

Routegebaseerde site-to-site VPN tussen ASA en FTD met BGP configureren als overlay

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[IPsec VPN op FTD configureren met FMC](#)

[Loopback-interface op FTD configureren met behulp van FMC](#)

[IPsec VPN configureren op ASA](#)

[Configureer de Loopback-interface op ASA](#)

[Overlay BGP op FTD configureren met behulp van FMC](#)

[Overlay BGP op ASA configureren](#)

[Verifiëren](#)

[Outputs op FTD](#)

[Uitgangen op ASA](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u een route-gebaseerde Site-to-Site VPN-tunnel kunt configureren tussen adaptieve security applicatie (ASA) en Firepower Threat Defence (FTD) die wordt beheerd door een Firepower Management Center (FMC) met BGP-protocol (Dynamic Routing Gateway Protocol) als overlay.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van IPsec site-to-site VPN
- BGP-configuraties op FTD en ASA
- Ervaring met het VCC

Gebruikte componenten

- Cisco ASA versie 9.20(2)E2
- Cisco FMC versie 7.4.1
- Cisco FTD versie 7.4.1

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

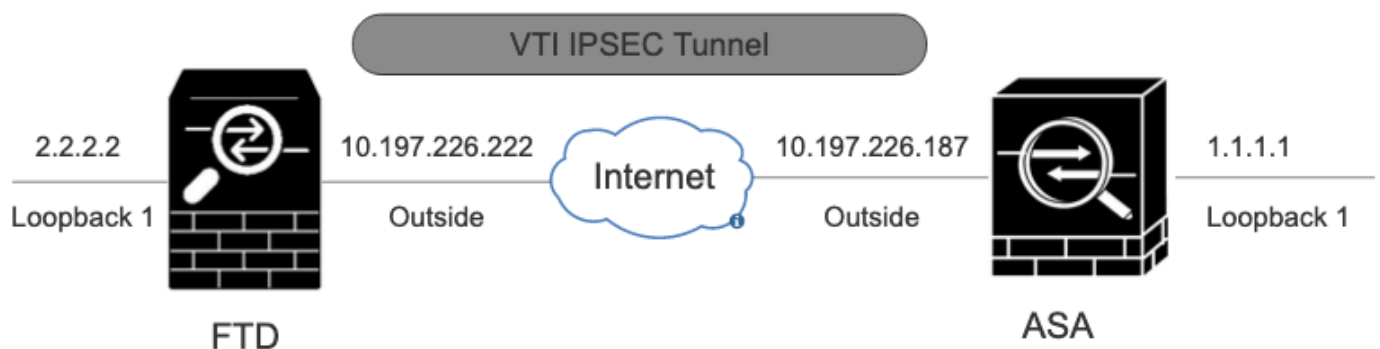
Op route gebaseerde VPN maakt het mogelijk om de vaststelling van interessant verkeer te versleutelen of via een VPN-tunnel te verzenden en gebruikt routing van verkeer in plaats van beleid/toeganglijst zoals in een op beleid gebaseerde of op Crypto-kaarten gebaseerde VPN. Het coderingsdomein is ingesteld om verkeer toe te staan dat de IPsec-tunnel binnenkomt. IPsec Local en Remote Traffic Selectors zijn ingesteld op 0.0.0.0/0.0.0.0. Om het even welk verkeer dat in de IPsec-tunnel wordt gerouteerd wordt versleuteld ongeacht het bron/doelsubnetje.

Dit document concentreert zich op Statische Virtual Tunnel Interface (SVTI) configuratie met dynamische routing BGP als overlay.

Configureren

In dit gedeelte worden de configuratie beschreven die op de ASA en FTD nodig is om BGP-naberschap te realiseren via een SVTI IPsec-tunnel.

Netwerkdigram



Netwerkdigram

Configuraties

IPsec VPN op FTD configureren met FMC

Stap 1. Navigeer naar [Devices > VPN > Site To Site](#) .

Stap 2. Klik op +Site to Site VPN .



Site-to-site VPN

Stap 3. Verstrek een bestand Topology Name en selecteer het type VPN zoals Route Based (VTI). Kies de IKE Version.

Voor deze demonstratie:

Naam topologie: ASAv-VTI

IKE versie: IKEv2

A screenshot of a web interface titled 'Edit VPN Topology'. It contains the following fields and options:

- Topology Name:*** A text input field containing 'ASAv-VTI'.
- VPN Type:** Two radio buttons: 'Policy Based (Crypto Map)' (unselected) and 'Route Based (VTI)' (selected).
- Network Topology:** Three buttons: 'Point to Point' (selected), 'Hub and Spoke', and 'Full Mesh'.
- IKE Version:*** Two checkboxes: 'IKEv1' (unselected) and 'IKEv2' (selected).

VPN-topologie

Stap 4. Kies Device waarop de tunnel moet worden geconfigureerd. U kunt een nieuwe Virtual Tunnel Interface toevoegen (klik op het + pictogram) of er een selecteren uit de bestaande lijst.

