Site-to-Site VPN configureren op FTD beheerd door FDM

Inhoud

Inleiding

Dit document beschrijft hoe u Site-to-Site VPN kunt configureren op Firepower Threat Defence (FTD), beheerd door FirePower Device Manager (FDM).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van VPN
- Ervaring met FDN
- Ervaring met opdrachtregel voor adaptieve security applicatie (ASA)

Gebruikte componenten

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

- Cisco FTD 6.5
- ASA 9.10(1)32
- IKEv2

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.

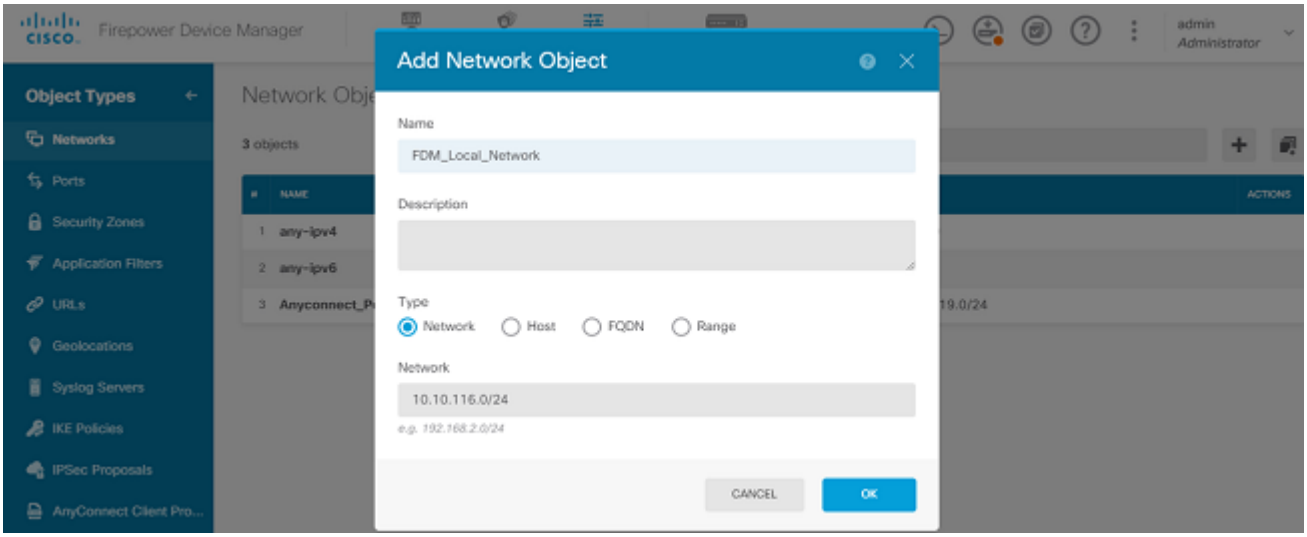
Configureren

Begin met de configuratie op FTD met FDM.

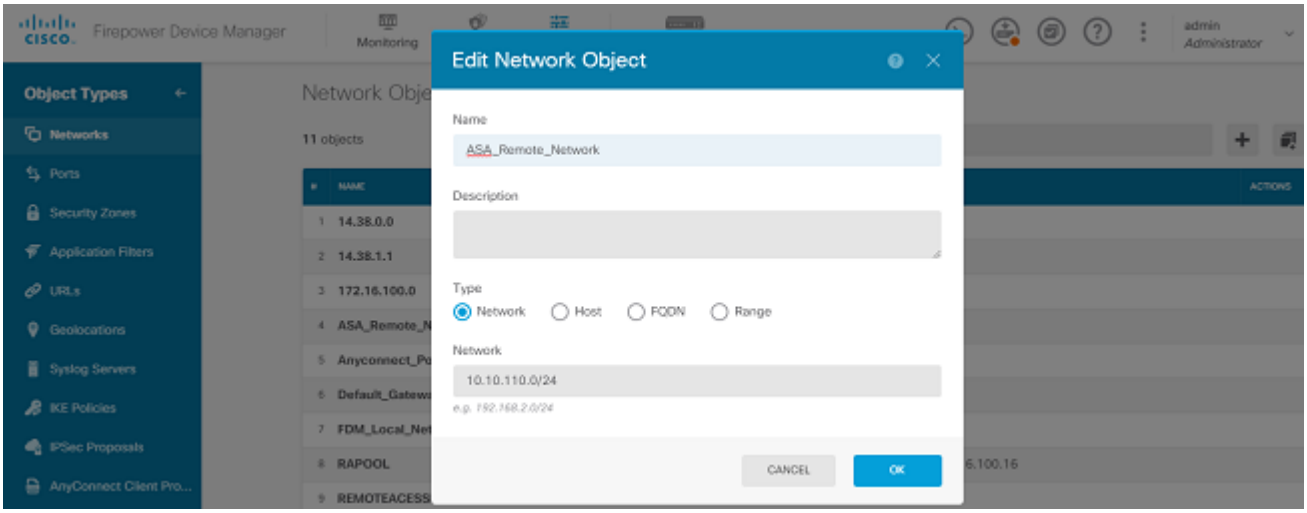
Beschermde netwerken definiëren

Ga naar **Objecten > Netwerken > Nieuw netwerk toevoegen**.

