

IKEv2 IPv6 site-to-site tunnel tussen ASA en FTD configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[ASA-configuratie](#)

[FTD-configuratie](#)

[Toegangsbeheer voor omzeilingen](#)

[NAT-vrijstelling configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Referenties](#)

Inleiding

Dit document biedt een configuratievoorbeeld voor het instellen van een IPv6-site om een IPv6-tunnel te creëren tussen een ASA (adaptieve security applicatie) en FTD (Firepower Threat Defense) door gebruik te maken van het protocol Internet Key Exchange versie 2 (IKEv2). De installatie omvat eind-aan-eind IPv6 netwerkconnectiviteit met ASA en FTD als VPN eindapparaten.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van de ASA CLI-configuratie
- Grondkennis van IKEv2- en IPSEC-protocollen
- Begrip van IPv6-adressering en -routing
- Basisbegrip van de FTD-configuratie via FMC

Gebruikte componenten

De informatie in dit document is gebaseerd op een virtuele omgeving, gemaakt van apparaten in een specifieke labo-instelling. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk in productie is, zorg ervoor dat u de

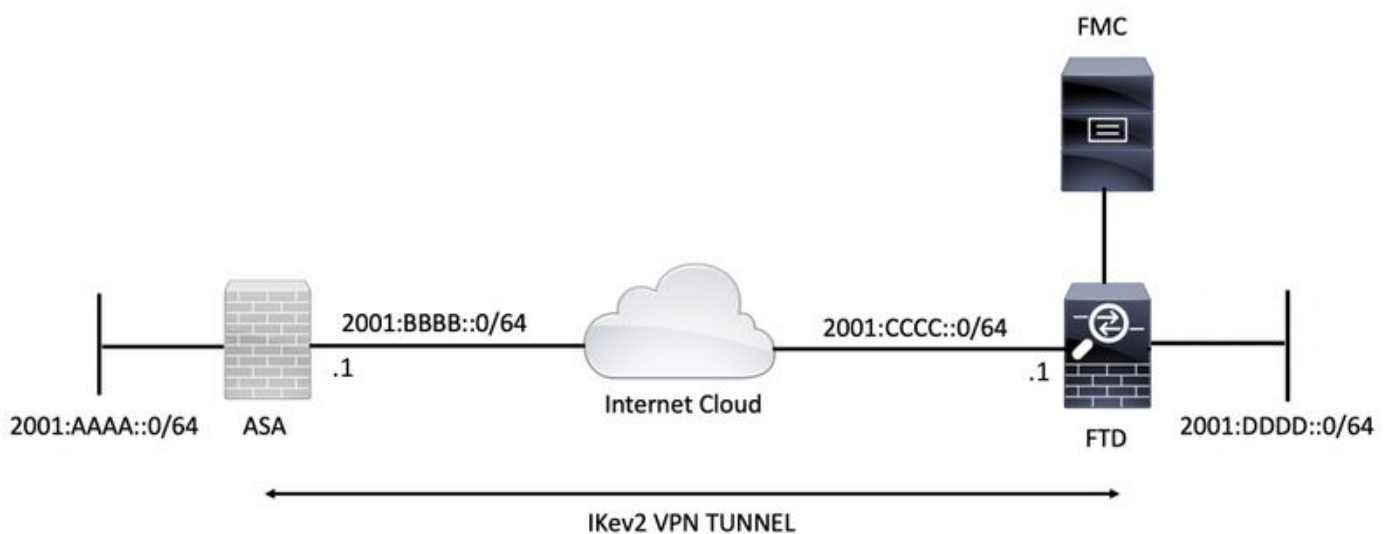
potentiële impact van om het even welke opdracht begrijpt.

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

- Cisco ASA 5500-X Series (4)12
- Cisco FTDv actief 6.5.0
- Cisco FMCv actief 6.6.0

Configureren

Netwerkdigram



ASA-configuratie

In dit deel wordt de configuratie beschreven die op de ASA-apparatuur vereist is.