Node A

Device:*

Virtual Tunnel Interface:*



Tunnel Source IP is Private [Edit VTI](#)

Send Local Identity to Peers

[+ Add Backup VTI \(optional\)](#)

▶ Advanced Settings

Endpoint Node A

Stap 5. Definieer de parameters van de New Virtual Tunnel Interface. Klik op de knop .Ok

Voor deze demonstratie:

Naam: ASA-VTI

Beschrijving (optioneel): VTI Tunnel met Extranet ASA

Security Zone: VTI-Zone

Tunnel-id: 1

IP-adres: 169.254.2.1/24

Tunnelbron: Gigabit Ethernet0/1 (buiten)

IPsec-tunnelmodus: IPv4

Add Virtual Tunnel Interface



General

Path Monitoring

Tunnel Type

- Static Dynamic

Name:*

ASAv-VTI

Enabled

Description:

VTI Tunnel with Extranet ASA

Security Zone:

VTI-Zone

Priority:

0

(0 - 65535)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VT.

Tunnel ID:*

3

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/1 (Outside)

10.197.226.222

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

- IPv4 IPv6

IP Address:*

Configure IP

169.254.2.1/24

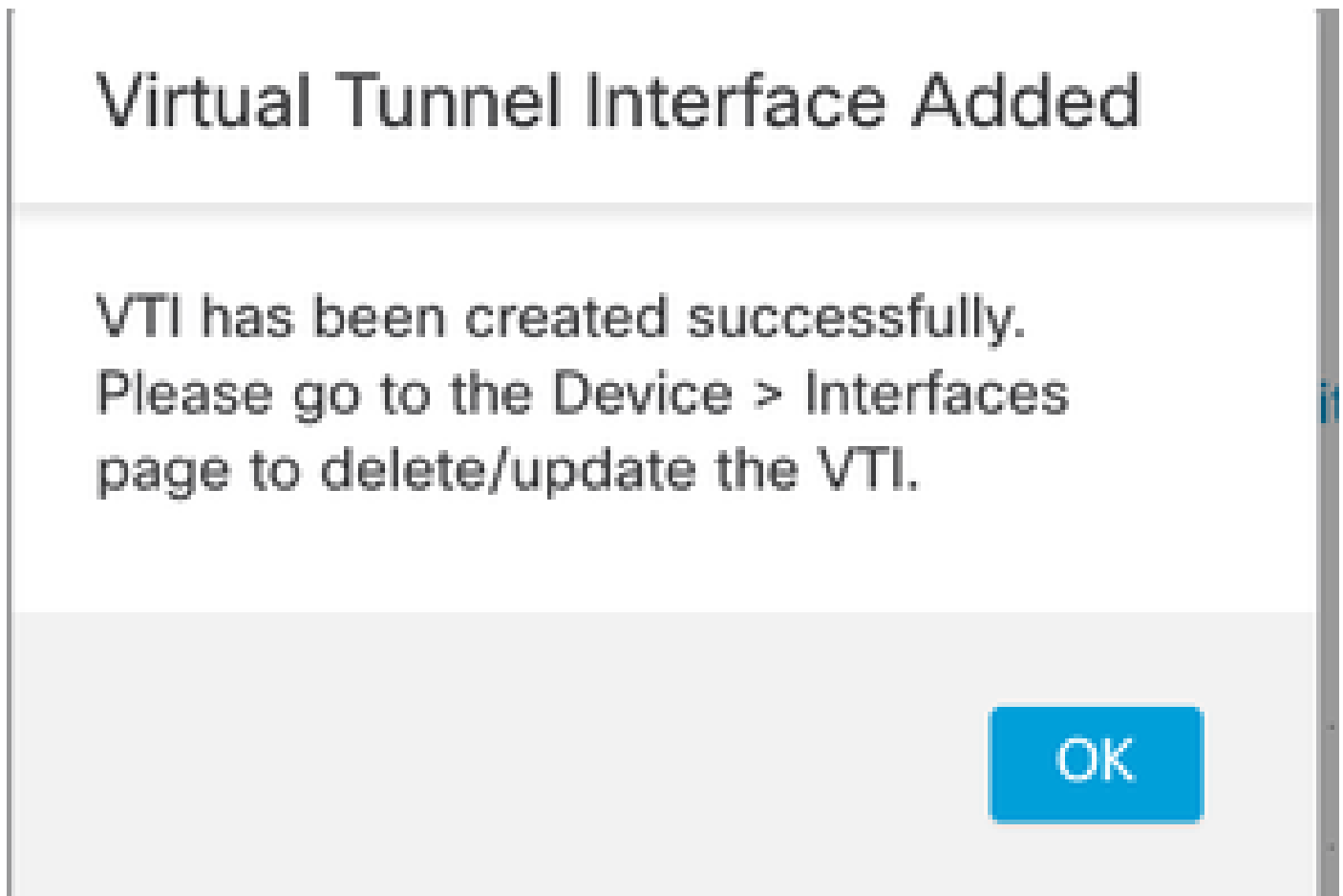
Borrow IP (IP unnumbered)

Loopback1 (loopback)

Cancel

OK

Stap 6. Klik OK op de pop-up om te vermelden dat het nieuwe VTI is gemaakt.