Configureer objecten voor de LAN-netwerken vanuit FDM GUI. Maak een object voor het lokale netwerk achter het FDM-apparaat zoals in de afbeelding.



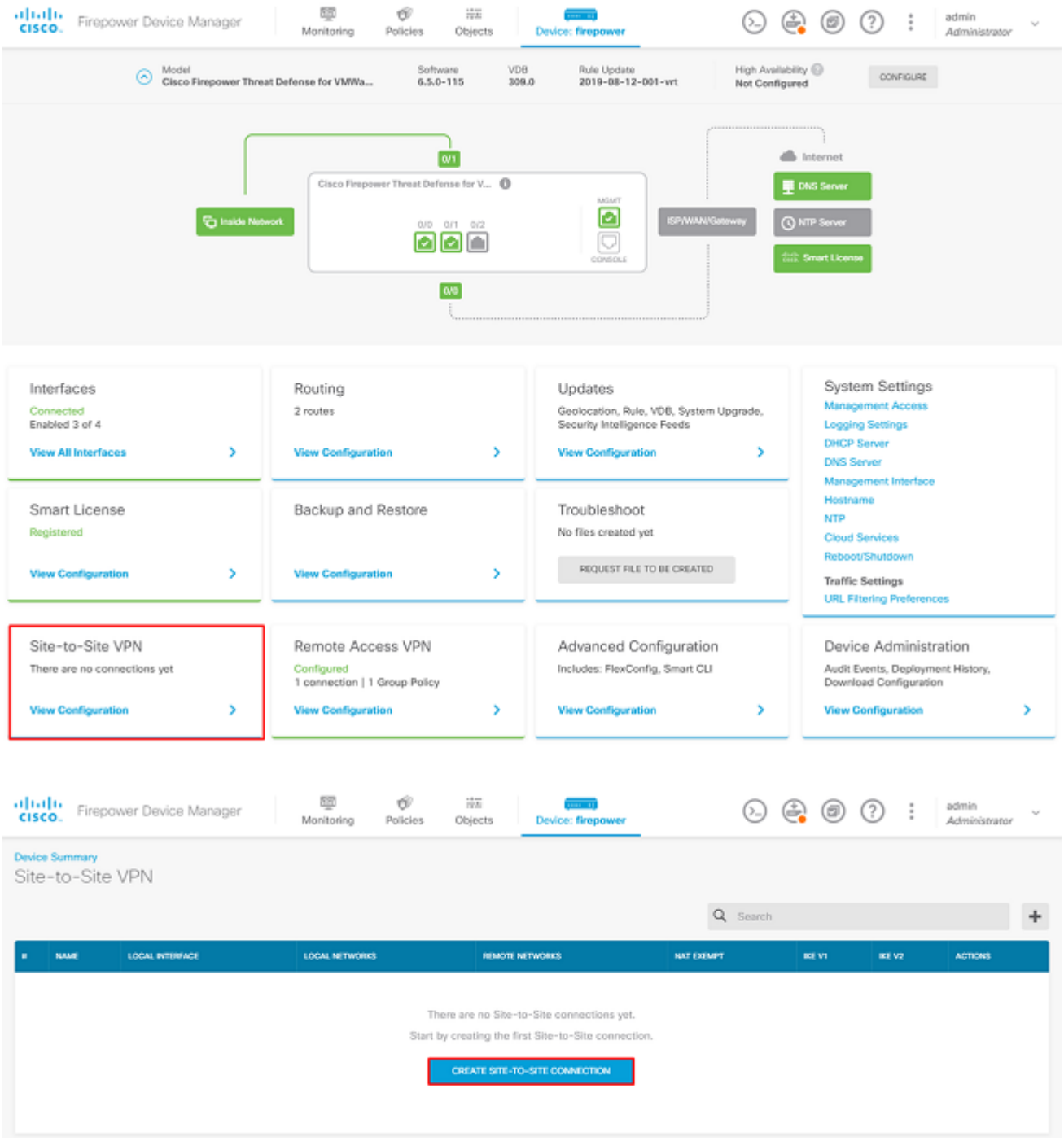
Maak een object voor het externe netwerk achter het ASA apparaat zoals in de afbeelding.



Site-to-Site VPN configureren

Ga naar **Site-to-Site VPN > Site-to-Site verbinding maken**.