Stap 1. Configuratie van de ASA-interfaces.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ipv6 address 2001:bbbb::1/64
ipv6 enable
```

```
interface GigabitEthernet0/1
nameif inside
security-level 100
ipv6 address 2001:aaaa::1/64
ipv6 enable
```

Stap 2. Stel een IPv6-standaardroute in.

```
ipv6 route outside ::/0 2001:bbbb::2
```

Stap 3. Configureer het IKEv2-beleid en stel IKEv2 in op de externe interface.

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 14
prf sha256
lifetime seconds 86400
```

```
crypto ikev2 enable outside
```

Stap 4. Configureer de tunnelgroep.

```
tunnel-group 2001:cccc::1 type ipsec-l2l
tunnel-group 2001:cccc::1 ipsec-attributes
ikev2 remote-authentication pre-shared-key cisco123
ikev2 local-authentication pre-shared-key cisco123
```

Stap 5. Maak de objecten en de toegangscontrolelijst (ACL) aan elkaar.

```
object-group network local-network
network-object 2001:aaaa::/64
```

```
object-group network remote-network
network-object 2001:dddd::/64
```

```
access-list CRYPTO_ACL extended permit ip object-group local-network object-group remote-network
```

Stap 6. Configuratie van de regels van het Netwerk van het Vertaling van het Adres van het Netwerk (NAT) voor het interessante verkeer.

```
nat (inside,outside) source static local-network local-network destination static remote-network
remote-network no-proxy-arp route-lookup
```

Stap 7. Configureer het IKEv2 IPsec-voorstel.

```
crypto ipsec ikev2 ipsec-proposal ikev2_aes256
protocol esp encryption aes-256
protocol esp integrity sha-1
```

Stap 8. Stel de Crypto Kaart in en pas het op de buiteninterface toe.

```
crypto map VPN 1 match address CRYPTO_ACL
crypto map VPN 1 set peer 2001:cccc::1
crypto map VPN 1 set ikev2 ipsec-proposal ikev2_aes256
crypto map VPN 1 set reverse-route
```

```
crypto map VPN interface outside
```

FTD-configuratie

Deze sectie verschaft instructies om een FTD te configureren met behulp van FMC.

De VPN-topologie definiëren

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

Selecteren 'Voeg VPN toe' en kies 'Firepower Threat Defense Devices', zoals weergegeven in deze afbeelding.