Toegevoegd aan virtuele tunnelinterface

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

Voor deze demonstratie:

Apparaat: Extranet

Apparaatnaam: ASAv-peer

Endpoint IP-adres: 10.197.226.187

Node A

Device:*
FTD

Virtual Tunnel Interface:*
ASAv-VTI (IP: 169.254.2.1)

Tunnel Source: Outside (IP: 10.197.226.222) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

[+ Add Backup VTI \(optional\)](#)

Additional Configuration ⓘ

Route traffic to the VTI : [Routing Policy](#)

Permit VPN traffic : [AC Policy](#)

Node B

Device:*
Extranet

Device Name*:
ASAv-Peer

Endpoint IP Address*:
10.197.226.187

Endpoint Node B



Stap 8. Navigeer naar het tabblad **IKE**. Klik op

. U kunt ervoor kiezen een vooraf gedefinieerde Policy te gebruiken of op de +knop naast het Policytabblad te klikken om een nieuwe knop te maken.

Stap 9. (Optioneel, als u een nieuw IKEv2-beleid maakt.) Verstrek een Name voor het Beleid en selecteer Algorithmste gebruiken in het beleid. Klik op de knop .Save

Voor deze demonstratie:

Naam: ASAv-IKEv2-policy

Integriteitsalgoritmen: SHA-256

Encryptiealgoritmen: AES-256

PRF-algoritmen: SHA-256

Diffie-Hellman groep: 14

Edit IKEv2 Policy



Name:*

ASAv-IKEv2-Policy


Description:

Priority: (1-65535)

1

Lifetime: seconds (120-2147483647)

86400

Integrity Algorithms	Available Algorithms	Add	Selected Algorithms
Encryption Algorithms PRF Algorithms Diffie-Hellman Group	MD5 SHA SHA512 SHA256 SHA384 NULL		SHA256 

Cancel

Save

IKEv2-beleid

Stap 10. Kies de nieuwe Policy of de bestaande Policyoptie. Selecteer het Authentication Type. Als een Pre-gedeelde Handmatige Sleutel wordt gebruikt, ga de sleutel in het Keyen Confirm Key vakje in.

Voor deze demonstratie:

Beleid: ASAv-IKEv2-Policy

Verificatietype: Vooraf gedeelde handmatige sleutel

IKEv2 Settings

Policies:*

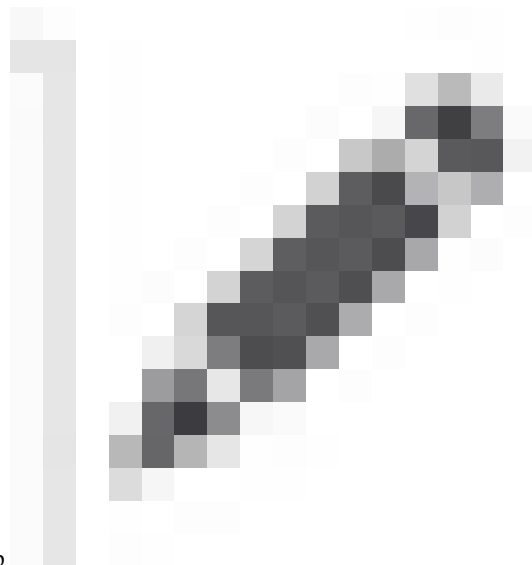
Authentication Type:


Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Verificatie



Stap 11. Navigeer naar het IPsec tabblad. Klik op  om een vooraf gedefinieerd IKEv2 IPsec-voorstel te gebruiken of een nieuw voorstel te maken. Klik op de +knop naast het IKEv2 IPsec Proposal tabblad.

Stap 12. (Optioneel, als u een nieuw IKEv2 IPsec-voorstel maakt.) Voer een Name voor het voorstel in en selecteer de in het Algorithms voorstel te gebruiken elementen. Klik op de knop .Save

Voor deze demonstratie:

Naam: ASAv-IPSec-Policy

ESP-hash: SHA-256

ESP-encryptie: AES-256

New IKEv2 IPsec Proposal



Name:*

ASAv-IPSec-Policy

Description:

ESP Hash

ESP Encryption

Available Algorithms

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

Add

Selected Algorithms

- SHA-256

Cancel

Save

IKEv2-IPsec-voorstel

Stap 13. Kies de nieuwe Proposal of Proposalbestaande uit de lijst met voorstellen die beschikbaar zijn. Klik op de knop .OK

IKEv2 IPsec Proposal



Available Transform Sets ⌂ +

AES-256-SHA-256

AES-GCM

AES-SHA

ASAv-IPSec-Policy

DES_SHA-1

Umbrella-AES-GCM-256

Add

Selected Transform Sets

ASAv-IPSec-Policy

Cancel

OK

Omzettingsset

Stap 14. (Optioneel) Kies de Perfect Forward Secrecy instellingen. Configureer de IPsec-Lifetime Duration and Lifetime Size.