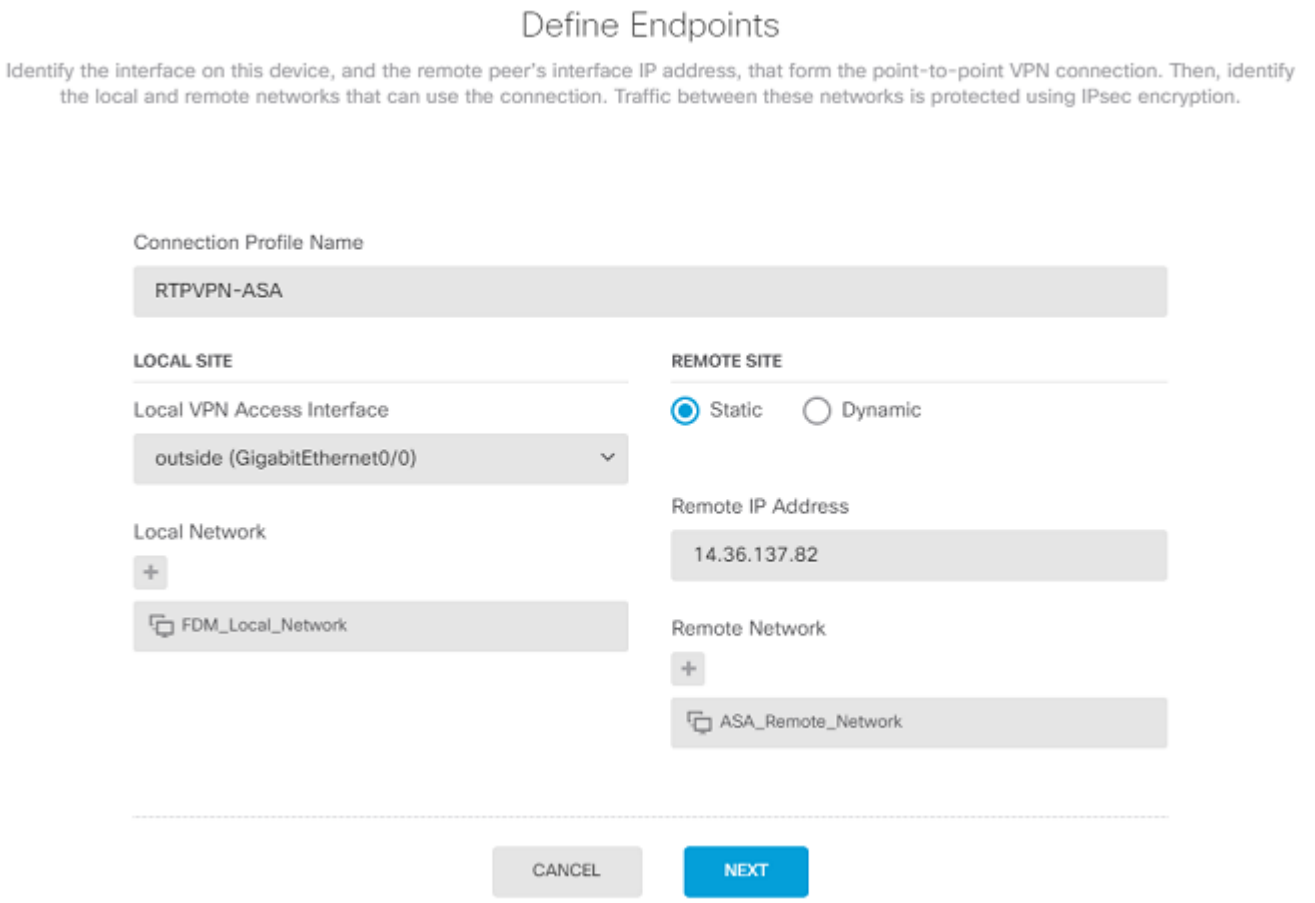
Ga door de site-to-site wizard op FDM zoals in de afbeelding.