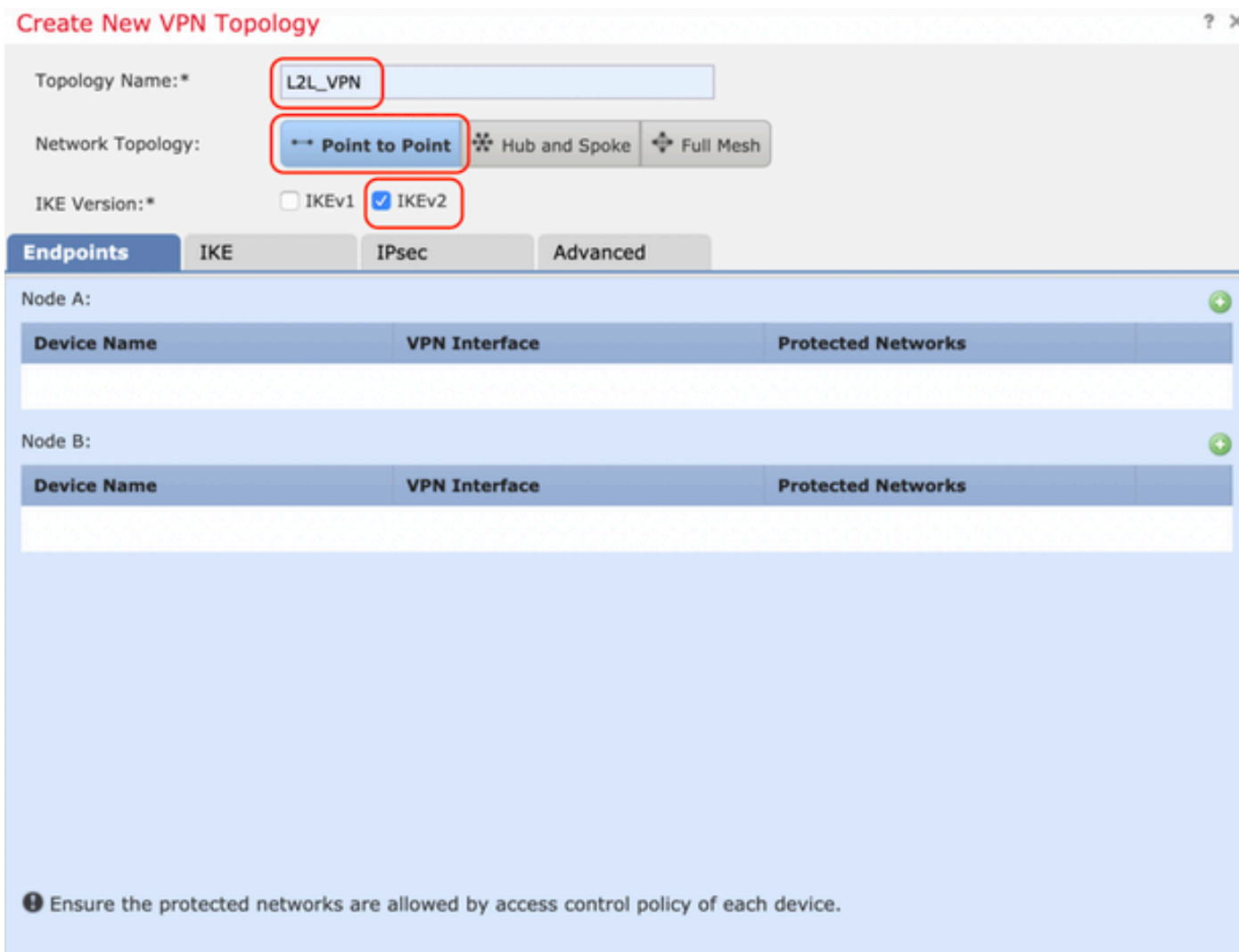


Stap 2. Het vakje 'Nieuwe VPN-topologie maken' verschijnt. Geef VPN een gemakkelijk te herkennen naam.

Netwerktopologie: Punt

IKE versie: IKEv2

In dit voorbeeld is bij het selecteren van endpoints knooppunt A de FTD. Knooppunt B is de ASA. Klik op de knop groen plus om apparaten aan de topologie toe te voegen.



Stap 3. Voeg het FTD toe als eerste eindpunt.

Kies de interface waar de crypto map wordt toegepast. Het IP-adres moet uit de apparaatconfiguratie automatisch worden ingevuld.

Klik op het pictogram green plus onder Protected Networks om subnetten te selecteren die via deze VPN-tunnel zijn versleuteld. In dit voorbeeld bestaat het 'Local Proxy'-netwerkobject op FMC uit IPv6-subgroep '2001:DDD:64'.

Edit Endpoint



Device:*

FTDv

Interface:*

OUTSIDE

IP Address:*

2001:CCCC::1

This IP is Private

Connection Type:

Bidirectional

Certificate Map:

Protected Networks:*

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



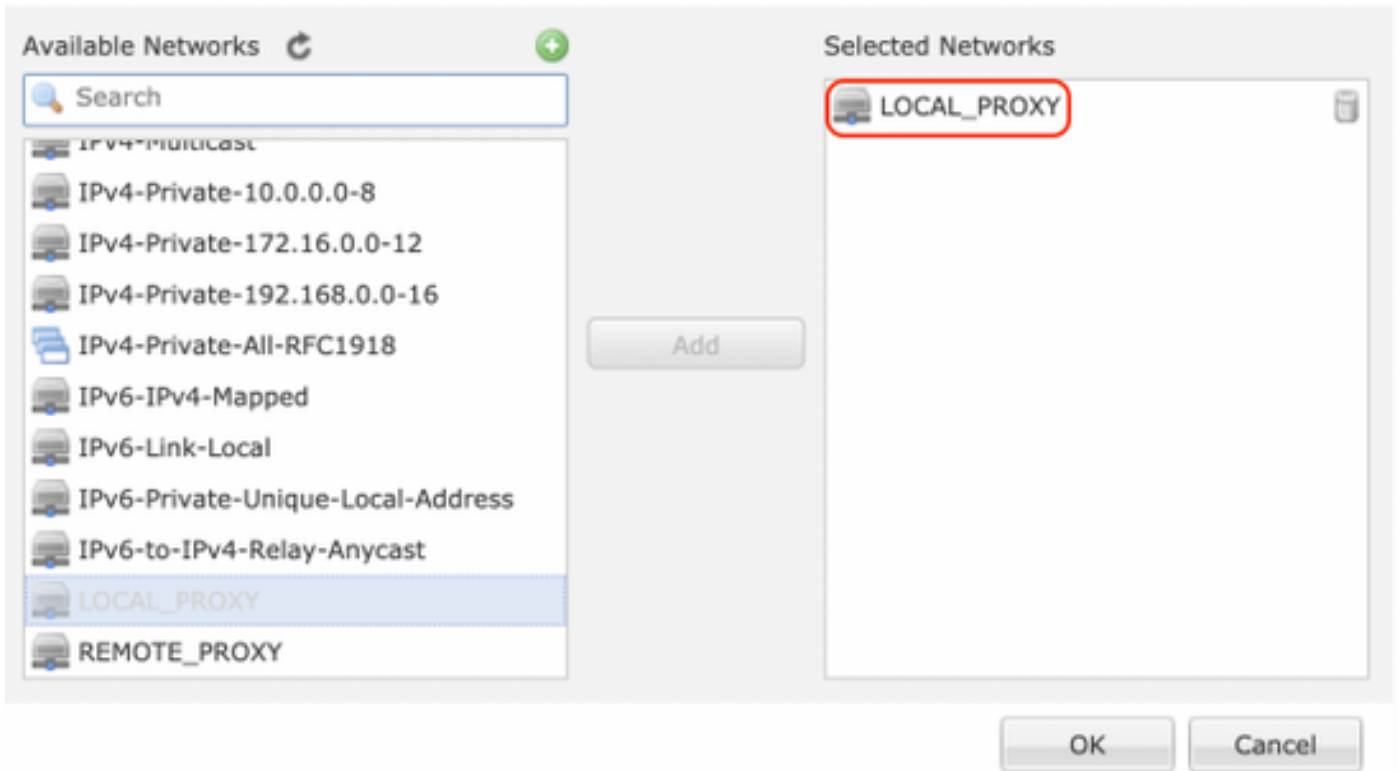
LOCAL_PROXY



OK

Cancel

Network Objects



De bovenstaande stap is de configuratie van het FTD-eindpunt voltooid.

Stap 4. Klik op het pictogram green plus voor knooppunt B, dat een ASA is in het configuratievoorbeeld. Apparaten die niet door het FMC worden beheerd, worden beschouwd als extranet. Voeg een apparatenaam en IP adres toe.

Stap 5. Selecteer het pictogram groene plus om beveiligde netwerken toe te voegen.

