

Site to Site VPN-configuratie op FTD beheerde door FMC

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratie](#)

[Stap 1. Bepaal de VPN-topologie.](#)

[Stap 2. Configuratie van IKE-parameters.](#)

[Stap 3. Configuratie van IPsec-parameters.](#)

[Stap 4. Bypass Access Control.](#)

[Stap 5. Maak een toegangscontrolebeleid.](#)

[Stap 6. Configureer de NAT-vrijstelling.](#)

[Stap 7. Configureer de ASA.](#)

[Verifiëren](#)

[Probleemoplossing en debug](#)

[Aanvankelijke connectiviteitsproblemen](#)

[Verkeersspecifieke kwesties](#)

Inleiding

Dit document biedt een configuratievoorbeeld voor Site VPN via Firepower Threat Defense (FTD), dat door FMC wordt beheerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basis begrip van VPN
- Ervaring met FireSIGHT Management Center
- Ervaring met ASA-opdrachtregel

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configuratie

Begin met de configuratie op FTD met FirePower Management Center.

Stap 1. Bepaal de VPN-topologie.

1. Navigeer naar **Apparaten > VPN > Site To Site**. Onder **Add VPN** klikt u op **Firepower Threat Defense Devices**, zoals in deze afbeelding wordt getoond.



2. Het vakje **Nieuwe VPN-topologie maken** verschijnt. Geef VPN een naam die gemakkelijk herkenbaar is.

Netwerktopologie: Punt

IKE versie: IKEv2

In dit voorbeeld wanneer u eindpunten selecteert, is Node A de FTD, en Node B de ASA. Klik op de knop groen plus om apparaten aan de topologie toe te voegen, zoals in deze afbeelding wordt weergegeven.

Create New VPN Topology

Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints | IKE | IPsec | Advanced

Node A: +

Device Name	VPN Interface	Protected Networks

Node B: +

Device Name	VPN Interface	Protected Networks

i Ensure the protected networks are allowed by access control policy of each device.

3. Voeg de FTD toe als eerste eindpunt.

Kies de interface waarop een crypto map is geplaatst. Het IP-adres moet uit de apparaatconfiguratie automatisch worden ingevuld.

Klik op groen plus onder Beschermd Netwerken, zoals in deze afbeelding wordt getoond, om te selecteren welke subnetten in dit VPN moeten worden versleuteld.

Add Endpoint




Device:*

Interface:*


IP Address:*

This IP is Private

Connection Type:

Certificate Map: 