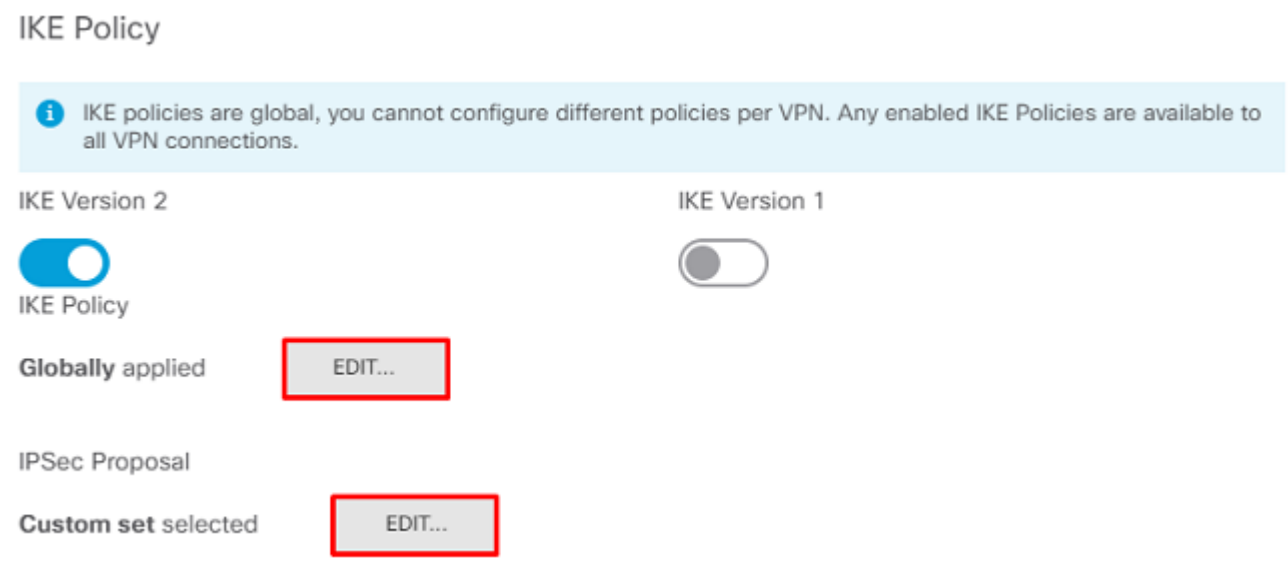
Geef de Site-to-Site verbinding een gemakkelijk herkenbare naam voor het verbindingsprofiel.

Kies de juiste externe interface voor de FTD en kies vervolgens het lokale netwerk dat moet worden versleuteld over de site naar site VPN.

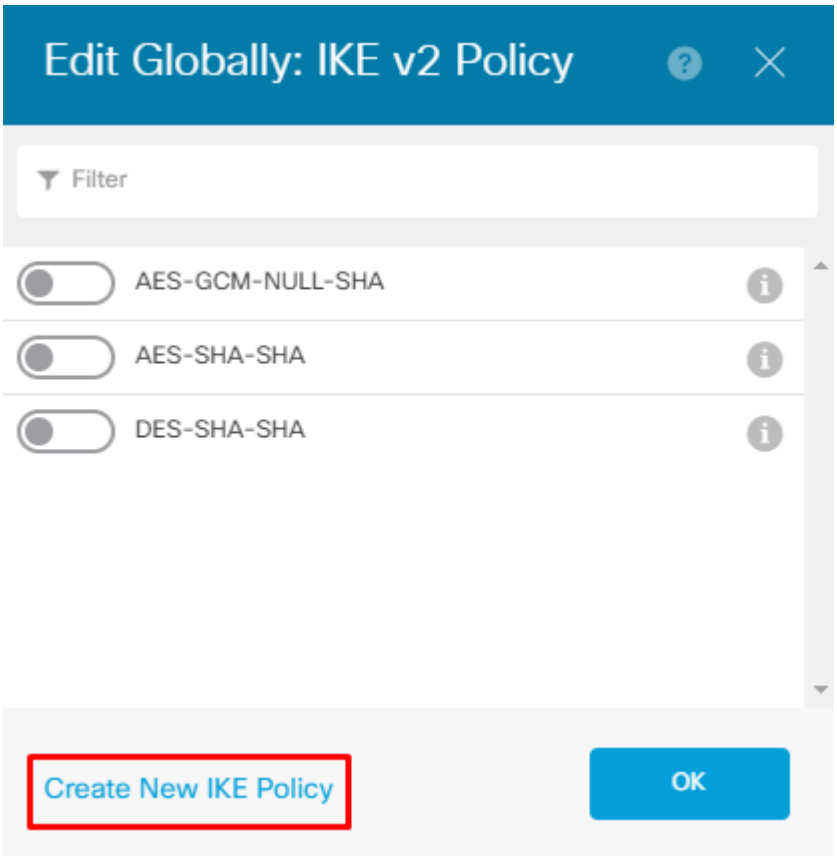
Stel de openbare interface van de remote peer in. Kies vervolgens het netwerk van externe peers dat over de Site-to-Site VPN is versleuteld zoals in de afbeelding.



Kies op de volgende pagina de knop **Bewerken** om de parameters voor Internet Key Exchange (IKE) in te stellen zoals in de afbeelding.