Edit Endpoint ? X

Device:*

Device Name:*

IP Address:* Static Dynamic

Certificate Map: +

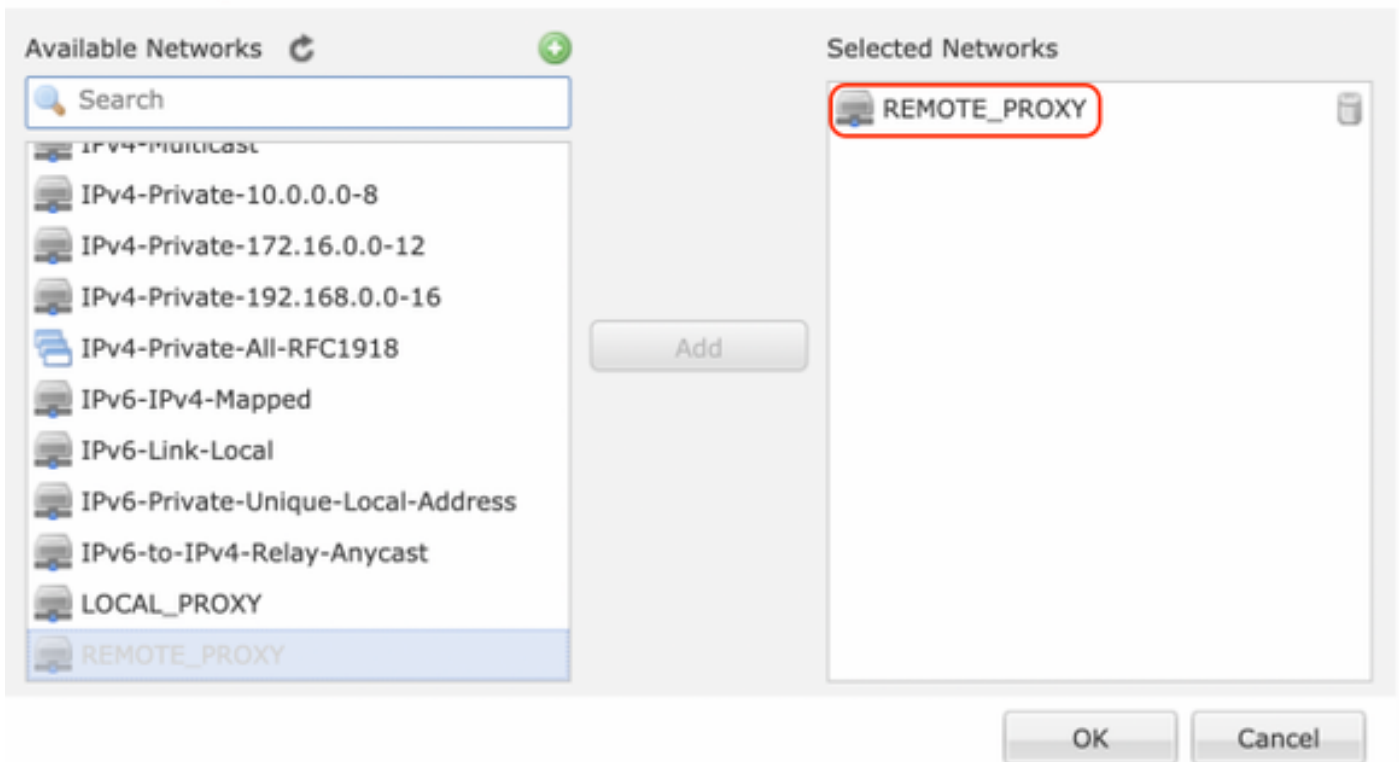
Protected Networks:*
 Subnet / IP Address (Network) Access List (Extended) +

-

Stap 6. Selecteer de ASA-subnetwerken die moeten worden versleuteld en voeg ze toe aan de geselecteerde netwerken.

'Remote Proxy' is het ASA-netwerk '2001:AAA:/64' in dit voorbeeld.

Network Objects



IKE-parameters configureren

Stap 1. Specificeer onder het tabblad IKE de parameters die moeten worden gebruikt voor de eerste IKEv2-uitwisseling. Klik op het pictogram green plus om een nieuw IKE-beleid te creëren.

Edit VPN Topology



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:

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

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

Al het IKE beleid op het apparaat zal naar de verre peer worden verzonden ongeacht wat in het geselecteerde beleidsgedeelte is. De eerste lucifers van de afstandsbediening worden geselecteerd voor de VPN-verbinding.

[Optioneel] Kies welk beleid eerst wordt verzonden met behulp van het prioriteitsveld. Prioriteit 1 wordt eerst verstuurd.

Edit IKEv2 Policy

Name:*

Ikev2_Policy

Description:

Priority:

(1-65535)

Lifetime:

86400

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

Edit 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

Add

Selected Algorithms

- AES-256

Save

Cancel

Edit IKEv2 Policy



Name:*

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)

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

Available Algorithms

- MDS
- SHA
- SHA512
- SHA256
- SHA384

Add

Selected Algorithms

- SHA256

Save

Cancel

Edit IKEv2 Policy



Name:* Ikev2_Policy

Description:

Priority: (1-65535)

Lifetime: 86400 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

Stap 3. Zodra de parameters zijn toegevoegd, selecteert u het hierboven beschreven beleid en kiest u het verificatietype.