Voor deze demonstratie:

Perfect Forward Secrecy: Modulus Groep 14

Levensduur: 28800 (standaard)

Levensduur Grootte: 4608000 (standaard)

Endpoints **IKE** IPsec Advanced

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

tunnel_aes256_sha

ASAv-IPSec-Policy

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 15. Controleer de ingestelde instellingen. Klik op Save, zoals in deze afbeelding.

Edit VPN Topology

Topology Name: ASAv-VTI

Policy Based (Crypto Map) Route Based (VTI)

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

IKE Version: IKEv1 IKEv2

Endpoints | **IKE** | IPsec | Advanced

Node A

Device: FTD

Virtual Tunnel Interface: ASAv-VTI (IP: 169.254.3.1) +

Tunnel Source: Outside (IP: 10.197.226.222) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

[+ Add Backup VTI \(optional\)](#)

Additional Configuration ⓘ

Route traffic to the VTI : [Routing Policy](#)

Permit VPN traffic : [ACL Policy](#)

Node B

Device: Extranet

Device Name: ASAv-Peer

Endpoint IP Address: 10.197.226.187

[Cancel](#) [Save](#)

De configuratie opslaan

Lopback-interface op FTD configureren met behulp van FMC

Navigeer naar Devices > Device Management . Bewerk het apparaat waar de loopback moet worden geconfigureerd.

Stap 1. Ga naar Interfaces > Add Interfaces > Loopback Interface .

Device | Routing | **Interfaces** | Inline Sets | DHCP | VTEP

All Interfaces | Virtual Tunnels

Search by name | Sync Device

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0	Inside	Physical	Inside		10.197.224.227(2)(Static)	Disabled	Global

Add Interfaces +
Redundant Interface
Bridge Group Interface
Loopback Interface

Navigeren naar Loopback-interface

Stap 2. Voer de naam "loopback" in, geef een loopback-id "1" en schakel de interface in.

Edit Loopback Interface



General

IPv4

IPv6

Name:

loopback

Enabled

Loopback ID:*

1

(1-1024)

Description

Cancel

OK

Loopback-interface inschakelen

Stap 3. Configureer het IP-adres voor de interface en klik OK .

Edit Loopback Interface



General

IPv4

IPv6

IP Type:

Use Static IP

IP Address:

2.2.2.2/24

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel

OK

IP-adres aan loopback-interface bieden

IPsec VPN configureren op ASA

!--- Configure IKEv2 Policy ---!

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

!--- Enable IKEv2 on the outside interface ---!

```
crypto ikev2 enable outside
```

!---Configure Tunnel-Group with pre-shared-key---!

```
tunnel-group 10.197.226.222 type ipsec-l2l
tunnel-group 10.197.226.222 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

!--- Configure IPsec Policy ---!

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

!--- Configure IPsec Profile ---!

```
crypto ipsec profile ipsec_profile_for_FTD
set ikev2 ipsec-proposal FTD-ipsec-proposal
set pfs group14
```

!--- Configure VTI ---!

```
interface Tunnel1
nameif FTD-VTI
ip address 169.254.2.2 255.255.255.0
tunnel source interface outside
tunnel destination 10.197.226.222
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec_profile_for_FTD
```

!--- Configure the WAN routes ---!

```
route outside 0.0.0.0 0.0.0.0 10.197.226.1 1
```

Configureer de Loopback-interface op ASA