Protected Networks:*

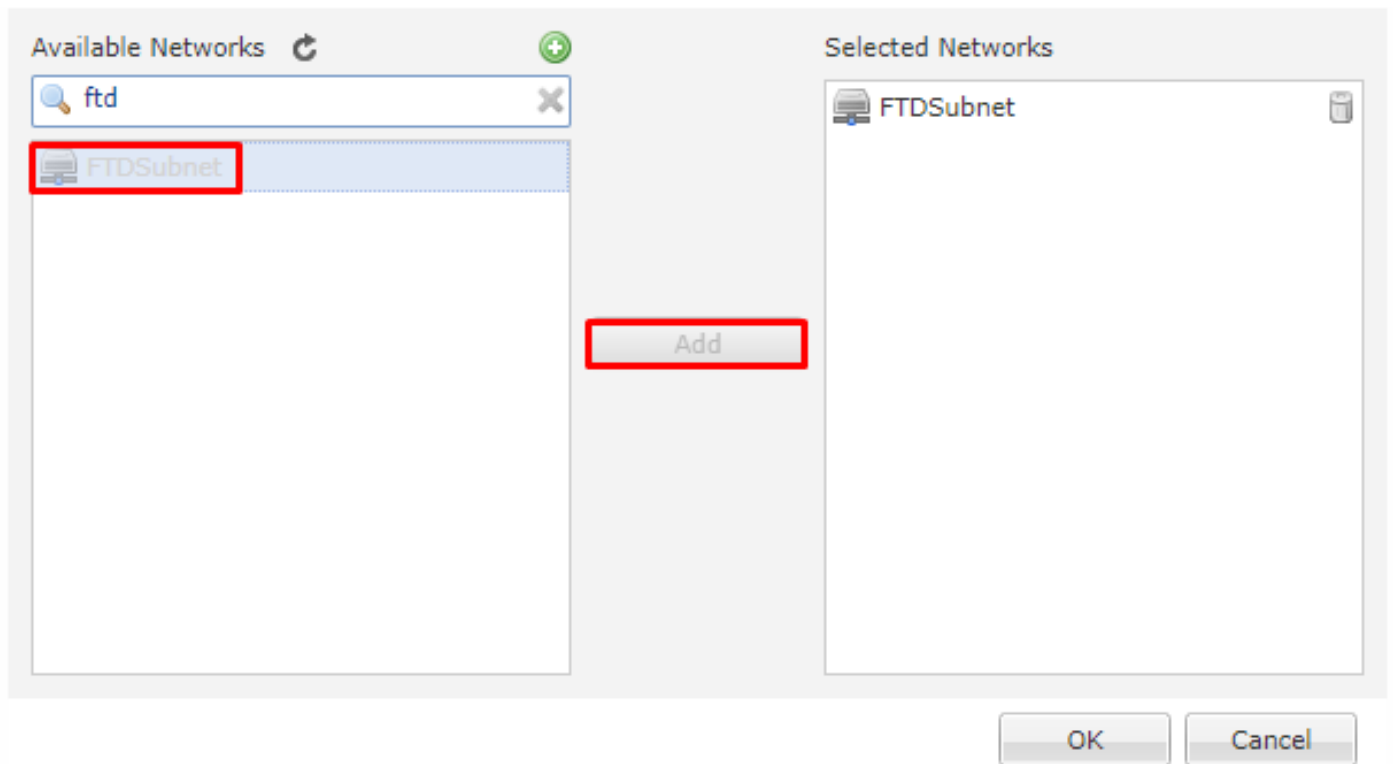
Subnet / IP Address (Network) Access List (Extended) 

4. Klik op groen plus en hier wordt een netwerkobject gemaakt.

5. Voeg alle lokale subnetten aan de FTD toe die moeten worden versleuteld. Klik op **Add** om ze naar de geselecteerde netwerken te verplaatsen. Klik nu op **OK**, zoals in deze afbeelding wordt weergegeven.

FTDSubnet = 10.10.113.0/24

Network Objects



Knooppunt A: (FTD) Het eindpunt is volledig. Klik op groen plus voor knooppunt B, zoals in de afbeelding wordt weergegeven.

Create New VPN Topology

Topology Name: RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version: IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Node A:

Device Name	VPN Interface	Protected Networks
FTD	outside/172.16.100.20	FTDSubnet

Node B:

Device Name	VPN Interface	Protected Networks

ⓘ Ensure the protected networks are allowed by access control policy of each device.

Save Cancel

Knooppunt B is een ASA. Apparaten die niet door het FMC worden beheerd, worden beschouwd als extranet.

6. Voeg een apparatennaam en IP adres toe. Klik op groen plus om beschermde netwerken toe te voegen, zoals in de afbeelding.