Selecteer de optie Vooraf gedeelde handleiding. Voor deze handleiding wordt de vooraf gedeelde sleutel 'cisco123' gebruikt.

Edit VPN Topology



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:

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

IPSEC-parameters configureren

Stap 1. Verplaats naar het tabblad IPsec en maak een nieuw IPsec-voorstel door op het pictogram van het pen te klikken om de transformatieset te bewerken.

Edit VPN Topology



Topology Name:*

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:

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

— **ESPv3 Settings**

Stap 2. Maak een nieuw IKEv2 IPsec-voorstel door het groene plus-pictogram te selecteren en voer de fase 2-parameters in zoals hieronder wordt weergegeven:

ESP-hash: SHA-1

ESP-encryptie : AES-256

Edit IKEv2 IPsec Proposal



Name:*

Ikev2__IPSec_Proposal

Description:

ESP Hash

ESP Encryption

Available Algorithms

- SHA-512
- SHA-384
- SHA-256
- SHA-1
- MD5
- NULL

Selected Algorithms

SHA-1

Add

Save

Cancel

Edit IKEv2 IPsec Proposal



Name:*

Description:

ESP Hash

ESP Encryption

Available Algorithms

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

Add

Selected Algorithms

- AES-256**

Save **Cancel**

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

IKEv2 IPsec Proposal



Available Transform Sets

- AES-GCM
- AES-SHA
- DES_SHA-1
- Ikev2__IPSec_Proposal**

Add

Selected Transform Sets

- Ikev2__IPSec_Proposal**

OK **Cancel**

Stap 4. Het nieuwe geselecteerde IPsec-voorstel is nu opgenomen in de IKEv2 IPsec-voorstellen.

Indien nodig kunnen de fase 2-levensduur en de PFS hier worden bewerkt. Bij dit voorbeeld wordt de levensduur ingesteld als standaard en PFS uitgeschakeld.

Edit VPN Topology ? X

Topology Name:* L2L_VPN

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*

tunnel_aes256_sha Ikev2_IPSec_Proposal

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group: [Dropdown]

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

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

ESPv3 Settings

Save Cancel

U dient de volgende stappen te configureren om toegangscontrole te omzeilen of regels van het toegangsbeleid te maken om VPN-subnetten door FTD toe te staan.

Toegangsbeheer voor omzeilingen

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 vergunning-vpn` wordt toegelaten skip die een toegangscontrolebeleid creëert. Dit configuratievoorbeeld gebruikt de optie "Toegangsbeheer omzeilen".

De parameter `sysopt licentie-vpn` kan worden ingeschakeld onder het kopje Geavanceerd > Tunnel.

Voorzichtig: Met deze optie wordt de mogelijkheid om het toegangscontrolebeleid te gebruiken om 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 mondiaal commando en is van toepassing op alle VPN's als dit selectieteken ingeschakeld is.

Edit VPN Topology



Topology Name:*

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: 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

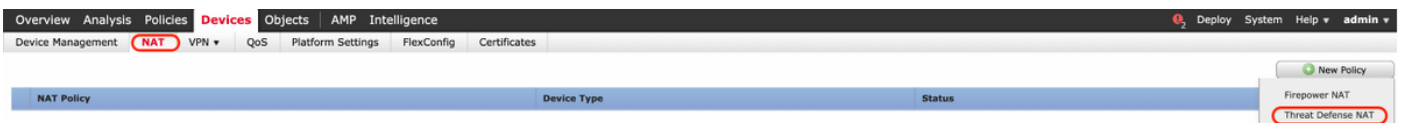
Use the IKE identity to determine the tunnel

Use the peer IP address to determine the tunnel

NAT-vrijstelling configureren

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

Stap 1. Navigatie naar **apparaten > NAT** en cStel een nieuw beleid in door op **Nieuw beleid > Bedreigingsdefensie NAT** te klikken.