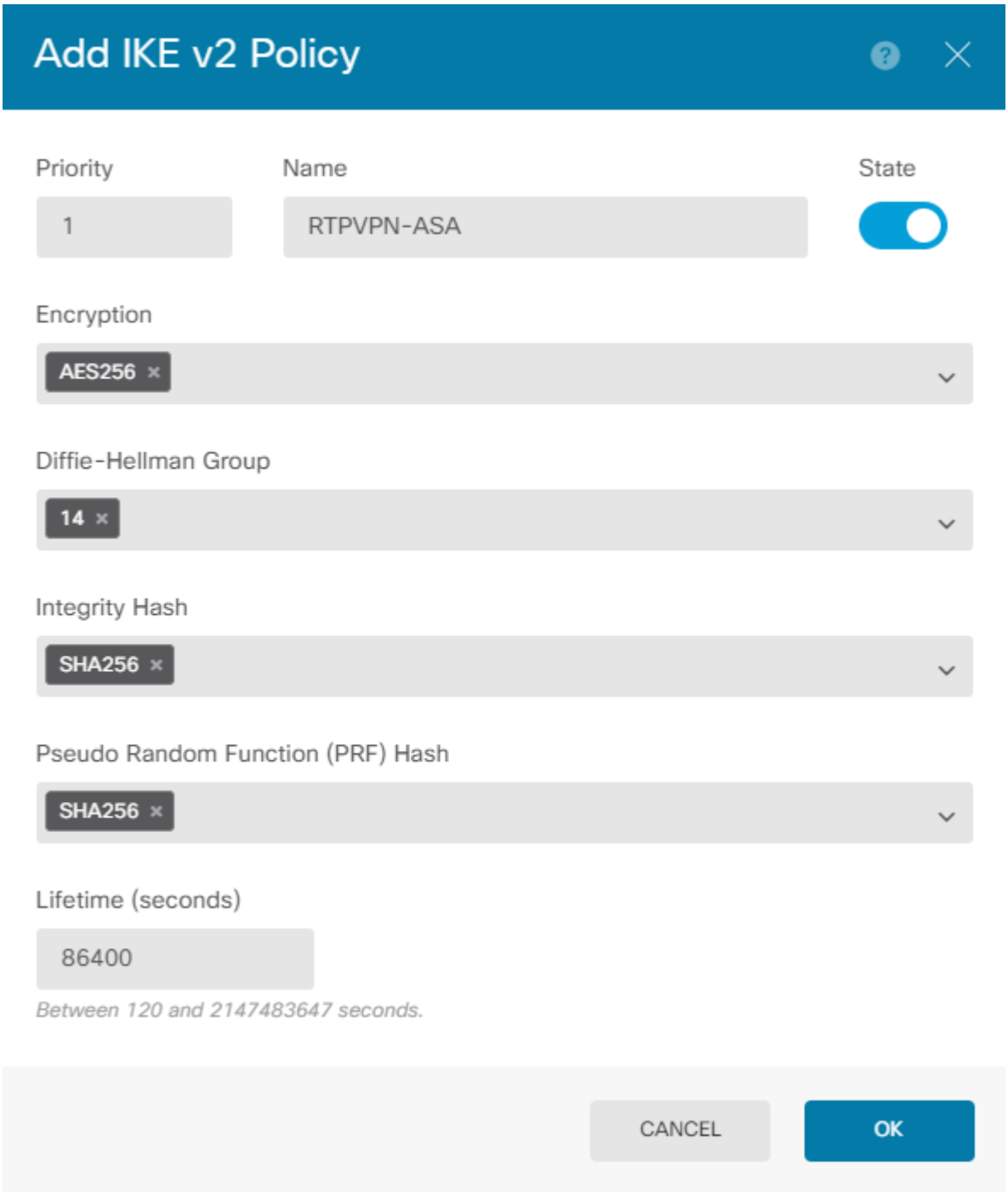


Kies de knop **Nieuw IKE-beleid maken** zoals in de afbeelding.

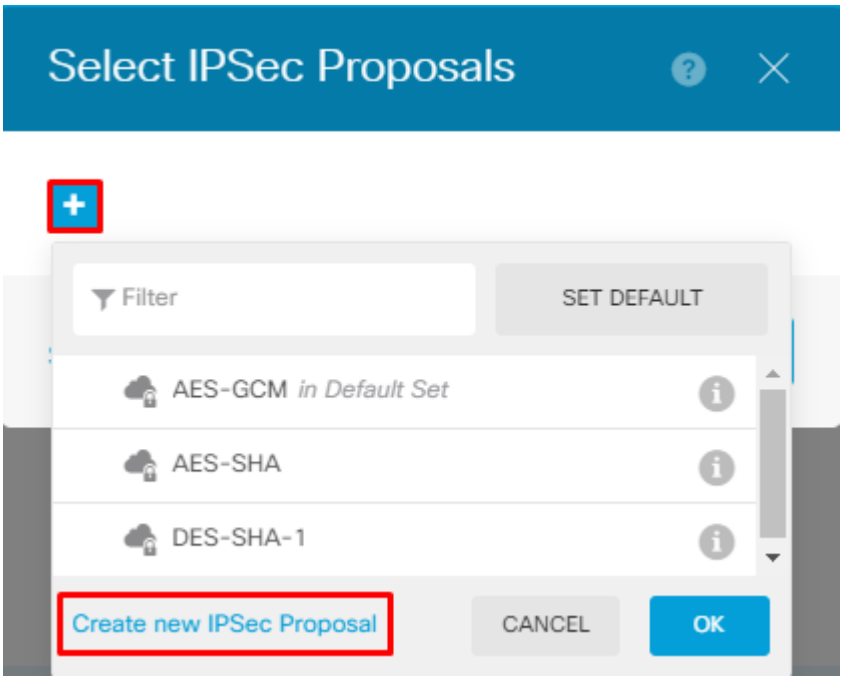


Deze gids gebruikt deze parameters voor de eerste uitwisseling IKEv2:

Encryptie AES-256
Integriteit SHA256
DH-groep 14
PRF-SHA256



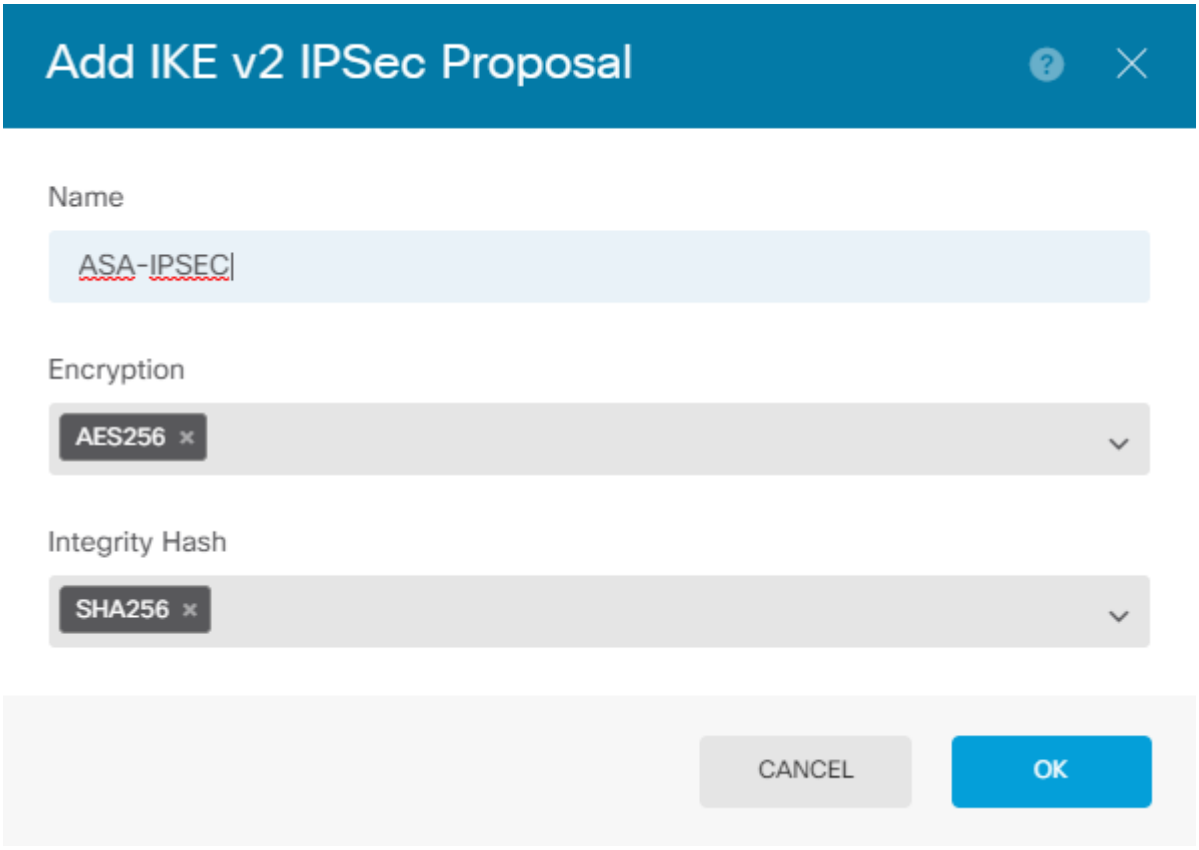
Eenmaal terug op de hoofdpagina, kies de **knop Bewerken** voor het IPSec-voorstel. Maak een nieuw IPSec-voorstel zoals in de afbeelding.



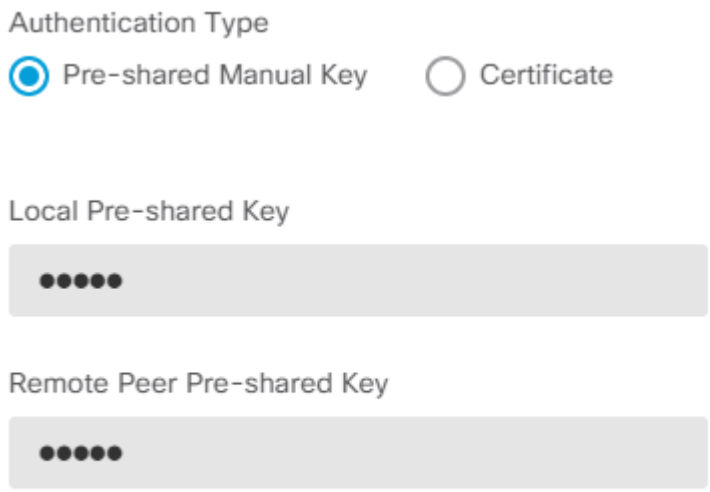
Deze handleiding gebruikt deze parameters voor IPSec:

Encryptie AES-256

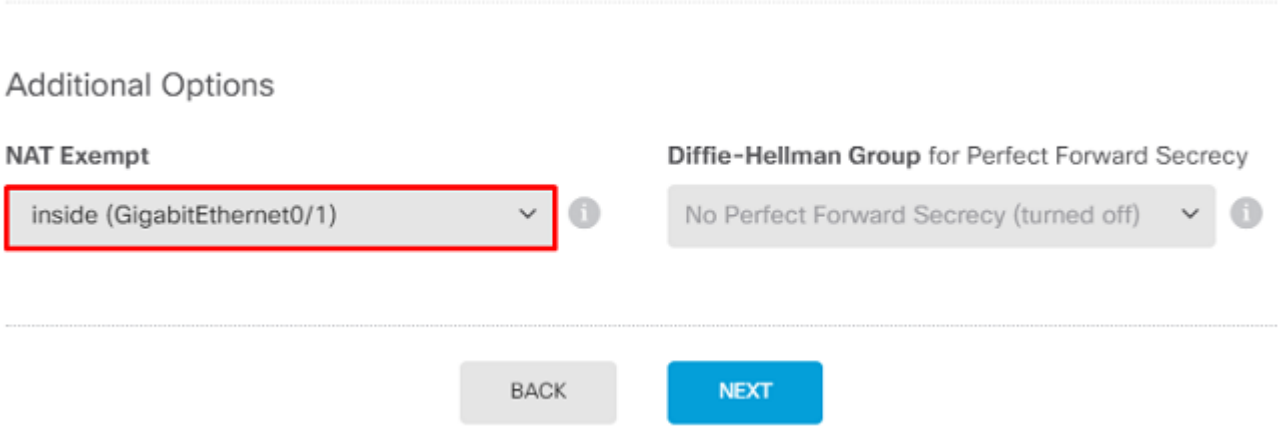
Integriteit SHA256



Stel de verificatie in op de vooraf gedeelde sleutel en voer de vooraf gedeelde sleutel (PSK) in die aan beide uiteinden wordt gebruikt. In deze handleiding wordt het PSK van Cisco gebruikt zoals in de afbeelding.



Stel de interne NAT Vrijgestelde interface in. Als er meerdere interne interfaces worden gebruikt, moet een handmatige NAT-vrijstellingsregel worden gemaakt onder **Beleid > NAT**.



Op de laatste pagina wordt een samenvatting van de Site-to-Site verbinding weergegeven. Zorg ervoor dat de juiste IP-adressen zijn geselecteerd, de juiste coderingsparameters worden gebruikt en druk op de knop Voltooien. Implementeer de nieuwe site-to-site VPN.

De ASA-configuratie is voltooid met het gebruik van de CLI.

ASA-configuratie

1. IKEv2 inschakelen op de buiteninterface van de ASA:

```
Crypto ikev2 enable outside
```

2. Maak het IKEv2-beleid dat dezelfde parameters definieert die op de FTD zijn geconfigureerd:

```
Crypto ikev2 policy 1
 Encryption aes-256
 Integrity sha256
 Group 14
 Prf sha256
 Lifetime seconds 86400
```

3. Maak een groepsbeleid dat het IKEv2 protocol toestaat:

```
Group-policy FDM_GP internal
Group-policy FDM_GP attributes
Vpn-tunnel-protocol ikev2
```

4. Maak een tunnelgroep voor het peer FTD openbare IP-adres. Verwijs naar het groepsbeleid en specificeer de pre-shared-key:

```
Tunnel-group 172.16.100.10 type ipsec-l2l
Tunnel-group 172.16.100.10 general-attributes
 Default-group-policy FDM_GP
Tunnel-group 172.16.100.10 ipsec-attributes
 ikev2 local-authentication pre-shared-key cisco
 ikev2 remote-authentication pre-shared-key cisco
```

5. Maak een toegangslijst waarin het te versleutelen verkeer wordt gedefinieerd: (FTDSubnet 10.10.116.0/24) (ASASubnet 10.10.110.0/24):

```
Object network FDMSubnet
 Subnet 10.10.116.0 255.255.255.0
Object network ASASubnet
 Subnet 10.10.110.0 255.255.255.0
Access-list ASAtoFTD extended permit ip object ASASubnet object FTDSubnet
```

6. Maak een IKEv2 IPsec-voorstel waarin wordt verwezen naar de algoritmen op de FTD:

```
Crypto ipsec ikev2 ipsec-proposal FDM
 Protocol esp encryption aes-256
 Protocol esp integrity sha-256
```

