmerking:** dit geldt voor zowel de site-to-site route als voor op beleid gebaseerde VPN-tunnels. Om een oudere FTD van het FMC te upgraden naar 6.7, wordt een pre-

validatiecontrole gestart waarin de gebruiker wordt gewaarschuwd voor veranderingen die betrekking hebben op de verwijderde algoritmen die de upgrade blokkeren.

### FTD 6.7 beheerd via FMC 6.7

Fresh Install

Upgraden: FTD alleen geconfigureerd met zwakke algoritmen

Upgraden: FTD alleen geconfigureerd met enkele zwakke algoritmen en enkele sterke algoritmen

Upgraden: Klasse C-land (geen sterke cryptolicensie)

### Beschikbare configuratie

Er zijn zwakke algoritmen beschikbaar, maar deze kunnen niet worden gebruikt om het FTD 6.7-apparaat te configureren.

Upgrade van FMC 6.7 UI, een pre-validatiecontrole toont een fout. De upgrade wordt geblokkeerd tot de aanpassing.

Upgrade van FMC 6.7 UI, een pre-validatiecontrole toont een fout. De upgrade wordt geblokkeerd tot de aanpassing.

Toestaan dat DES wordt toegestaan

### Site-to-site VPN-tunnel

Er zijn zwakke algoritmen beschikbaar, maar deze kunnen niet worden gebruikt om het FTD 6.7-apparaat te configureren.

Na FTD upgrade, en verondersteld dat de peer zijn instellingen niet heeft gewijzigd, dan wordt de tunnel beëindigd.

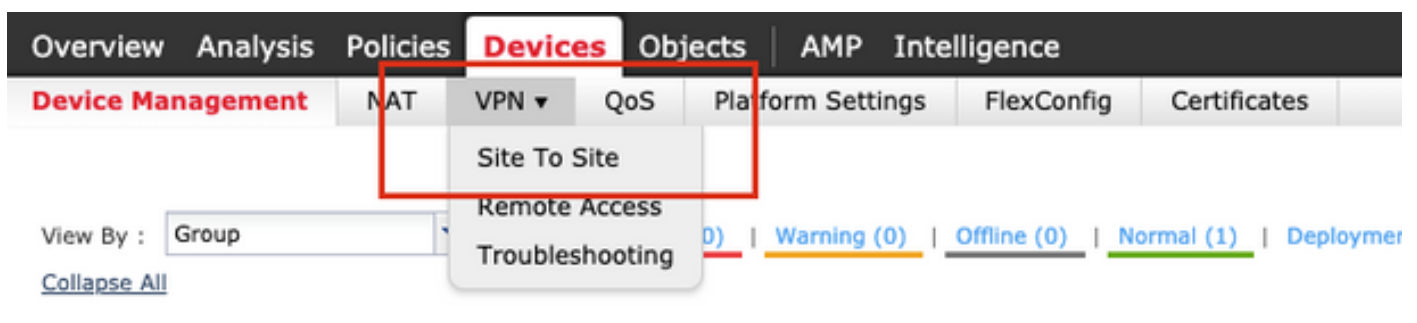
Na FTD-upgrade, en verondersteld dat de peer sterke algoritmen heeft ingesteld, dan wordt de tunnel opnieuw ingesteld.

Toestaan dat DES wordt toegestaan

**Opmerking:** er is geen extra licentie nodig, routegebaseerde VPN kan worden geconfigureerd in zowel gelicentieerde als evaluatiemodes. Zonder crypto-compatibiliteit (Export Controlled Properties Enabled) kan alleen DES worden gebruikt als een encryptie-algoritme.

## Configuratiestappen op FMC

Stap 1. Ga naar **Apparaten >VPN >Site to Site**.



Stap 2. Klik op **Add VPN** en kies **Firepower Threat Defence Device**, zoals in de afbeelding.

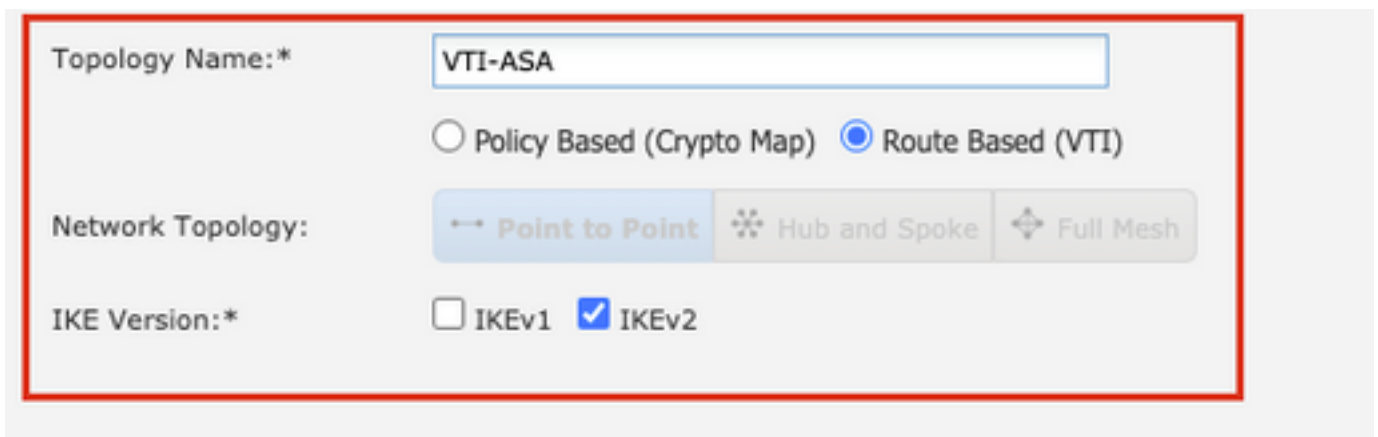


Stap 3. Geef een **topologienaam** op en selecteer het type VPN als **routegebaseerd (VTI)**. Kies de **IKE-versie**.