New Policy



Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

FTDv

Selected Devices

FTDv

Step 2. Klik op **Add Rule**.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPK QoS Platform Settings FlexConfig Certificates

NAT_Exempt Show Warnings Show Cancel

Policy Assignments (1)

Filter by Device

#	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											
▼ NAT Rules After											

Step 3. Maak een nieuwe statische handleiding voor NAT.

Verwijs de binnen en buiten interfaces voor de NAT regel. Het specificeren van de interfaces op tabblad Interfaceobjecten voorkomt deze regels om verkeer van andere interfaces te beïnvloeden.

Blader naar het tabblad Vertaling en selecteer de bron- en doelsubnetten. Aangezien dit een NAT-vrijstellingsregel is, moet u ervoor zorgen dat de oorspronkelijke bron/bestemming en de vertaalde bron/bestemming dezelfde zijn.

Add NAT Rule



NAT Rule: Insert:

Type: Enable

Description:

Interface Objects: **Translation** PAT Pool Advanced

Original Packet

Original Source:* +

Original Destination: +

Original Source Port: +

Original Destination Port: +

Translated Packet

Translated Source: +

Translated Destination: +

Translated Source Port: +

Translated Destination Port: +

Klik op het tabblad Geavanceerd en selecteer de optie zonder proxy en de optie.

Add NAT Rule



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

Sla deze regel op en bevestig de definitieve NAT-verklaring in de NAT-lijst.

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

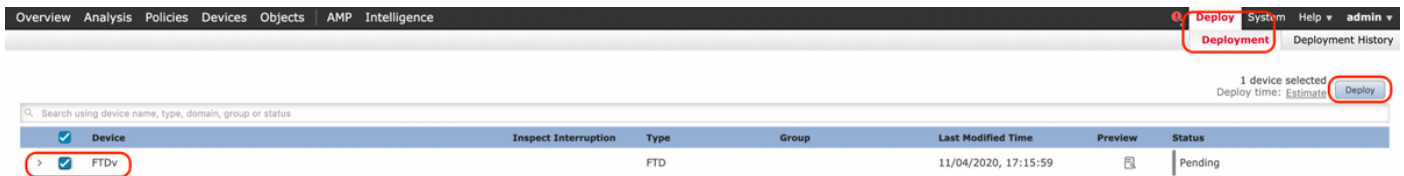
Device Management NAT VPN QoS Platform Settings FlexConfig Certificates Show Warnings Save Cancel

NAT_Exempt
Enter Description Policy Assignments (1)

Rules Filter by Device Add Rule

#	Direction	Type	Original Packet			Translated Packet			Options
			Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	
1		Static	LAN	WAN	LOCAL_PROXY	REMOTE_PROXY	LOCAL_PROXY	REMOTE_PROXY	Dns: false route-lookup no-proxy-arp

Step 4. Nadat de configuratie is voltooid, slaat u de configuratie op en stelt u deze in op de FTD.



Verifiëren

Stel interessant verkeer vanaf de LAN-machine in of u kunt de onderstaande opdracht pakkettracer in de ASA-modus uitvoeren.

```
packet-tracer input inside icmp 2001:aaaa::23 128 0 2001:dddd::33 detail
```

Opmerking: Hier type = 128 en Code=0 staat voor ICMPv6 "Echo-aanvraag".

In de onderstaande sectie worden de opdrachten beschreven die u op ASA v of FTD LINA CLI kunt uitvoeren om de status van de IKEv2-tunnel te controleren.