```
interface Loopback1
nameif loopback
ip address 1.1.1.1 255.255.255.0
```

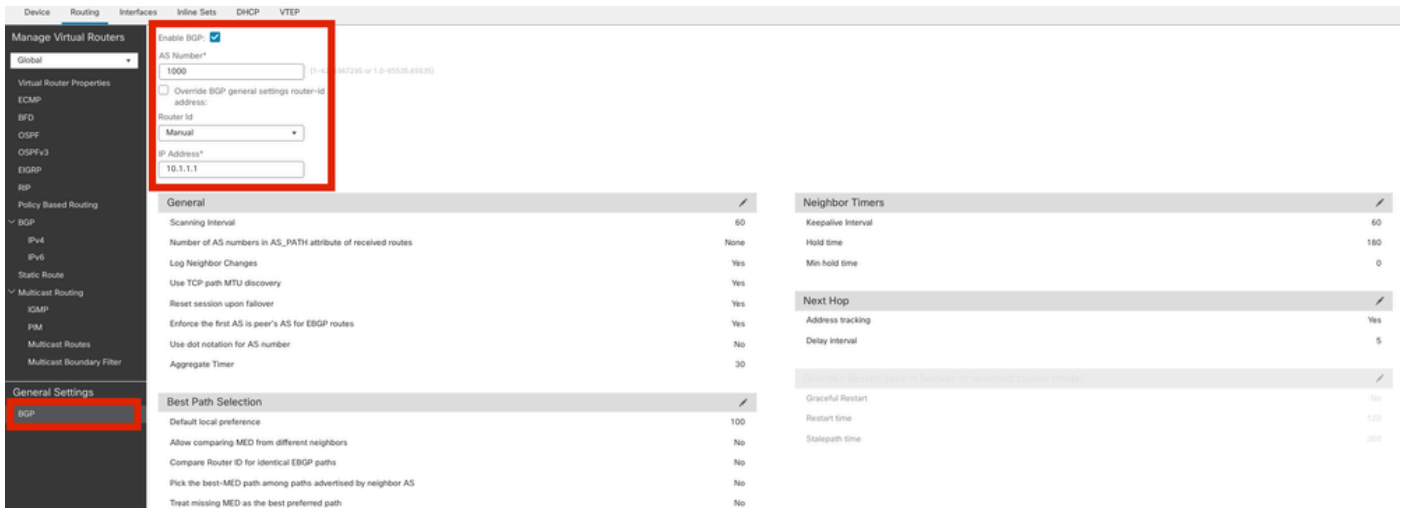
Overlay BGP op FTD configureren met behulp van FMC

Navigeer naar Devices > Device Management. Edit het apparaat waar de VTI-tunnel is geconfigureerd en navigeer dan naar Routing > General Settings > BGP.

Stap 1. Schakel BGP in en configureer het Autonomous System (AS) nummer en router-id, zoals in deze afbeelding.

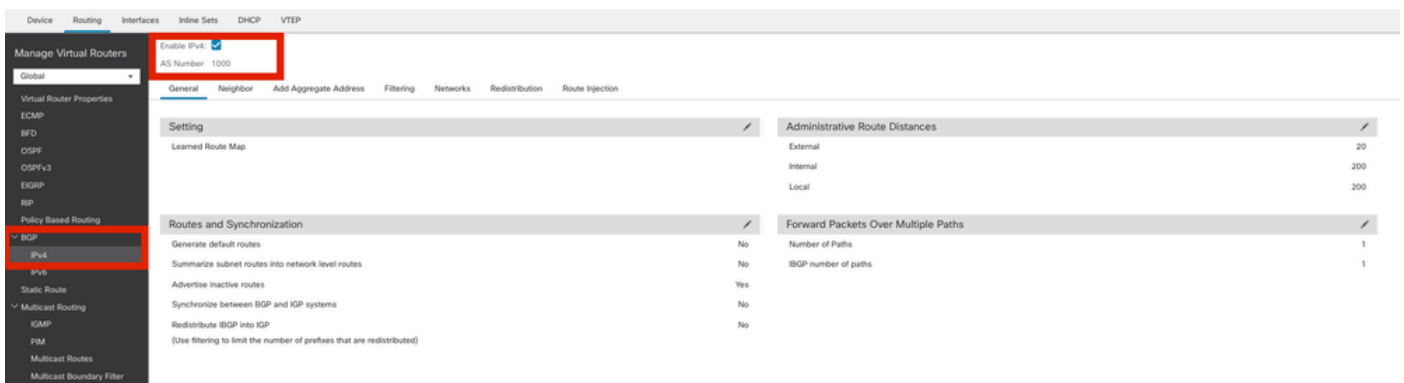
Het AS-nummer moet hetzelfde zijn op zowel de FTD-apparaten als de ASA.

De router-ID wordt gebruikt om elke router te identificeren die aan BGP deelneemt.



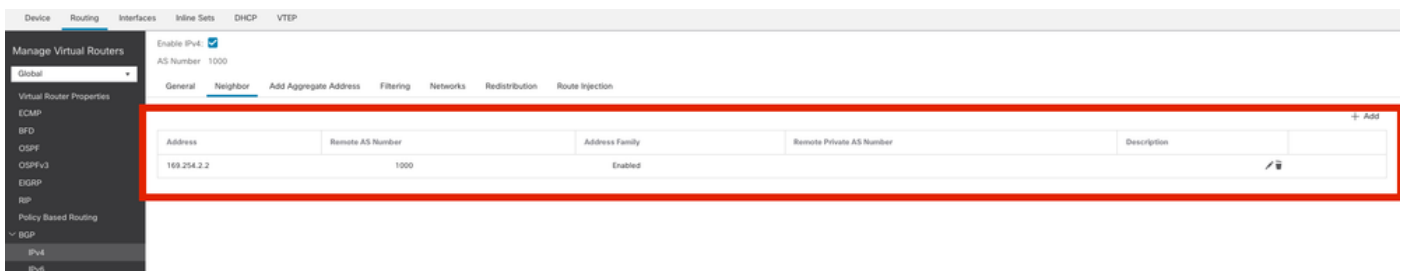
Navigeren om BGP te configureren