Edit Endpoint



Device:*

Device Name:*

IP Address:* Static Dynamic

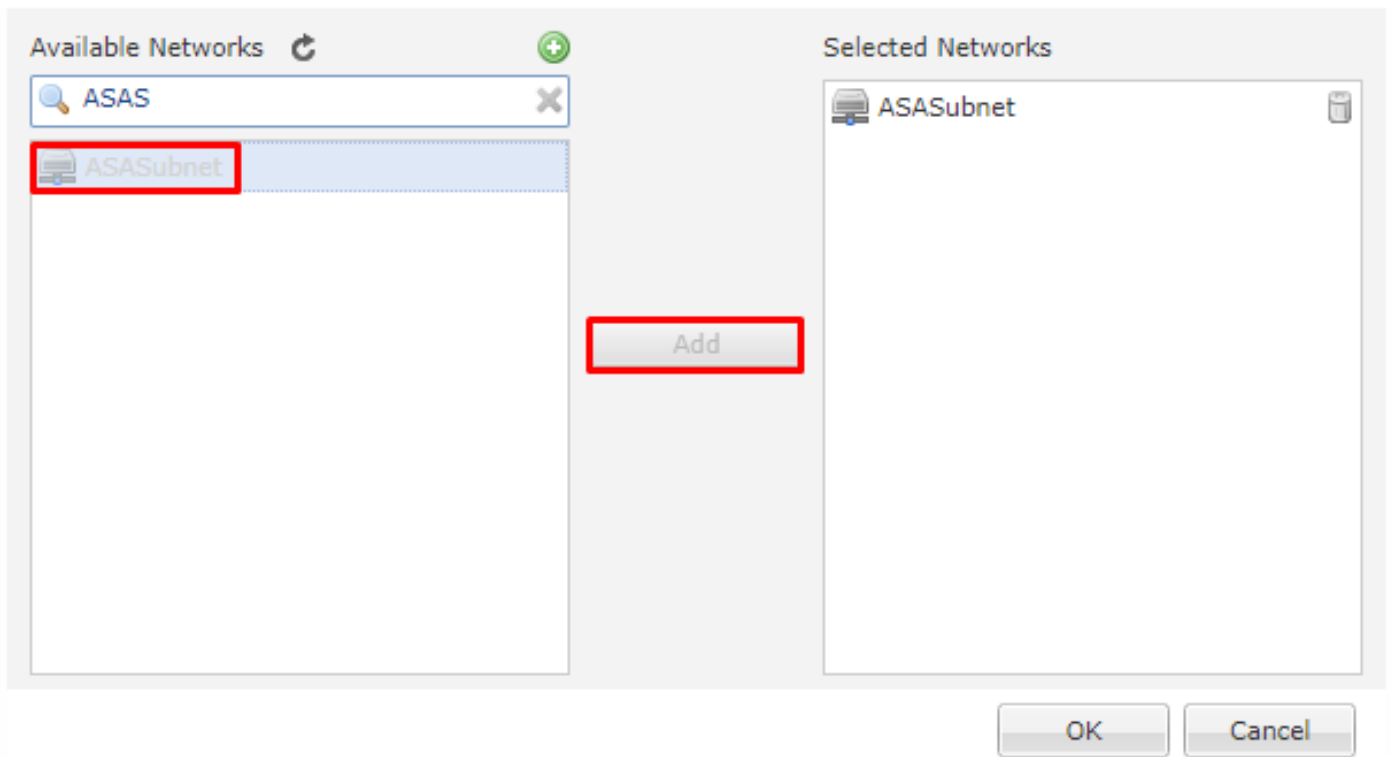
Certificate Map:

Protected Networks:*
 Subnet / IP Address (Network) Access List (Extended)

7. Zoals in deze afbeelding wordt getoond, selecteert u de **ASA**-subnetwerken die moeten worden versleuteld en voegt u deze toe aan de geselecteerde netwerken.

ASASubnet = 10,10.110.0/24

Network Objects



Stap 2. Configuratie van IKE-parameters.

Beide eindpunten zijn nu ingesteld in de IKE/IPSEC-configuratie.

1. Specificeer onder het tabblad **IKE** de parameters die worden gebruikt voor de eerste IKEv2-uitwisseling. Klik op groen plus om een nieuw IKE-beleid te maken, zoals in de afbeelding wordt weergegeven.

Create New VPN Topology ? X


Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced


IKEv1 Settings

Policy:* 

Authentication Type:

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

IKEv2 Settings

Policy:* 

Authentication Type:

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

2. Specificeer in het nieuwe IKE-beleid een prioriteitsnummer en de levensduur van fase 1 van de verbinding. Dit document gebruikt deze parameters voor de eerste uitwisseling: Integrity (SHA256), Encryption (AES-256), PRF (SHA256) en Diffie-Hellman groep (groep 14)

Opmerking: Al het IKE beleid op het apparaat wordt verzonden naar de verre peer ongeacht wat in het geselecteerde beleidsgedeelte is. Het eerste IKE-beleid dat door de externe peer wordt aangepast, wordt geselecteerd voor de VPN-verbinding. Kies eerst welk beleid er wordt verstuurd met behulp van het prioriteitsveld. Prioriteit 1 zal eerst worden verstuurd.