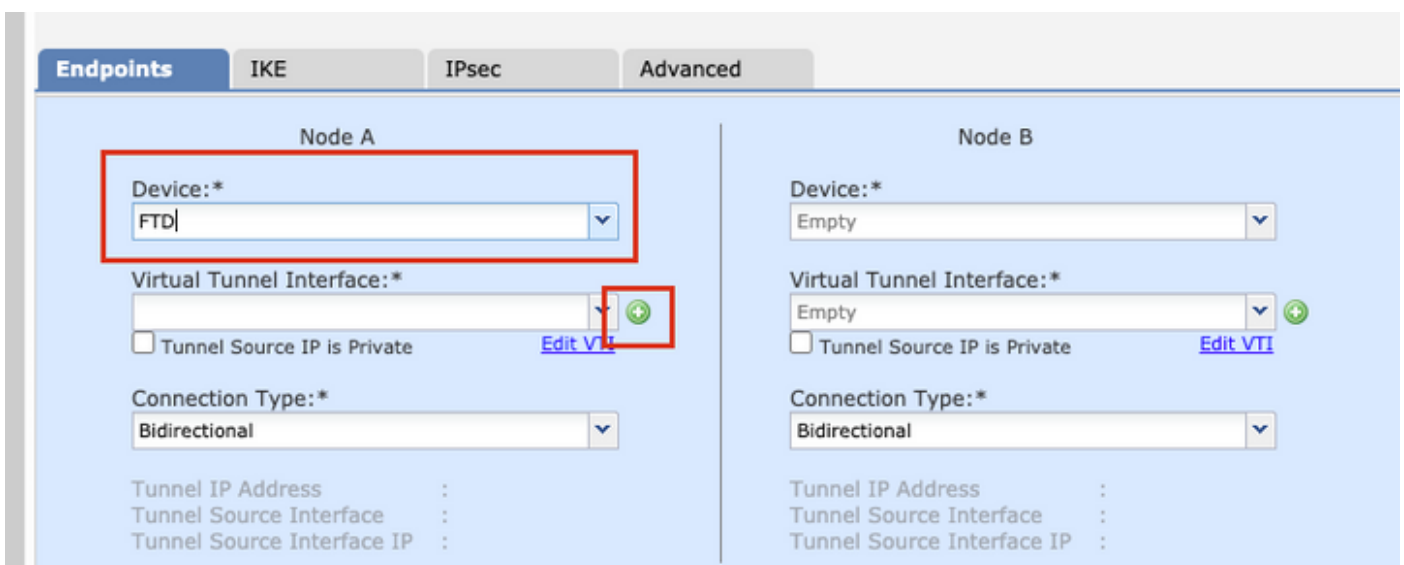
Ten behoeve van deze demonstratie:

**Naam topologie:** VTI-ASA

**IKE versie:** IKEv2



Stap 4. Kies het **apparaat** waarop de tunnel moet worden geconfigureerd, U kunt kiezen om een nieuwe **virtuele sjabloon interface** toe te voegen (klik op het + pictogram) of selecteer een van de lijst die bestaat.



Stap 5. Definieer de parameters van de **Nieuwe virtuele tunnelinterface**. Klik op OK.

Ten behoeve van deze demonstratie:

**Name:** VTI-ASA

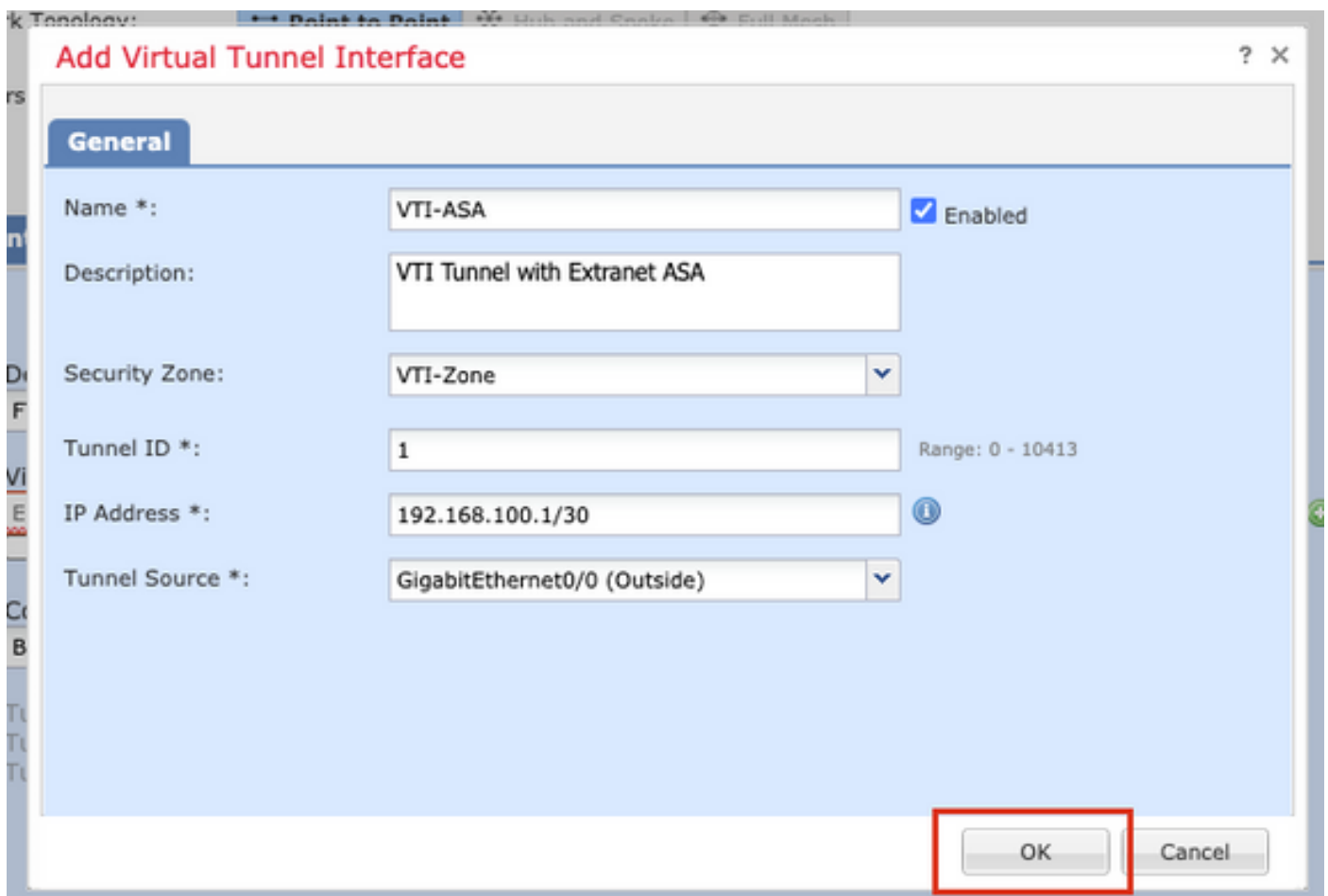
**Beschrijving (optioneel):** VTI-tunnel met extranet ASA