Stap 2. Navigeer naar BGP > IPv4 BGP IPv4 op de FTD en schakel deze in.



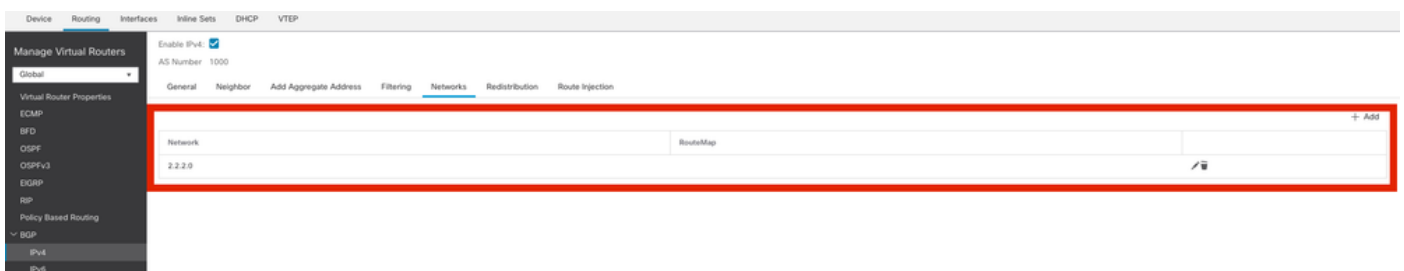
BGP inschakelen

Stap 3. Voeg onder het Neighbor tabblad het ASAv VTI-tunnelip-adres toe als buur en schakel de buur in.



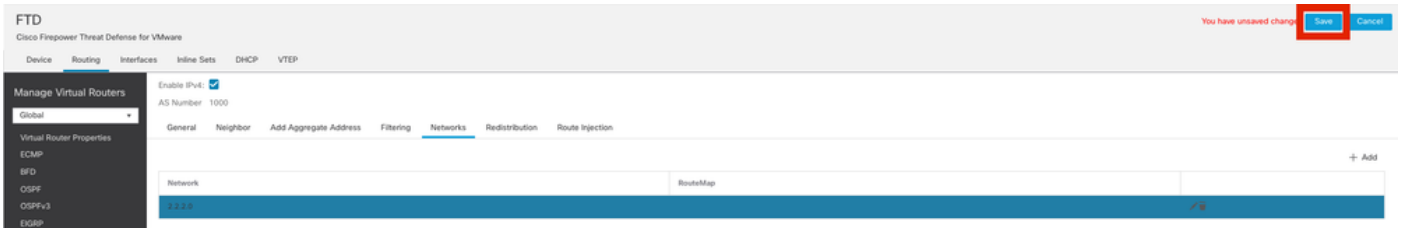
BGP-buur toevoegen

Stap 4. Onder Networks, voeg de netwerken toe u door BGP wilt adverteren die door de tunnel VTI moeten gaan, in dit geval, loopback1.



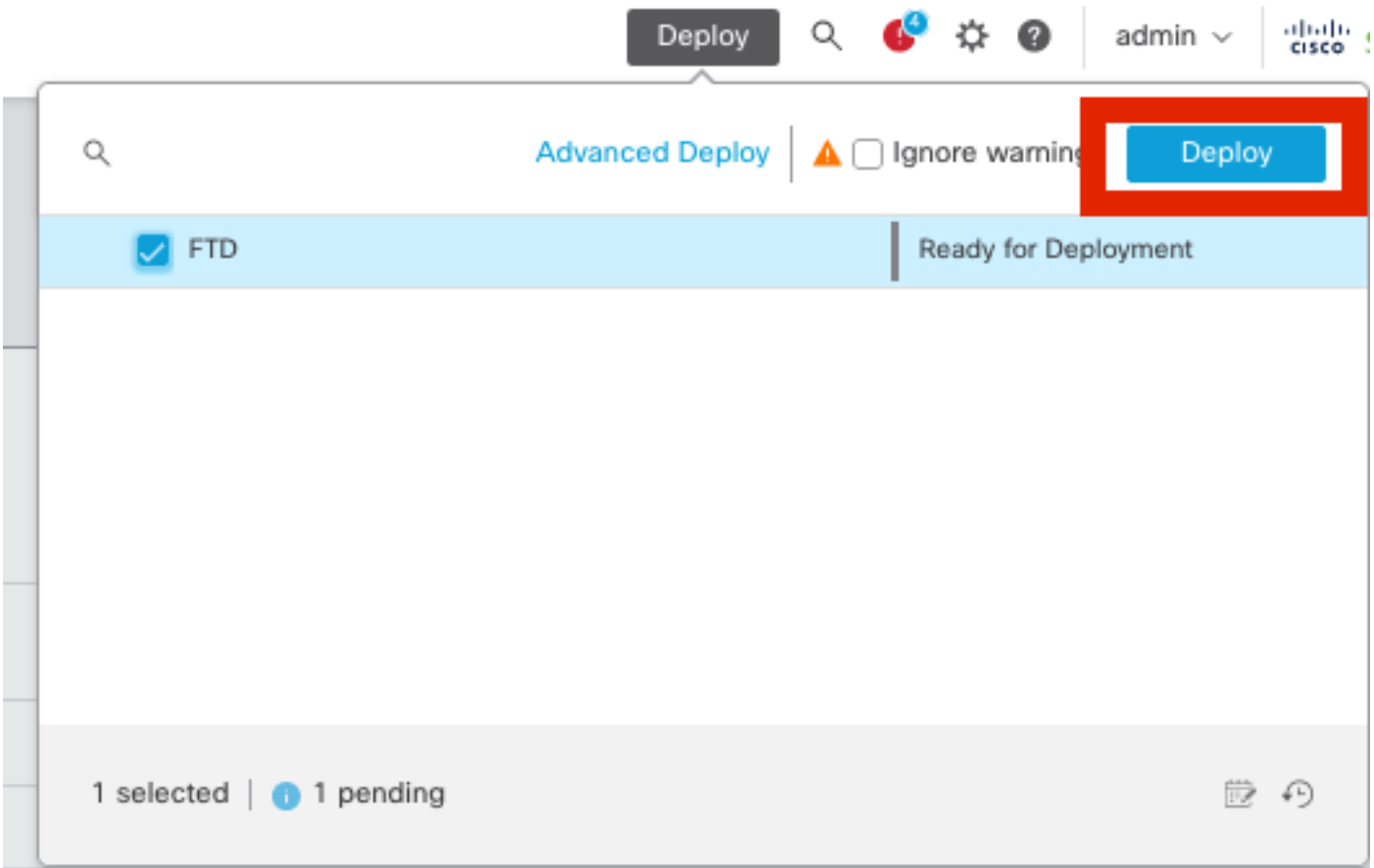
BGP-netwerken toevoegen

Stap 5. Alle andere BGP-instellingen zijn optioneel en u kunt deze instellen volgens uw omgeving. Controleer de configuratie en klik op Save.



BGP-configuratie opslaan

Stap 6. Stel alle configuraties in.



Implementatie

Overlay BGP op ASA configureren