Dit is een voorbeeld van een output van de ASA:

```
ciscoasa# show crypto ikev2 sa
```

```
IKEv2 SAs:
```

```
Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local                               Remote
           Status                               Role
6638313 2001:bbbb::1/500                       2001:cccc::1/500
           READY                               INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/224 sec
Child sa: local selector 2001:aaaa::/0 - 2001:aaaa::ffff:ffff:ffff:ffff/65535
           remote selector 2001:dddd::/0 - 2001:dddd::ffff:ffff:ffff:ffff/65535
           ESP spi in/out: 0xa0fd3fe6/0xd95ecdb8
```

```
ciscoasa# show crypto ipsec sa detail
```

```
interface: outside
```

```
  Crypto map tag: VPN, seq num: 1, local addr: 2001:bbbb::1
```

```
access-list CRYPTO_ACL extended permit ip 2001:aaaa::/64 2001:dddd::/64
local ident (addr/mask/prot/port): (2001:aaaa::/64/0/0)
remote ident (addr/mask/prot/port): (2001:dddd::/64/0/0)
current_peer: 2001:cccc::1
```

```
#pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 11
#pkts decaps: 11, #pkts decrypt: 11, #pkts verify: 11
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #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
#pkts no sa (send): 0, #pkts invalid sa (rcv): 0
#pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
#pkts invalid prot (rcv): 0, #pkts verify failed: 0
#pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
```

#pkts invalid pad (rcv): 0,
#pkts invalid ip version (rcv): 0,
#pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
#pkts replay failed (rcv): 0
#pkts min mtu frag failed (send): 0, #pkts bad frag offset (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv): 0

local crypto endpt.: 2001:bbbb::1/500, remote crypto endpt.: 2001:cccc::1/500
path mtu 1500, ipsec overhead 94(64), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: D95ECDB8
current inbound spi : A0FD3FE6

inbound esp sas:

spi: 0xA0FD3FE6 (2700951526)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings =(L2L, Tunnel, IKEv2,)
slot: 0, conn_id: 1937408, crypto-map: VP
sa timing: remaining key lifetime (kB/sec): (4055040/28535)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

outbound esp sas:

spi: 0xD95ECDB8 (3646868920)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings =(L2L, Tunnel, IKEv2,)
slot: 0, conn_id: 1937408, crypto-map: VPN
sa timing: remaining key lifetime (kB/sec): (4193280/28535)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

ciscoasa# **show vpn-sessiondb detail l2l filter name 2001:cccc::1**

Session Type: LAN-to-LAN Detailed

Connection : 2001:cccc::1
Index : 473 IP Addr : 2001:cccc::1
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA256 IPsec: (1)SHA1
Bytes Tx : 352 Bytes Rx : 352
Login Time : 12:27:36 UTC Sun Apr 12 2020
Duration : 0h:06m:40s

IKEv2 Tunnels: 1

IPsec Tunnels: 1

IKEv2:

Tunnel ID : 473.1
UDP Src Port : 500 UDP Dst Port : 500
Rem Auth Mode: preSharedKeys
Loc Auth Mode: preSharedKeys
Encryption : AES256 Hashing : SHA256
Rekey Int (T): 86400 Seconds Rekey Left(T): 86000 Seconds
PRF : SHA256 D/H Group : 14
Filter Name :

IPsec:

Tunnel ID : 473.2

Local Addr	: 2001:aaaa::/64/0/0		
Remote Addr	: 2001:dddd::/64/0/0		
Encryption	: AES256	Hashing	: SHA1
Encapsulation:	Tunnel		
Rekey Int (T)	: 28800 Seconds	Rekey Left (T)	: 28400 Seconds
Rekey Int (D)	: 4608000 K-Bytes	Rekey Left (D)	: 4608000 K-Bytes
Idle Time Out:	: 30 Minutes	Idle TO Left	: 23 Minutes
Bytes Tx	: 352	Bytes Rx	: 352
Pkts Tx	: 11	Pkts Rx	: 11

Problemen oplossen

Om IKEv2-tunnelproblemen op ASA en FTD op te lossen moet u de volgende debug-opdrachten uitvoeren:

```
debug van crypto-conditie door peer <peer IP>  
debug van crypto ikev2 - protocol 25  
debug van crypto ikev2 - platform 25
```

Hier zie je een voorbeeld van IKEv2-debuggs ter referentie:

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debuggs.html>

Referenties

<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/119425-configure-ipsec-00.html>

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/81824-common-ipsec-trouble.html>

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/vpn/asa-95-vpn-config/vpn-site2site.html>