**Security zone:** VTI-zone

**Tunnel-ID:** 1

**IP-adres:** 192.168.100.1/30

**Tunnelbron:** Gigabit Ethernet0/0 (buiten)

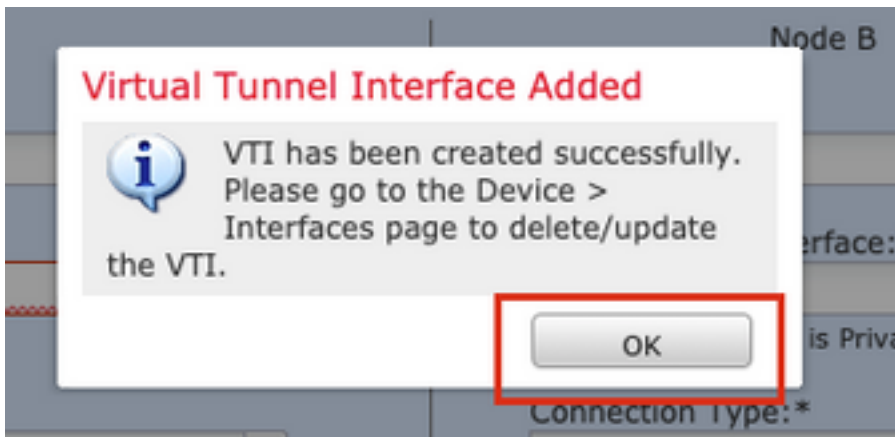


The screenshot shows a dialog box titled "Add Virtual Tunnel Interface" with a "General" tab. The fields are as follows:

- Name \*: VTI-ASA
- Description: VTI Tunnel with Extranet ASA
- Security Zone: VTI-Zone
- Tunnel ID \*: 1 (Range: 0 - 10413)
- IP Address \*: 192.168.100.1/30
- Tunnel Source \*: GigabitEthernet0/0 (Outside)

The "Enabled" checkbox is checked. The "OK" button is highlighted with a red rectangle.

Stap 6. Klik op **OK** in de pop-up waarin wordt aangegeven dat het nieuwe VTI is gemaakt.



Stap 7. Kies het nieuwe VTI of een VTI die onder **Virtual Tunnel Interface** bestaat. Verstrek de informatie voor **Knooppunt B** (dat het peer apparaat is).

Ten behoeve van deze demonstratie:

**Apparaat:** Extranet

**Apparaatnaam:** ASA-peer

**IP-adres eindpunt:** 10.106.67.252

**Create New VPN Topology**

Topology Name: \*

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:

IKE Version: \*  IKEv1  IKEv2

**Endpoints** | IKE | IPsec | Advanced

**Node A**

Device: \*

Virtual Tunnel Interface: \*   Tunnel Source IP is Private [Edit VTI](#)

Connection Type: \*

Tunnel IP Address : 192.168.100.1  
 Tunnel Source Interface : Outside  
 Tunnel Source Interface IP : 10.197.224.90

Additional Configuration ⓘ  
 Route traffic to the VTI : [Routing Policy](#)  
 Permit VPN traffic : [AC Policy](#)

**Node B**

Device: \*

Device Name: \*

Endpoint IP Address: \*

Stap 8. Navigeer naar het tabblad **IKE**. U kunt ervoor kiezen een vooraf gedefinieerd **beleid** te gebruiken of op de **+**-knop naast het **tabblad Beleid** te klikken en een nieuw tabblad te maken.

**IKEv2 Settings**

Policy: \*

Authentication Type:

Pre-shared Key Length: \*  Characters (Range 1-127)

Stap 9. (Optioneel Als u een nieuw IKEv2-beleid maakt) Geef een **naam** voor het beleid en selecteer de **algoritmen** die in het beleid moeten worden gebruikt. Klik op Save (Opslaan).

Ten behoeve van deze demonstratie:

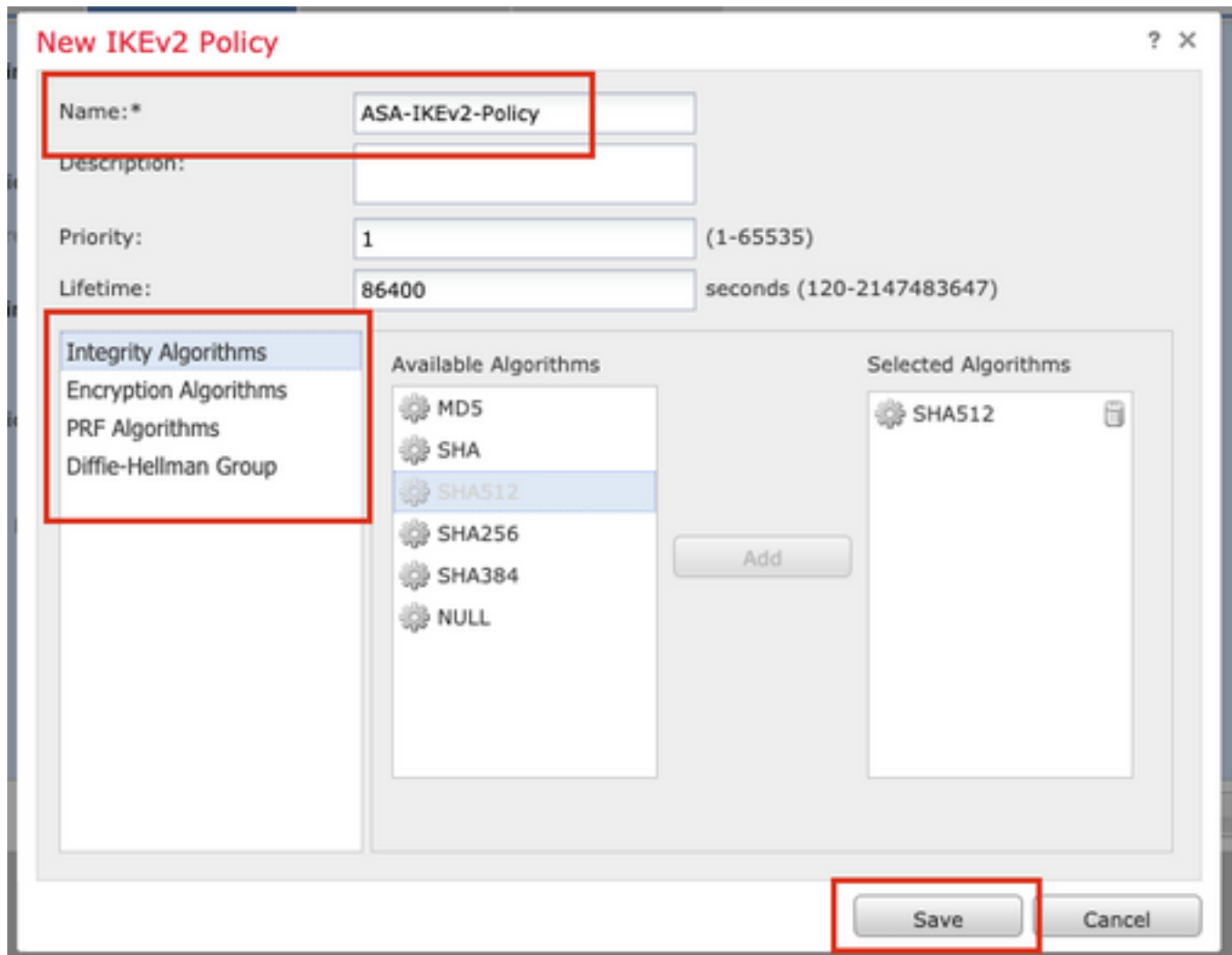
**Name:** ASA 5500-IKEv2-beleid

Integriteitsalgoritmen: SHA-512-software

Encryptiealgoritmen: AES-256 router

PRF-algoritmen: SHA-512-software

Diffie-Hellman groep: 21



Stap 10. Kies het nieuwe ontwerp of het **beleid** dat bestaat. Selecteer het **verificatietype**. Als een **Vooraf gedeelde handmatige sleutel** wordt gebruikt, geef dan de sleutel op in de **sleutelvakjes** en **bevestig de sleutelvakjes**.