7. Maak een crypto map-ingang die de configuratie aan elkaar koppelt:

```
Crypto map outside_map 20 set peer 172.16.100.10
Crypto map outside_map 20 match address ASAtoFTD
Crypto map outside_map 20 set ikev2 ipsec-proposal FTD
Crypto map outside_map 20 interface outside
```

8. Maak een NAT-vrijstellingsverklaring die voorkomt dat het VPN-verkeer door de firewall wordt genaturaliseerd:

```
Nat (inside,outside) 1 source static ASASubnet ASASubnet destination static FDMSubnet FDMSubnet
no-proxy-arp route-lookup
```

Verifiëren

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

Probeer verkeer via de VPN-tunnel te initiëren. Met toegang tot de opdrachtregel van de ASA of FTD, kan dit worden gedaan met de pakkettracer-opdracht. Wanneer u de opdracht packet-tracer gebruikt om de VPN-tunnel te openen, moet deze twee keer worden uitgevoerd om te controleren of de tunnel omhoog komt. De eerste keer dat de opdracht wordt gegenereerd, is de VPN-tunnel ingedrukt zodat de pakkettracer-opdracht mislukt met VPN-encryptie DROP. Gebruik niet het binnen IP adres van de firewall als bron IP adres in de pakkettracer aangezien dit altijd ontbreekt.

```
firepower# packet-tracer input inside icmp 10.10.116.10 8 0 10.10.110.10

Phase: 9
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:


firepower# packet-tracer input inside icmp 10.10.116.10 8 0 10.10.110.10

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.100.1 using egress ifc outside

Phase: 2
Type: UN-NAT
Subtype: static
```

```
Result: ALLOW
Config:
nat (inside,outside) source static |s2sAclSrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 |s2sAclSrcNwgV4|
Additional Information:
NAT divert to egress interface outside
Untranslate 10.10.110.10/0 to 10.10.110.10/0

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group NGFW_ONBOX_ACL global
access-list NGFW_ONBOX_ACL advanced trust object-group |acSvcg-268435457 ifc inside any ifc outside any
access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule
object-group service |acSvcg-268435457
service-object ip
Additional Information:

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static |s2sAclSrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 |s2sAclSrcNwgV4|
Additional Information:
Static translate 10.10.116.10/0 to 10.10.116.10/0

Phase: 9
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Ga naar de CLI van de FTD of ASA om de tunnelstatus te bewaken.

Controleer vanuit de FTD CLI fase 1 en fase 2 met de opdracht **show crypto ikev2 sa**.

```
> show crypto ikev2 sa

IKEv2 SAs:

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
  3821043 172.16.100.10/500                               192.168.200.10/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
```

```
      Life/Active Time: 86400/1150 sec
Child sa: local selector  10.10.116.0/0 - 10.10.116.255/65535
          remote selector 10.10.110.0/0 - 10.10.110.255/65535
          ESP spi in/out: 0x7398dcbd/0x2303b0c0
```

Problemen oplossen

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

Aanvankelijke connectiviteitsproblemen

Wanneer je een VPN bouwt, zijn er twee partijen die onderhandelen over de tunnel. Daarom is het best om beide kanten van het gesprek te krijgen wanneer u problemen oplost elk type tunnelmislukking. Hier vindt u een gedetailleerde handleiding over het debuggen van IKEv2-tunnels: Hoe IKEv2 VPNâ€™s te debuggen

De meest voorkomende oorzaak van tunneluitval is een connectiviteitsprobleem. De beste manier om dit te bepalen is pakketopnamen op het apparaat te nemen.

Gebruik deze opdracht om pakketopnamen op het apparaat te maken:

```
Capture capout interface outside match ip host 172.16.100.10 host 192.168.200.10
```

Zodra de opname op zijn plaats is, probeer verkeer via VPN te verzenden en controleer op bidirectioneel verkeer in de pakketopname.

Herzie de pakketopname met het bevel **tonen GLB capout**.

```
firepower# show cap capout

4 packets captured

   1: 01:21:06.763983       172.16.100.10.500 > 192.168.200.10.500:  udp 574
   2: 01:21:06.769415       192.168.200.10.500 > 172.16.100.10.500:  udp 619
   3: 01:21:06.770666       172.16.100.10.500 > 192.168.200.10.500:  udp 288
   4: 01:21:06.773748       192.168.200.10.500 > 172.16.100.10.500:  udp 256
```

Verkeerspecifieke problemen

Gemeenschappelijke verkeersproblemen die gebruikers ervaren zijn:

- Routingproblemen achter het FTD - interne netwerk dat geen pakketten kan routeren naar de toegewezen IP-adressen en VPN-clients.
- Toegangscontrolelijsten die verkeer blokkeren.

- Netwerkadresomzetting (NAT) wordt niet overgeslagen voor VPN-verkeer.

Gerelateerde informatie

Voor meer informatie over site-to-site VPNâ€™s op de FTD die door FDM wordt beheerd, vindt u hier de volledige configuratiehandleiding.

- FTD beheerd door FDM Configuration Guide.

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.