

BGP over routegebaseerde VPN op FTD beheerde switch met FDM

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties op VPN](#)

[Configuraties op BGP](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft het configureren van BGP via route-gebaseerde site-to-site VPN op FTDv beheerd door FirePower Device Manager (FDM).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van VPN
- BGP-configuraties op FTDv
- Ervaring met FDM

Gebruikte componenten

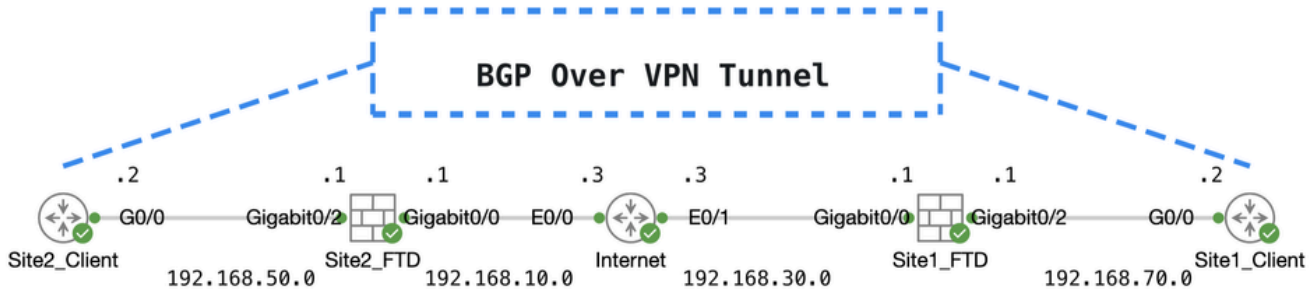
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco FTDv versie 7.4.2
- Cisco FDM versie 7.4.2

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

Netwerkdigram



Topo

Configuraties op VPN

Stap 1. Zorg ervoor dat de IP-interconnectiviteit tussen knooppunten gereed en stabiel is. De slimme licentie op FDM wordt met succes geregistreerd bij de smart account.

Stap 2. De gateway van Site1 Client is geconfigureerd met het binnenste IP-adres van Site1 FTD (192.168.70.1). De gateway van de Site2-client is geconfigureerd met het interne IP-adres van Site2 FTD (192.168.50.1). Zorg er ook voor dat de standaardroute op beide FTD's correct is geconfigureerd na FDM-initialisatie.

Meld u aan bij de GUI van elke FDM. Navigeer naar `Device > Routing`. Klik op de knop `.View Configuration`. Klik op het `Static Routing` tabblad om de standaard statische route te controleren.

The screenshot shows the Firewall Device Manager GUI for device ftdv742. The 'Routing' section is active, and the 'Static Routing' tab is selected. A table displays the configured static routes:

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	StaticRoute_IPv4	outside	IPv4	0.0.0.0/0	192.168.30.3		1	

Site1_FTD_Gateway

Device Summary
Routing

Add Multiple Virtual Routers

Static Routing | BGP | OSPF | EIGRP | ECMP Traffic Zones

1 route

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	StaticRoute_IPv4	outside	IPv4	0.0.0.0/0	192.168.10.3		1	

Site2_FTD_Gateway

Stap 3. Configureer route-gebaseerde site-to-site VPN. In dit voorbeeld, vorm eerst Site1 FTD.

Stap 3.1. Aanmelden bij de FDM GUI van Site1 FTD. Maak een nieuw netwerkobject voor het interne netwerk van Site1 FTD. Navigeer naar **Objects > Networks**, klik op de knop +.

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: ftdv742

Object Types

Networks

Network Objects and Groups

9 objects

Filter

Preset filters: System defined, User defined

Maken_Netwerk_Object

Stap 3.2. Verstrek de nodige informatie. Klik op de OK knop.