Ten behoeve van deze demonstratie:

**Beleid:** ASA-IKEv2-Policy

**Verificatietype:** Vooraf gedeelde handmatige sleutel

**Sleutel:** Cisco IP123

**Bevestig sleutel:** Cisco IP123



Endpoints   **IKE**   IPsec   Advanced

**IKEv1 Settings**

Policy:\*   preshared\_sha\_aes256\_dh14\_3   +

Authentication Type:   Pre-shared Automatic Key

Pre-shared Key Length:\*   24   Characters   (Range 1-127)

**IKEv2 Settings**

Policy:\*   ASA-IKEv2-Policy   +

Authentication Type:   Pre-shared Manual Key

Key:\*   .....

Confirm Key:\*   .....

Enforce hex-based pre-shared key only

**Opmerking:** als beide eindpunten op hetzelfde VCC zijn geregistreerd, kan ook de optie **Pre-Shared Automatic Key (Vooraf gedeelde automatische sleutel)** worden gebruikt.

Stap 1. Navigeer naar het tabblad **IPsec**. U kunt een vooraf gedefinieerd **IKEv2 IPsec-voorstel** gebruiken of een nieuw voorstel maken. Klik op de knop **Bewerken** naast het tabblad **Voorstel voor IKEv2 IPsec**.

Crypto Map Type:    Static    Dynamic

IKEv2 Mode:   Tunnel

Transform Sets:

**IKEv1 IPsec Proposals**

tunnel\_aes256\_sha

**IKEv2 IPsec Proposals\***

AES-GCM

Enable Security Association (SA) Strength Enforcement

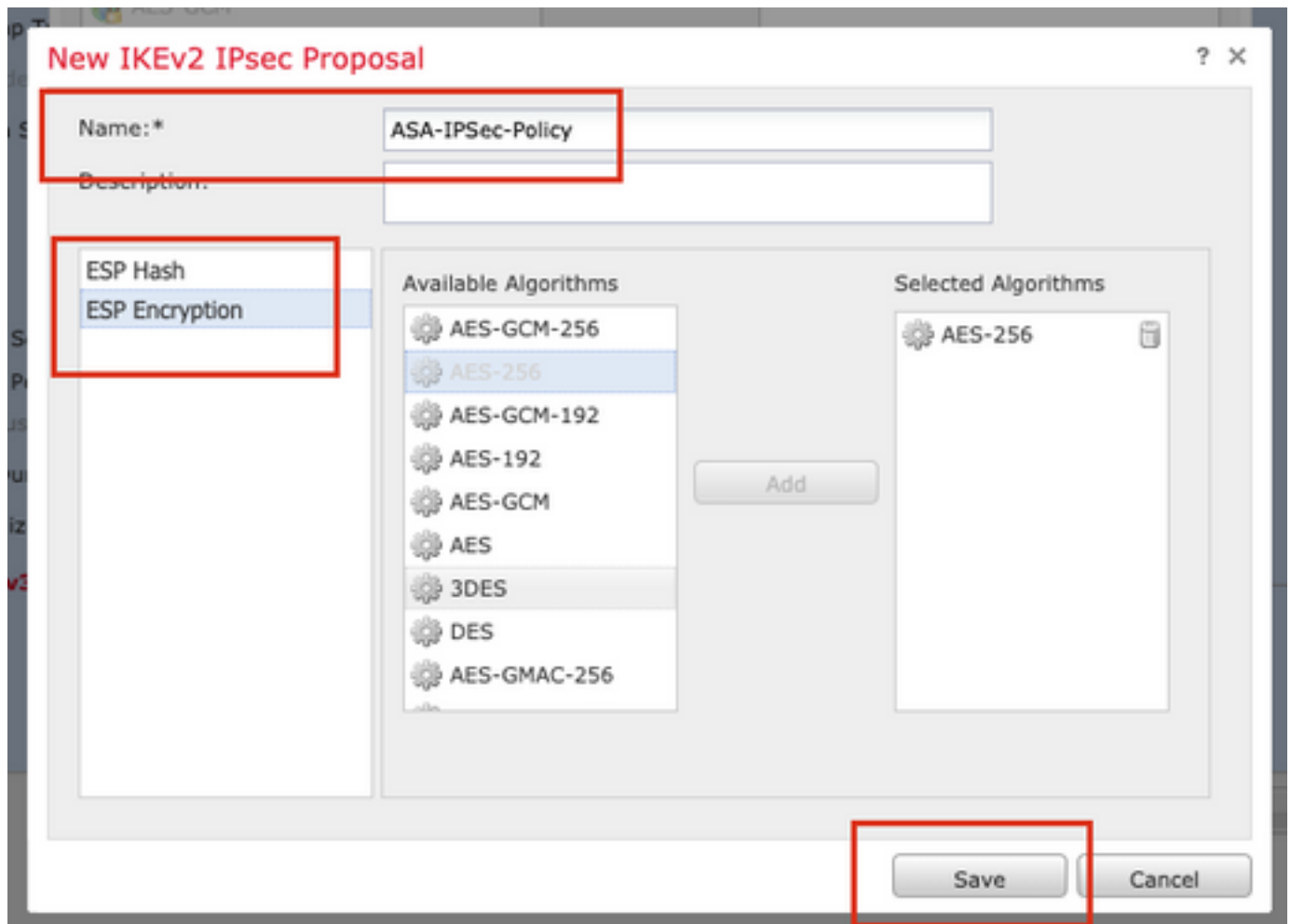
Stap 12. (optioneel Als u een nieuw IKEv2 IPsec-voorstel maakt) Geef een **naam** voor het voorstel en selecteer de **algoritmen** die in het voorstel moeten worden gebruikt. Klik op **Save (Opslaan)**.