New IKEv2 Policy

Name:*

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)

- Integrity Algorithms**
- Encryption Algorithms
- PRF Algorithms
- Diffie-Hellman Group

- Available Algorithms
- MD5
 - SHA
 - SHA512
 - SHA256**
 - SHA384
 - NULL

Add

- Selected Algorithms
- SHA256

Save Cancel

New IKEv2 Policy

Name:*

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- AES
- AES-256
- DES
- 3DES
- AES-192
- AES-GCM
- AES-GCM-192
- AES-GCM-256
- NULL

Selected Algorithms

- AES-256

Add

New IKEv2 Policy



Name:*

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)

- Integrity Algorithms
- Encryption Algorithms
- PRF Algorithms**
- Diffie-Hellman Group

Available Algorithms

- MD5
- SHA
- SHA512
- SHA256
- SHA384

Add

Selected Algorithms

- SHA256

Save Cancel

New IKEv2 Policy



Name:*

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Groups

- 1
- 2
- 5
- 14**
- 15
- 16
- 19
- 20
- 21

Add

Selected Groups

- 14

Save Cancel

3. Zodra de parameters zijn toegevoegd, selecteert u dit beleid en kiest u het **verificatietype**.

4. Kies **de** handleiding **van de voorgedeelde sleutel**. Voor dit document wordt de PSK cisco123 gebruikt.

Create New VPN Topology ? X

Topology Name:* RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh5_5

Authentication Type: Pre-shared Automatic Key

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

IKEv2 Settings

Policy:* **ASA**

Authentication Type: **Pre-shared Manual Key**

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Save Cancel

Stap 3. Configuratie van IPsec-parameters.

1. Klik onder **IPsec** op het potlood om de transformatieset te bewerken en om een nieuw IPsec-voorstel te maken, zoals in deze afbeelding wordt getoond.

Create New VPN Topology

Topology Name:* RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE **IPsec** Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group: 14

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

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

— ESPv3 Settings

Save Cancel

2. Om een nieuw IKEv2 IPsec-voorstel te maken, klikt u op groen plus en voert u de fase 2-parameters in.

Selecteer **ESP Encryption > AES-GCM-256**. Wanneer het GCM-algoritme wordt gebruikt voor encryptie, is er geen Hash-algoritme nodig. Met de GCM is de hashfunctie ingebouwd.

Edit IKEv2 IPsec Proposal



Name:* ASA

Description:

ESP Hash

ESP Encryption

Available Algorithms

- AES-GCM-256
- AES-256
- AES-GCM-192
- AES-192
- AES-GCM
- AES
- 3DES
- DES
- AES-GMAC-25

Add

Selected Algorithms

- AES-GCM-256

Save Cancel

3. Nadat het nieuwe IPsec-voorstel is gemaakt, voegt u dit toe aan de geselecteerde transformatiesets.

IKEv2 IPsec Proposal



Available Transform Sets

Search

- AES-GCM
- AES-SHA
- ASA
- DES_SHA-1

Add

Selected Transform Sets

- ASA

OK Cancel

Het nieuw geselecteerde IPsec-voorstel is nu opgenomen in de IKEv2 IPsec-voorstellen.

Indien nodig kunnen de fase 2-levensduur en de PFS hier worden bewerkt. Dit voorbeeld: de levensduur wordt standaard ingesteld en PFS uitgeschakeld.

Create New VPN Topology

Topology Name: RTPVPN-ASA

Network Topology: Point to Point | Hub and Spoke | Full Mesh

IKE Version: IKEv1 IKEv2

Endpoints | IKE | **IPsec** | Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets:

- IKEv1 IPsec Proposals: tunnel_aes256_sha
- IKEv2 IPsec Proposals: ASA

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group: 14

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

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

ESPv3 Settings

Save Cancel

Optioneel - U moet de optie Vultooien om toegangscontrole te omzeilen of een toegangsbeheerbeleid maken.

Stap 4. Bypass Access Control.

Optioneel kan **sysopt licentie-VPN** ingeschakeld worden onder **Advanced > Tunnel**.

Hierdoor wordt de mogelijkheid om het toegangscontrolebeleid te gebruiken om het verkeer van de gebruikers te inspecteren geschrapt. VPN-filters of downloadbare ACL's kunnen nog steeds worden gebruikt om gebruikersverkeer te filteren. Dit is een wereldwijde opdracht en is van toepassing op alle VPN's als deze selectietekens ingeschakeld zijn.