```
router bgp 1000
  bgp log-neighbor-changes
  bgp router-id 10.1.1.2
  address-family ipv4 unicast
  neighbor 169.254.2.1 remote-as 1000
  neighbor 169.254.2.1 transport path-mtu-discovery disable
  neighbor 169.254.2.1 activate
  network 1.1.1.0 mask 255.255.255.0
  no auto-summary
  no synchronization
  exit-address-family
```

Verifiëren

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

Outputs op FTD

<#root>

```
#show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:20, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote	fvr/f/ivrf	Status	Role
666846307	10.197.226.222/500	10.197.226.187/500	Global/Global	READY	RESPONDER

Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/1201 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
 remote selector 0.0.0.0/0 - 255.255.255.255/65535
 ESP spi in/out: 0xa14edaf6/0x8540d49e

```
#show crypto ipsec sa
```

interface: ASAv-VTI

Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 10.197.226.222

Protected vrf (ivrf): Global

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: 10.197.226.187

#pkts encaps: 45, #pkts encrypt: 45, #pkts digest: 45

#pkts decaps: 44, #pkts decrypt: 44, #pkts verify: 44

#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

#send errors: 0, #recv errors: 0

local crypto endpt.: 10.197.226.222/500, remote crypto endpt.: 10.197.226.187/500
path mtu 1500, ipsec overhead 78(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 8540D49E
current inbound spi : A14EDAF6

inbound esp sas:

spi: 0xA14EDAF6 (2706299638)
SA State: active
transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={L2L, Tunnel, PFS Group 14, IKEv2, VTI, }
slot: 0, conn_id: 49, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4331517/27595)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
000001FFF 0xFFFFFFFF

outbound esp sas:

spi: 0x8540D49E (2235618462)
SA State: active
transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={L2L, Tunnel, PFS Group 14, IKEv2, VTI, }
slot: 0, conn_id: 49, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4101117/27595)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

#show bgp summary

BGP router identifier 10.1.1.1, local AS number 1000
BGP table version is 5, main routing table version 5
2 network entries using 400 bytes of memory
2 path entries using 160 bytes of memory
2/2 BGP path/bestpath attribute entries using 416 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 976 total bytes of memory
BGP activity 21/19 prefixes, 24/22 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down
169.254.2.2	4	1000	22	22	5		0	0

#show bgp neighbors

```

BGP neighbor is 169.254.2.2, vrf single_vf, remote AS 1000, internal link
  BGP version 4, remote router ID 10.1.1.2
  BGP state = Established, up for 00:19:49
  Last read 00:01:04, last write 00:00:38, hold time is 180, keepalive interval is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Multisession Capability:
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

```

	Sent	Rcvd
Opens	1	1
Notifications:	0	0
Updates:	2	2
Keepalives:	19	19
Route Refresh: 0	0	
Total:	22	22