Ten behoeve van deze demonstratie:

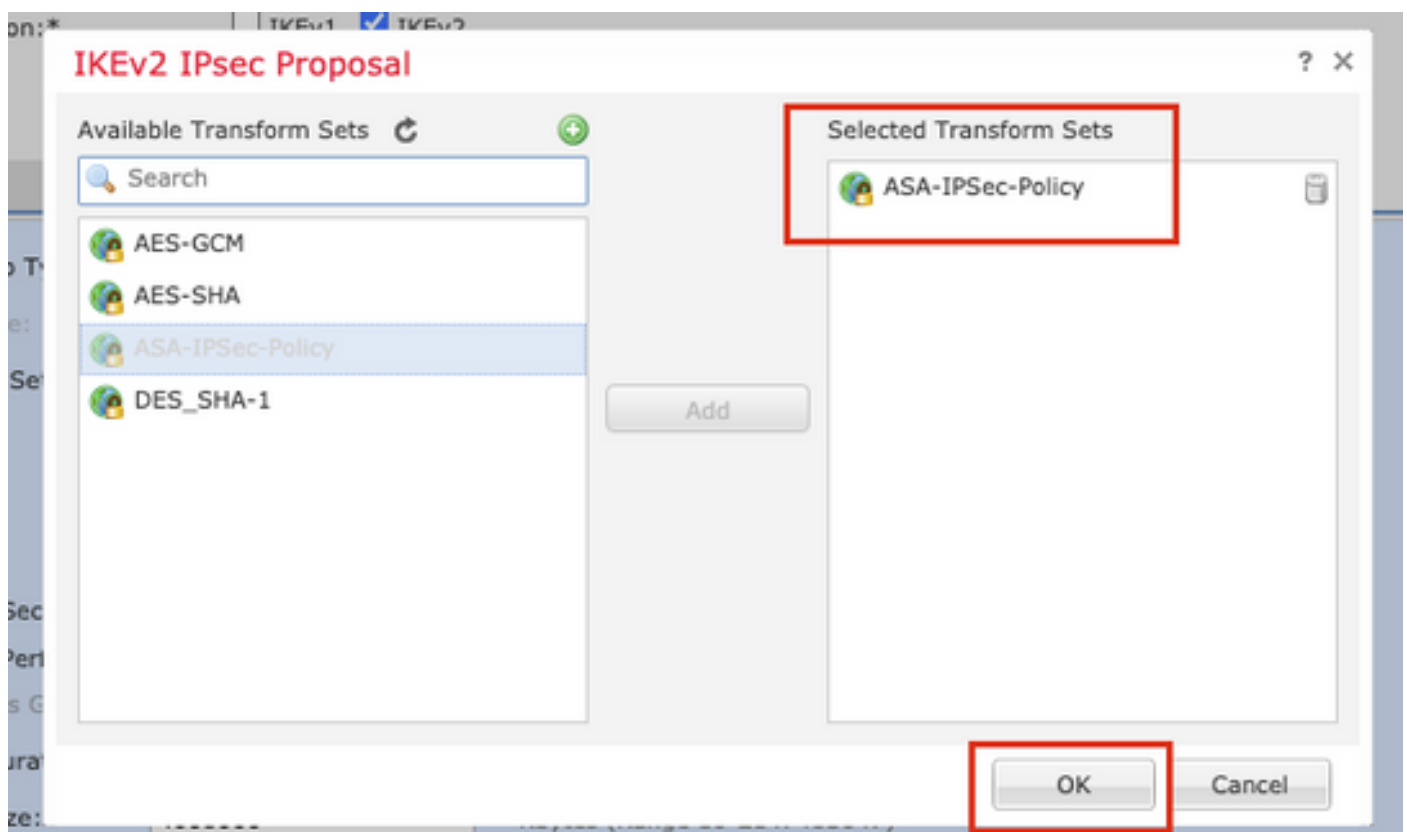
**Name:** ASA 5500-IPS beleid

**ESP-hash:** SHA-512-software

## ESP-encryptie: AES-256 router



Stap 13. Kies het nieuwe voorstel of voorstel uit de lijst met voorstellen die beschikbaar zijn. Klik op OK.



Stap 14. (Optioneel) Kies de **perfecte voorwaartse** instellingen voor **geheimhouding**. Configureer de **duur** en de **grootte van de levensduur van IPsec**.

Ten behoeve van deze demonstratie:

**Perfect voorwaartse geheimhouding:** Modulus-groep 21

**Levensduur:** 28800 (standaard)

**Levensduur:** 4608000 (standaard)

Enable Security Association (SA) Strength Enforcement

Enable Perfect Forward Secrecy

Modulus Group: 21

Lifetime Duration\*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

ESPv3 Settings

Stap 15. Controleer de ingestelde instellingen. Klik op **Opslaan**, zoals in deze afbeelding.

Topology Name:\*

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:

IKE Version:\*  IKEv1  IKEv2

---

Endpoints    IKE    **IPsec**    Advanced

Crypto Map Type:  Static  Dynamic

IKEv2 Mode:

Transform Sets: **IKEv1 IPsec Proposals**     **IKEv2 IPsec Proposals\***

Enable Security Association (SA) Strength Enforcement

Enable Perfect Forward Secrecy

Modulus Group:

Lifetime Duration\*:  Seconds (Range 120-2147483647)

Lifetime Size:  Kbytes (Range 10-2147483647)

—  —

Stap 16. (Optioneel) Configureer het **NAT**-beleid. Ga naar **Apparaten > NAT**. Kies het NAT-beleid dat aan dit FTD is toegewezen.

Geef de **broninterfaceobjecten** en de **doelinterfaceobjecten** op het tabblad **Interfaceobjecten** op.

Vermeld de oorspronkelijke bron, de **oorspronkelijke bestemming**, de **vertaalde bron**, de **vertaalde bestemming** in het **tabblad Vertaling**. Klik op OK.

Ten behoeve van deze demonstratie:

**Broninterfaceobjecten:** In zone

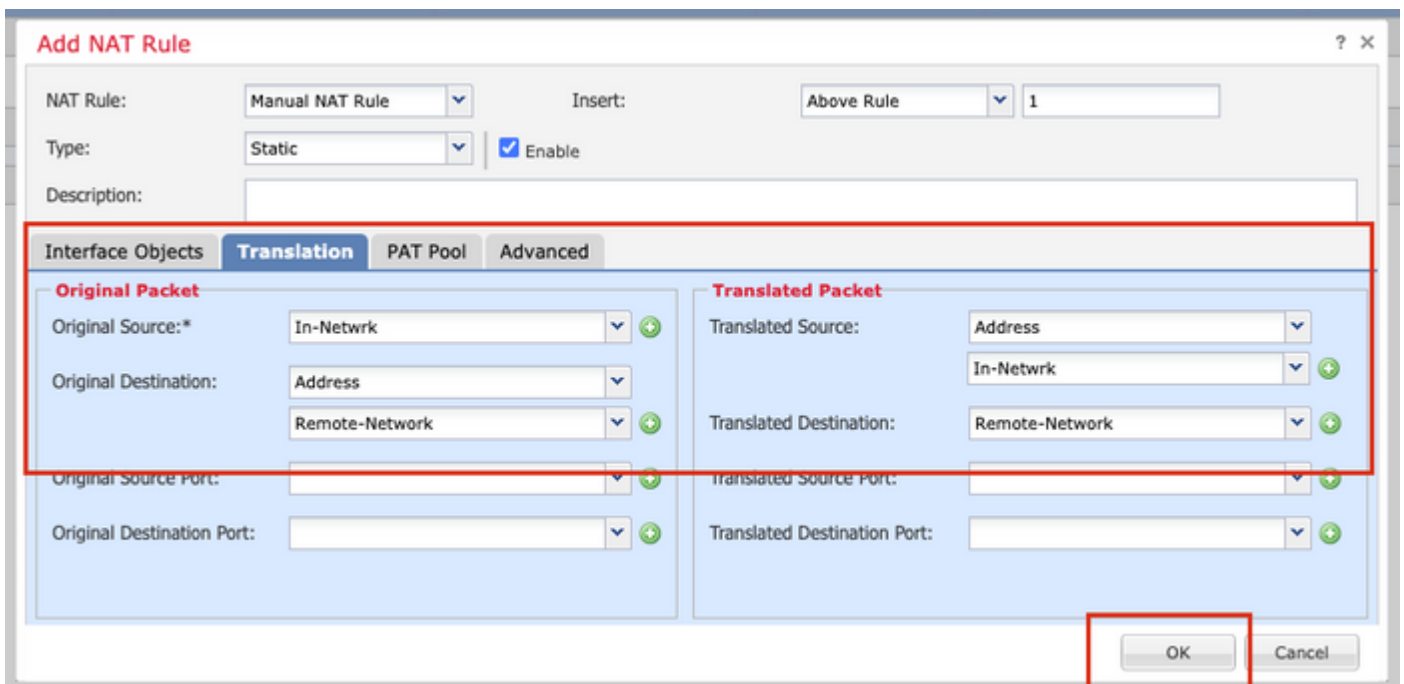
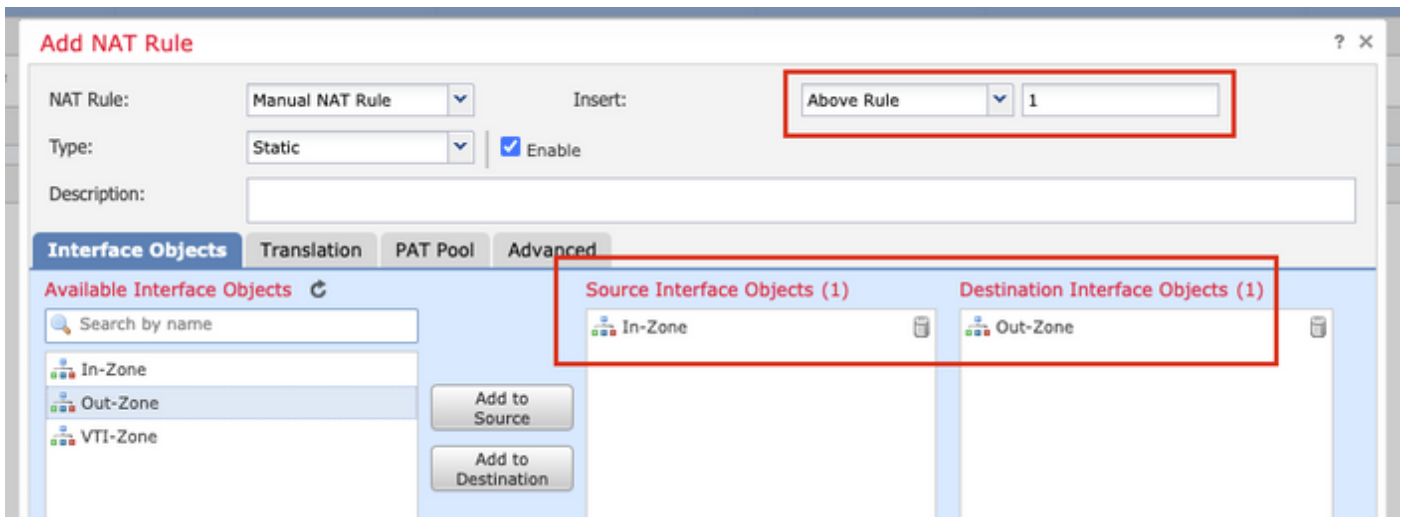
**Doelinterfaceobjecten:** out-zone

**Oorspronkelijke bron:** In het netwerk

**Oorspronkelijke bestemming:** Remote-Network

**Vertaalde bron:** In het netwerk

**Vertaalde bestemming:** Remote-Network



**Opmerking:** Zorg ervoor dat de statische NAT-vrijstelling voor de site-to-site tunnel wordt toegevoegd bovenop de dynamische NAT/PAT-regels.

Stap 17. Configureer het **toegangscontrolebeleid**. Ga naar **Beleid > Toegangsbeheer > Toegangsbeheer**. **Bewerk** het op het FTD toegepaste beleid.

**Opmerking:** **sysopt connection license-vpn** werkt niet met routegebaseerde VPN-tunnels. De toegangscontrole-regels moeten worden geconfigureerd voor zowel IN-> OUT-zones als OUT-> IN-zones.

Geef de **bronzones** en de **doelzones** op in het tabblad **Zones**.

Verstrek de **Bronnetwerken**, **Bestemmingsnetwerken** in het tabblad **Netwerken**. Klik op Add (Toevoegen).