Create New VPN Topology ? x

Topology Name:* RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE IPsec **Advanced**

IKE
IPsec
Tunnel

NAT Settings

Keepalive Messages Traversal
Interval: 20 Seconds (Range 10 - 3600)

Access Control for VPN Traffic

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Certificate Map Settings

Use the certificate map configured in the Endpoints to determine the tunnel

Use the certificate OU field to determine the tunnel

Use the IKE identity to determine the tunnel

Use the peer IP address to determine the tunnel

Save Cancel

Als **sysopt vergunning-vpn** niet is ingeschakeld moet er een toegangscontrolebeleid worden ontwikkeld om het VPN-verkeer via het FTD-apparaat mogelijk te maken. Als **sysopt licentie-vpn** is ingeschakeld, moet u een toegangsbeheerbeleid instellen.

Stap 5. Maak een toegangscontrolebeleid.

Onder Toegangsbeheer Beleid, navigeer naar **Beleid > Toegangsbeheer > Toegangsbeheer** en selecteer het Beleid dat op het FTD apparaat gericht is. Als u een regel wilt toevoegen, klikt u op **Regel toevoegen**, zoals in de afbeelding hier wordt weergegeven.

Het verkeer moet worden toegestaan vanaf het interne netwerk naar het externe netwerk en vanaf het externe netwerk naar het interne netwerk. Eén regel maken om beide regels te doen of twee regels te maken om ze gescheiden te houden. In dit voorbeeld wordt één regel gecreëerd om beide te doen.

Editing Rule - VPN_Traffic

Name: VPN_Traffic Enabled [Move](#)

Action: Allow

Zones: **Networks** | VLAN Tags | Users | Applications | Ports | URLs | SGT/ISE Attributes | Inspection | Logging | Comments

Available Networks:

Source Networks (2):

Source	Original Client
ASASubnet	
FTDSubnet	

Destination Networks (2):

ASASubnet
FTDSubnet

Buttons: Add To Source Networks, Add to Destination, Save, Cancel

Rules | Security Intelligence | HTTP Responses | Logging | Advanced

Filter by Device | Show Rule Conflicts | Add Category | Add Rule | Search Rules

Name	Source Zone	Dest Zones	Source Networks	Dest Networks	VL...	Us...	Ap...	So...	De...	URLs	So...	De...	A...	Options
1 VPN_Traffic	Inside Outside	Inside Outside	ASASubnet FTDSubnet	ASASubnet FTDSubnet	Any	Any	Any	Any	Any	Any	Any	Any	Any	0

Default Action: Access Control: Block All Traffic

Stap 6. Configureer de NAT-vrijstelling.

Configureer een NAT-vrijstellingsverklaring voor het VPN-verkeer. NAT-vrijstelling moet aanwezig zijn om te voorkomen dat VPN-verkeer een andere NAT-verklaring ondergaat en VPN-verkeer onjuist vertaalt.

1. navigeren naar **Apparaten > NAT**, selecteer het NAT beleid dat gericht is op de FTD. Maak een nieuwe regel zoals u op de knop **Toevoegen Regel** klikt.

Overview | Analysis | Policies | **Devices** | Objects | AMP | Intelligence

Device Management | **NAT** | VPN | QoS | Platform Settings | FlexConfig | Certificates