Default minimum time between advertisement runs is 0 seconds

```

For address family: IPv4 Unicast
  Session: 169.254.2.2
  BGP table version 5, neighbor version 5/0
  Output queue size : 0
  Index 15
  15 update-group member

```

	Sent	Rcvd	
Prefix activity:	----	----	
Prefixes Current:	1	1	(Consumes 80 bytes)
Prefixes Total:	1	1	
Implicit Withdraw:	0	0	
Explicit Withdraw:	0	0	
Used as bestpath:	n/a	1	
Used as multipath:	n/a	0	

	Outbound	Inbound
Local Policy Denied Prefixes:	-----	-----
Bestpath from this peer:	1	n/a
Invalid Path:	1	n/a
Total:	2	0

Number of NLRIs in the update sent: max 1, min 0

```

Address tracking is enabled, the RIB does have a route to 169.254.2.2
Connections established 7; dropped 6
Last reset 00:20:06, due to Peer closed the session of session 1
Transport(tcp) path-mtu-discovery is disabled
Graceful-Restart is disabled

```

```
#show route bgp
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is 10.197.226.1 to network 0.0.0.0

B 1.1.1.0 255.255.255.0 [200/0] via 169.254.2.2, 00:19:55

Uitgangen op ASA

<#root>

#show crypto ikev2 sa

IKEV2 SAs:

Session-id:7, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote	fvr/ivrf	Status
442126361	10.197.226.187/500	10.197.226.222/500	Global/Global	READY

Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/1200 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0x8540d49e/0xa14edaf6

#show crypto ipsec sa

interface: FTD-VTI

Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 10.197.226.187

Protected vrf (ivrf): Global

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: 10.197.226.222

#pkts encaps: 44 #pkts encrypt: 44, #pkts digest: 44
#pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45
#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
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.197.226.187/500, remote crypto endpt.: 10.197.226.222/500
path mtu 1500, ipsec overhead 78(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: A14EDAF6
current inbound spi : 8540D49E

inbound esp sas:

spi: 0x8540D49E (2235618462)
SA State: active
transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={L2L, Tunnel, PFS Group 14, IKEv2, VTI, }
slot: 0, conn_id: 9, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4147198/27594)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x007FFFFF

outbound esp sas:

spi: 0xA14EDAF6 (2706299638)
SA State: active
transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={L2L, Tunnel, PFS Group 14, IKEv2, VTI, }
slot: 0, conn_id: 9, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (3916798/27594)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

#show bgp summary

BGP router identifier 10.1.1.2, local AS number 1000
BGP table version is 7, main routing table version 7
2 network entries using 400 bytes of memory
2 path entries using 160 bytes of memory
2/2 BGP path/bestpath attribute entries using 416 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 976 total bytes of memory

BGP activity 5/3 prefixes, 7/5 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/Pf
169.254.2.1	4	1000	22	22	7	0	0	00:19:42	1

#show bgp neighbors

BGP neighbor is 169.254.2.1, context single_vf, remote AS 1000, internal link
BGP version 4, remote router ID 10.1.1.1
BGP state = Established, up for 00:19:42
Last read 00:01:04, last write 00:00:38, hold time is 180, keepalive interval is 60 seconds
Neighbor sessions:
1 active, is not multisession capable (disabled)
Neighbor capabilities:
Route refresh: advertised and received(new)
Four-octets ASN Capability: advertised and received
Address family IPv4 Unicast: advertised and received
Multisession Capability:
Message statistics:
InQ depth is 0
OutQ depth is 0

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	2	2
Keepalives:	19	19
Route Refresh:	0	0
Total:	22	22

Default minimum time between advertisement runs is 0 seconds
For address family: IPv4 Unicast
Session: 169.254.2.1
BGP table version 7, neighbor version 7/0
Output queue size : 0

Index 5

5 update-group member

	Sent	Rcvd
Prefix activity:	----	----
Prefixes Current:	1	1 (Consumes 80 bytes)
Prefixes Total:	1	1
Implicit Withdraw:	0	0
Explicit Withdraw:	0	0
Used as bestpath:	n/a	1
Used as multipath:	n/a	0

	Outbound	Inbound
Local Policy Denied Prefixes:	-----	-----
Bestpath from this peer:	1	n/a
Invalid Path:	1	n/a
Total:	2	0

Number of NLRI in the update sent: max 1, min 0

Address tracking is enabled, the RIB does have a route to 169.254.2.1
Connections established 5; dropped 4

Last reset 00:20:06, due to Peer closed the session of session 1
Transport(tcp) path-mtu-discovery is disabled
Graceful-Restart is disabled

`#show route bgp`

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is 10.197.226.1 to network 0.0.0.0

B 2.2.2.0 255.255.255.0 [200/0] via 169.254.2.1, 00:19:55

Problemen oplossen

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

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug ip bgp all
```

- Ondersteunt alleen IPv4 interfaces, evenals IPv4, beschermde netwerken of VPN-payload (geen ondersteuning voor IPv6).

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.