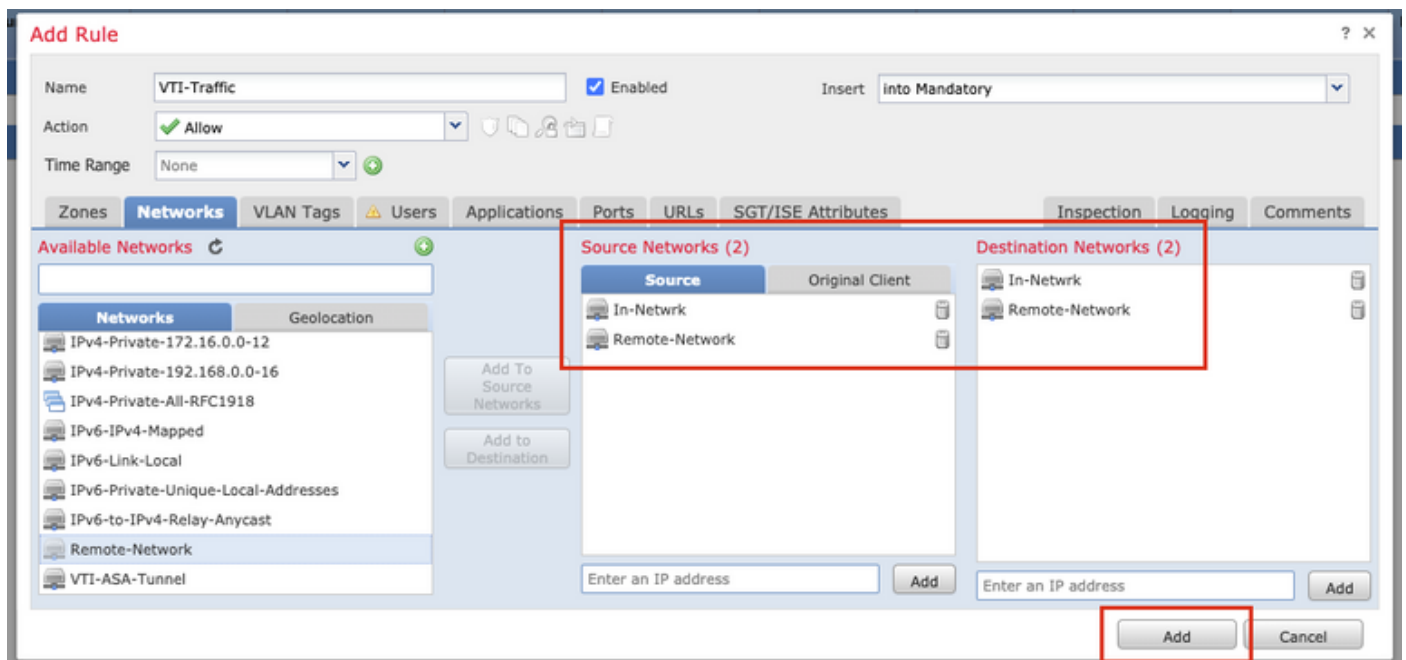
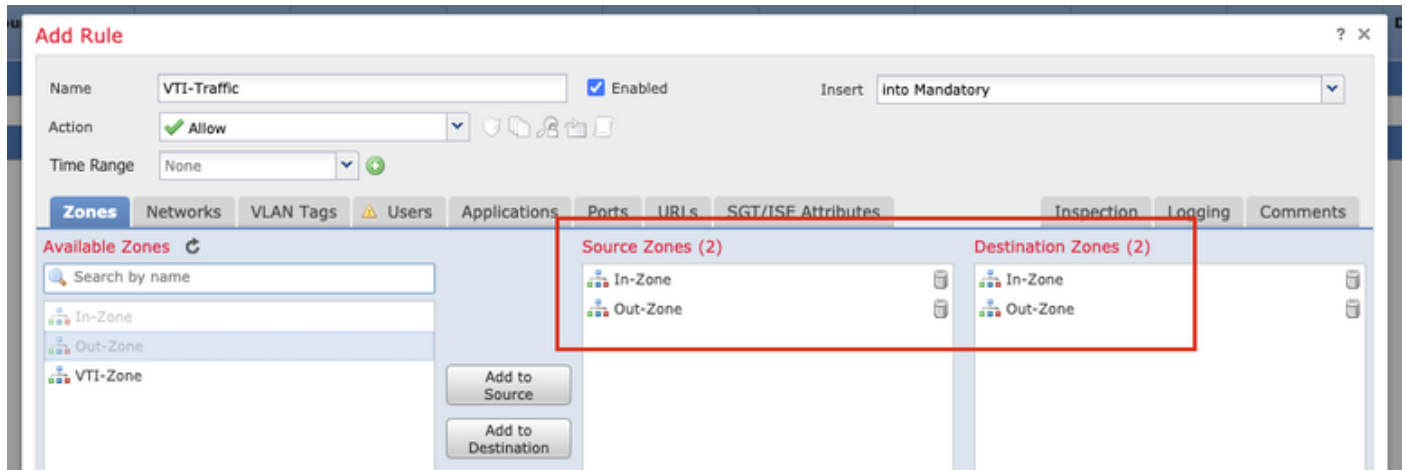
Ten behoeve van deze demonstratie:

Source Zones: In-Zone en Out-Zone

Bestemmingszones: out-zone en in-zone

Bronnetwerken: In-Network en Remote-Network

Bestemmingsnetwerken: Remote-Network en In-Network



Stap 18. Voeg de routing toe via de VTI-tunnel. Ga naar **Apparaten > Apparaatbeheer**. **Bewerk** het apparaat waarop de VTI-tunnel is ingesteld.

Navigeer naar **statische route** onder het tabblad **Routing**. Klik op **Route toevoegen**.

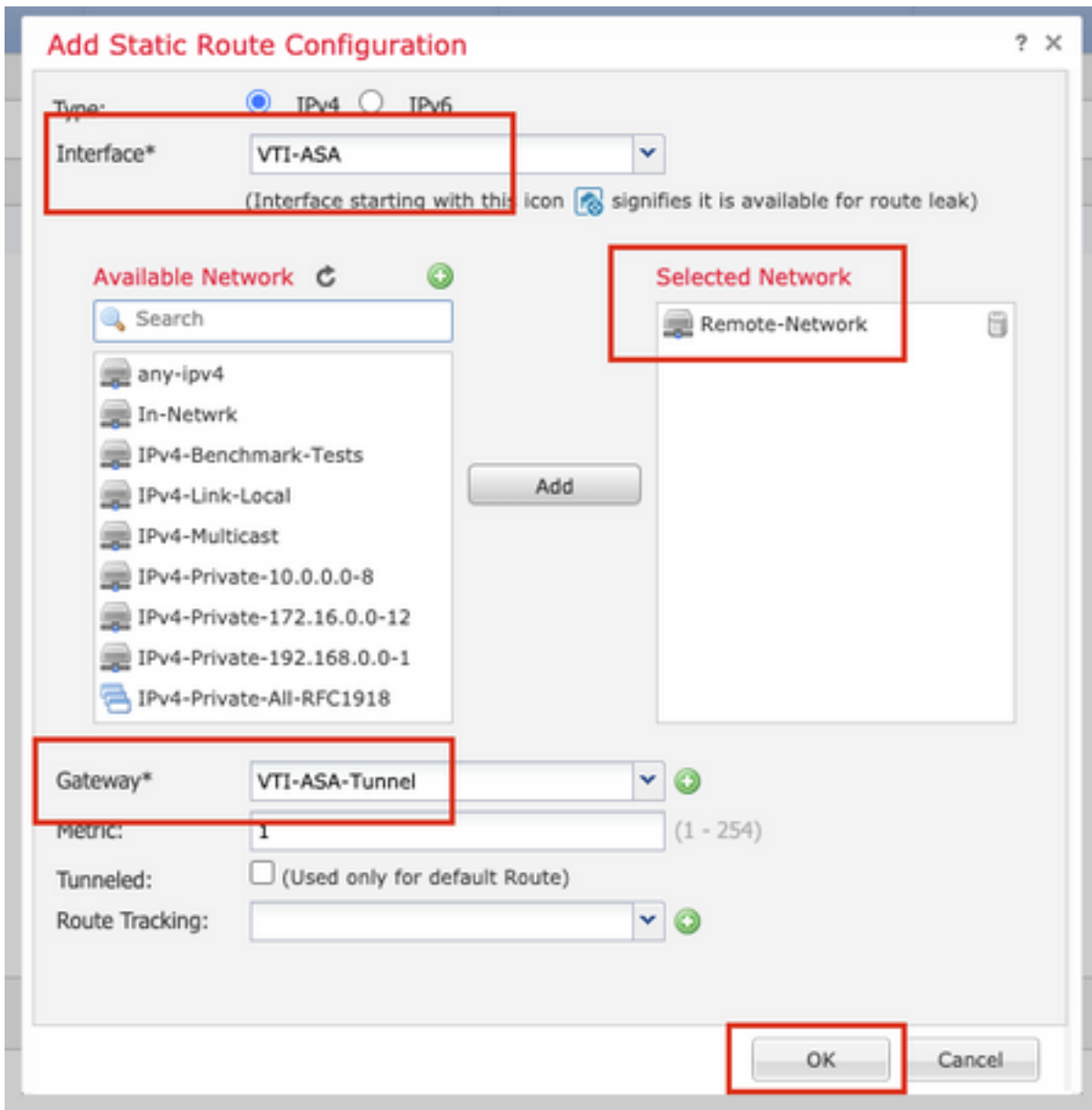
Verstrek de **interface**, kies het **netwerk**, verstrek de **gateway**. Klik op **OK**.