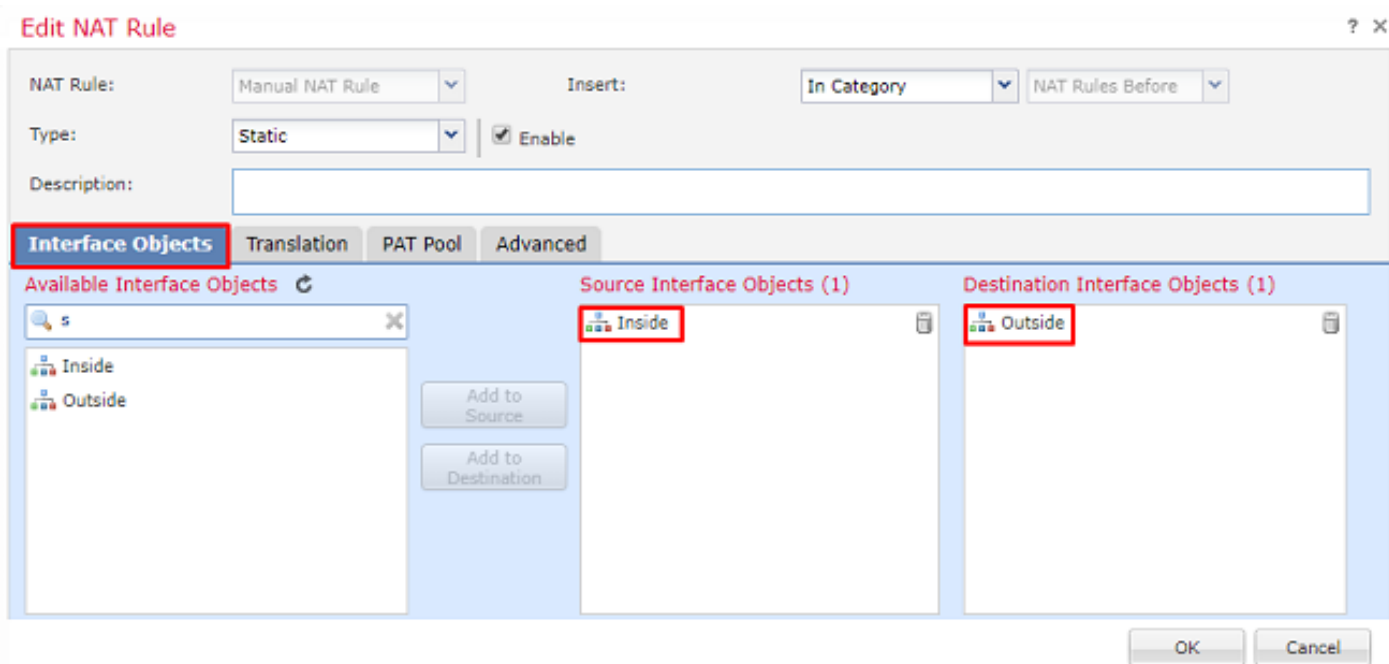
VirtualFTDNAT

Rules

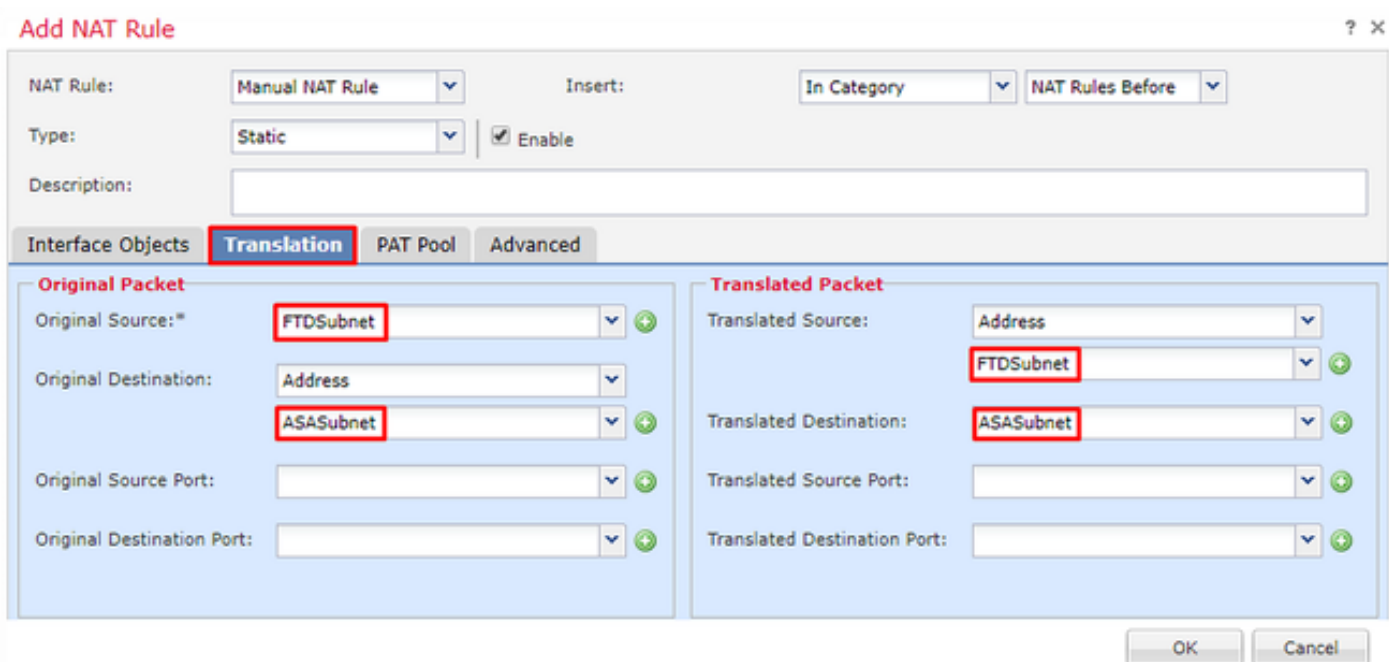
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
NAT Rules Before											
Auto NAT Rules											

Buttons: Show Warnings, Add Rule

2. Maak een nieuwe statische handleiding voor NAT-regels. Verwijzing naar de binnen- en buitenkant interfaces.



3. Onder het tabblad **Vertaling** selecteert u de bron- en doelsubnetten. Aangezien dit een NAT-vrijstellingsregel is, moet u de oorspronkelijke bron/bestemming en de vertaalde bron/bestemming hetzelfde maken als in deze afbeelding:



4. Ten slotte, verplaats naar het tabblad **Geavanceerd** en laat geen-proxy-arp en routelookup toe.

Add NAT Rule ? X

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Fallthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

5. Sla deze regel op en kijk naar de uiteindelijke resultaten in de NAT-lijst.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates Show Warnings Save Cancel

VirtualFTDNAT
Enter Description Policy Assignments

Rules Filter by Device Add Rule

#	Direction	Type	Source Interface...	Destination Interface...	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
▼ NAT Rules Before											
1	↔	Static	Inside	Outside	FTDSubnet	ASASubnet		FTDSubnet	ASASubnet		Dns:fal route-k no-pro
▼ Auto NAT Rules											
#	↔	Dynamic	Inside	Outside	any-obj			Interface			Dns:fal
▼ NAT Rules After											

6. Nadat de configuratie is voltooid, slaat u de configuratie op en stelt u deze in op de FTD.

Stap 7. Configureer de ASA.

1. Inschakelen van IKEv2 op de externe interface 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 protocol ikev2 toestaat:

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

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

```
Tunnel-group 172.16.100.20 type ipsec-l2l
Tunnel-group 172.16.100.20 general-attributes
Default-group-policy FTD_GP
Tunnel-group 172.16.100.20 ipsec-attributes
ikev2 local-authentication pre-shared-key cisco123
ikev2 remote-authentication pre-shared-key cisco123
```

5. Maak een toegangslijst waarin het te versleutelen verkeer wordt gedefinieerd: (FTDSubnet 10.10.113.0/24) (ASASubnet 10.10.110.0/24)

```
Object network FTDSUBNET
Subnet 10.10.113.0 255.255.255.0
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 dat verwijst naar de algoritmen die op de FTD zijn gespecificeerd:

```
Crypto ipsec ikev2 ipsec-proposal FTD
Protocol esp encryption aes-gcm-256
```

7. Maak een crypto map ingang die de configuratie verbindt:

```
Crypto map outside_map 10 set peer 172.16.100.20
Crypto map outside_map 10 match address ASAToFTD
Crypto map outside_map 10 set ikev2 ipsec-proposal FTD
Crypto map outside_map 10 interface outside
```

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

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

Verifiëren

Opmerking: Op dit moment is er geen manier om de VPN-tunnelstatus van het FMC te herzien. Er is een verbeteringsverzoek voor deze mogelijkheid [CSCvh77603](#).

Probeer verkeer door de VPN-tunnel te openen. Met toegang tot de opdrachtregel van de ASA of FTD, kan dit worden gedaan met de opdracht van de pakkettracer. Wanneer u de pakkettracer opdracht gebruikt om de VPN-tunnel op te halen, moet deze tweemaal worden uitgevoerd om te controleren of de tunnel omhoog komt. De eerste keer dat de opdracht wordt gegeven, is de VPN-tunnel afgedraaid, zodat de opdracht Packet-tracer niet verloopt met VPN-encryptie DROP. Gebruik het binnen IP-adres van de firewall niet als het bron-IP-adres in de pakketgeleider, aangezien dit altijd faalt.