Ten behoeve van deze demonstratie:

**Interface:** VTI-ASA

**Netwerk:** Remote-Network

**Gateway:** VTI-ASA-Tunnel



Stap 19. Navigeer om > **Plaatsing te implementeren**. Kies de FTD waarop de configuratie moet worden ingezet en klik op **Implementeren**.

Configuratie naar de FTD CLI geduwd na succesvolle implementatie:

```

crypto ikev2 policy 1
encryption aes-256
integrity sha512
group 21
prf sha512
lifetime seconds 86400
crypto ikev2 enable Outside

crypto ipsec ikev2 ipsec-proposal CSM_IP_1
protocol esp encryption aes-256
protocol esp integrity sha-512
crypto ipsec profile FMC_IPSEC_PROFILE_1
set ikev2 ipsec-proposal CSM_IP_1
set pfs group21

group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
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 ikev1 ikev2

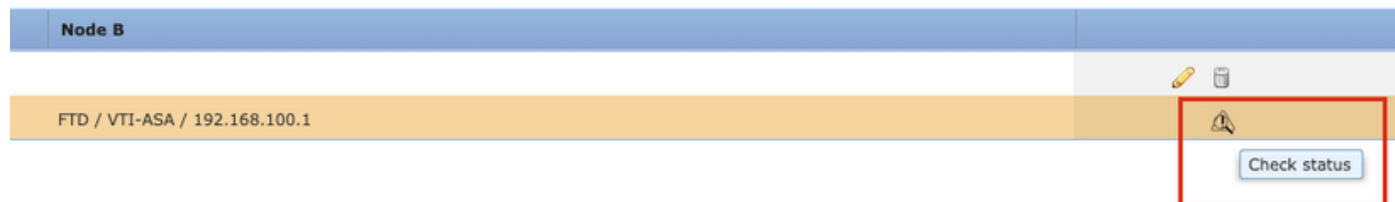
tunnel-group 10.106.67.252 type ipsec-l2l
tunnel-group 10.106.67.252 general-attributes
default-group-policy .DefaultS2SGroupPolicy
tunnel-group 10.106.67.252 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

```
interface Tunnel1
description VTI Tunnel with Extranet ASA
nameif VTI-ASA
ip address 192.168.100.1 255.255.255.252
tunnel source interface Outside
tunnel destination 10.106.67.252
tunnel mode ipsec ipv4
tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

## Verifiëren

### Van FMC GUI

Klik op de optie **Status controleren** om de live status van de VPN-tunnel vanuit de GUI zelf te bewaken



Dit omvat de volgende opdrachten die zijn overgenomen van de FTD CLI:

- **crypto ipsec tonen als peer <peer IP-adres>**
- **toon vpn-sessiondb detail l2l filter ipaddress <Peer IP Address>**



**Tunnel Status**

**extranet : ASA-Peer**

```
> show crypto ipsec sa peer
Not applicable for extranet peer
```

```
> show vpn-sessiondb detail l2l filter ipaddress
Not applicable for extranet peer
```

**FTD/VTI-ASA**

```
> show crypto ipsec sa peer 10.106.67.252
peer_address: 10.106.67.252
Crypto map tag: __vti-crypto-map-4-0-1, seq num: 65280, local addr:
10.197.224.90

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 10.106.67.252

#pkts encaps: 100, #pkts encrypt: 100, #pkts digest: 100
#pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 100, #pkts comp failed: 0, #pkts decomp
failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments
created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.197.224.90/500, remote crypto endpt.:
10.106.67.252/500
```

```
> show vpn-sessiondb detail l2l filter ipaddress 10.106.67.252
Session Type: LAN-to-LAN Detailed
Connection      : 10.106.67.252
Index           : 44
Protocol        : IKEv2 IPsec
Encryption     : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing        : IKEv2: (1)SHA512 IPsec: (1)SHA512
Bytes Tx       : 10000
Bytes Rx       : 10000
Login Time     : 03:54:57 UTC Thu Nov 12 2020
Duration       : 0h:02m:12s
Tunnel Zone    : 0

IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
Tunnel ID      : 44.1
UDP Src Port   : 500
Rem Auth Mode  : preSharedKeys
Loc Auth Mode  : preSharedKeys
Encryption     : AES256
Rekey Int (T) : 86400 Seconds
PRF            : SHA512
UDP Dst Port   : 500
Hashing        : SHA512
Rekey Left(T) : 86268 Seconds
D/H Group      : 21
```

Refresh Close

## Van FTD CLI

Deze opdrachten kunnen vanuit de FTD CLI worden gebruikt om de configuratie en de status van de VPN-tunnels te bekijken.

```
show running-config crypto
show running-config nat
show running-config route
show crypto ikev1 sa detailed
show crypto ikev2 sa detailed
show crypto ipsec sa detailed
show vpn-sessiondb detail l2l
```

## 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.