```
firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10
```

```
Phase: 10
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:
```

```
firepower# packet-tracer input inside icmp 10.10.113.10 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 FTDSubnet FTDSubnet destination static ASASubnet ASASubnet
no-proxy-arp route-lookup
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 CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip ifc Inside object-group FMC_INLINE_src_rule_268436483
ifc outside object-group FMC_INLINE_dst_rule_268436483 rule-id 268436483
access-list CSM_FW_ACL_ remark rule-id 268436483: ACCESS POLICY: FTD-Access-Control-Policy -
Mandatory
access-list CSM_FW_ACL_ remark rule-id 268436483: L7 RULE: VPN_Traffic
object-group network FMC_INLINE_src_rule_268436483
description: Auto Generated by FMC from src of UnifiedNGFWRule# 1 (FTD-Access-Control-
Policy/mandatory)
network-object object ASASubnet
network-object object FTDSubnet
object-group network FMC_INLINE_dst_rule_268436483
description: Auto Generated by FMC from dst of UnifiedNGFWRule# 1 (FTD-Access-Control-
Policy/mandatory)
network-object object ASASubnet
network-object object FTDSubnet
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached
```

```
Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet
no-proxy-arp route-lookup
```

Additional Information:

Static translate 10.10.113.10/0 to 10.10.113.10/0

Phase: 10

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

Om de tunnelstatus te controleren, navigeer naar de CLI van de FTD of ASA.

Van de FTD CLI controleer fase-1 en fase-2 met deze opdracht:

Crypto ikev2 sa weergeven

```
> show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local

Remote

Status

Role

9528731 172.16.100.20/500

192.168.200.10/500

READY INITIATOR

Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK

Life/Active Time: 86400/118 sec

Child sa: local selector **10.10.113.0/0 - 10.10.113.255/65535**

remote selector **10.10.110.0/0 - 10.10.110.255/65535**

ESP spi in/out: **0x66be357d/0xb74c8753**

Probleemoplossing en debug

Aanvankelijke connectiviteitsproblemen

Wanneer je een VPN bouwt, onderhandelen er twee kanten over de tunnel. Daarom is het best om beide kanten van het gesprek te krijgen wanneer u een of ander type tunnelfalen problemen oplossen. Een gedetailleerde gids over hoe u tunnels IKEv2 kunt zuiveren kan hier worden gevonden: [Hoe te om IKEv2 VPN's te zuiveren](#)

De meest voorkomende oorzaak van tunnelfouten is een aansluitingsprobleem. De beste manier om dit te bepalen is pakketvastlegging op het apparaat te nemen. Gebruik deze opdracht om pakketopnamen op het apparaat te nemen:

```
Capture capout interface outside match ip host 172.16.100.20 host 192.168.200.10
```

Nadat de opname is geïnstalleerd, probeer dan verkeer via VPN te verzenden en controle te houden op bidirectioneel verkeer in de pakketvastlegging.

Controleer de pakketvastlegging met deze opdracht:

dop omhoog tonen

```
firepower# show cap capout
```

```
4 packets captured
```

```
1: 11:51:12.059628      172.16.100.20.500 > 192.168.200.10.500:  udp 690
2: 11:51:12.065243      192.168.200.10.500 > 172.16.100.20.500:  udp 619
3: 11:51:12.066692      172.16.100.20.500 > 192.168.200.10.500:  udp 288
4: 11:51:12.069835      192.168.200.10.500 > 172.16.100.20.500:  udp 240
```

Verkeersspecifieke kwesties

Vaak voorkomende verkeersproblemen:

- Routing issues achter de FTD — intern netwerk niet in staat om pakketten terug te sturen naar de toegewezen IP-adressen en VPN-clients.
- Toegangscontrolelijsten die verkeer blokkeren.
- Netwerkadresomzetting wordt niet omzeild voor VPN-verkeer.

Voor meer informatie over VPN's op de FTD die wordt beheerd door FMC, kunt u de volledige configuratiehandleiding hier vinden: [FTD beheerd door FMC-configuratiehandleiding](#)