- Naam: inside_192.168.70.0
- Type: netwerk
- Netwerk: 192.168.70.0/24

Add Network Object



Name

inside_192.168.70.0

Description

Type



Network



Host



FQDN



Range

Network

192.168.70.0/24

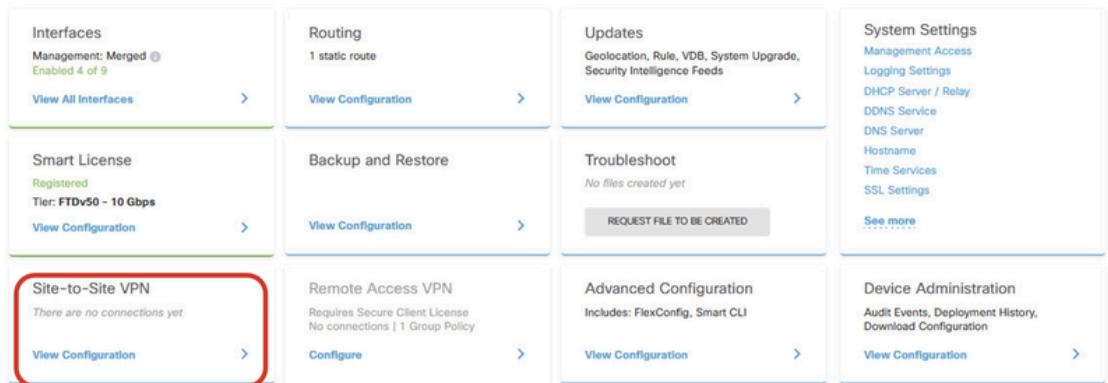
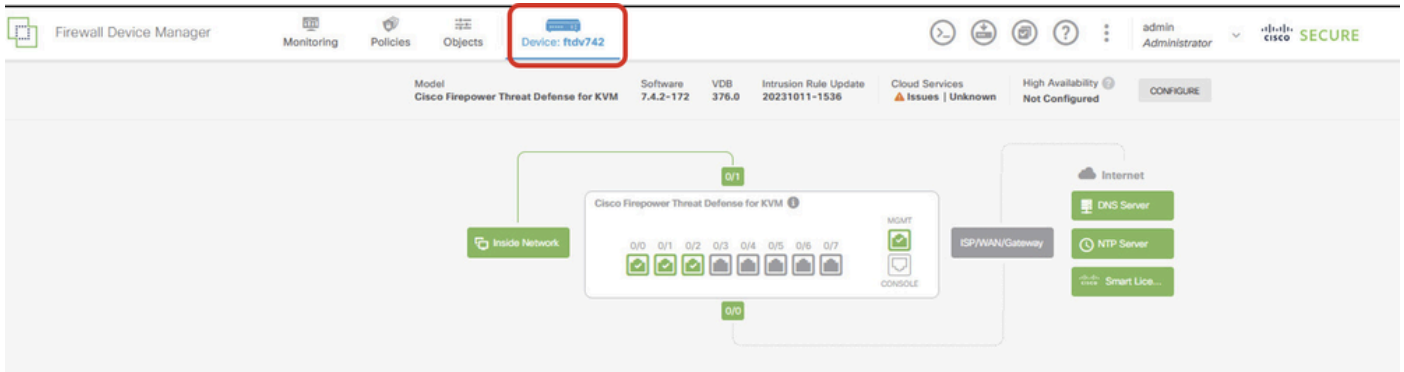
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

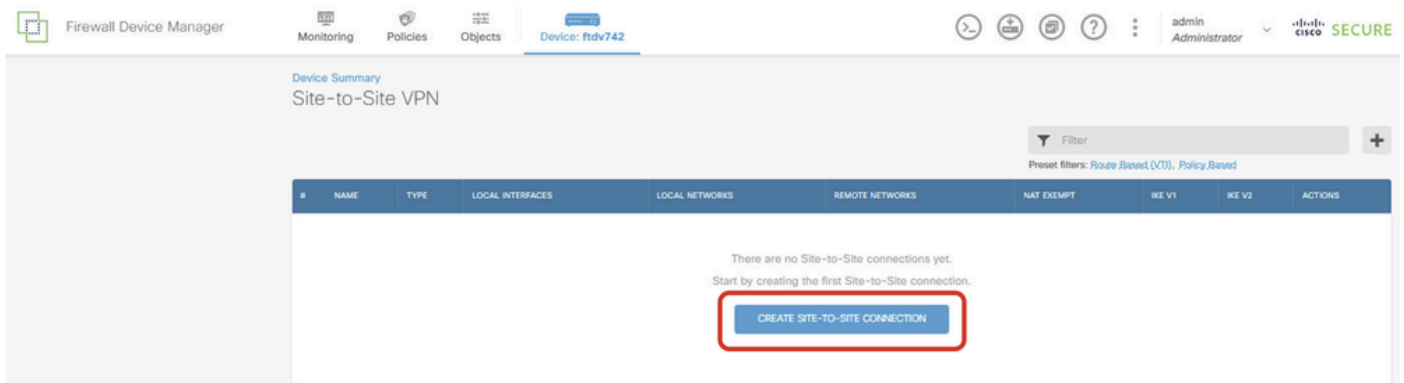
Site1_Binnen_Netwerk

Stap 3.3. Navigeer naar **Device > Site-to-Site VPN** . Klik op de knop **.View Configuration**



Site-to-Site VPN bekijken

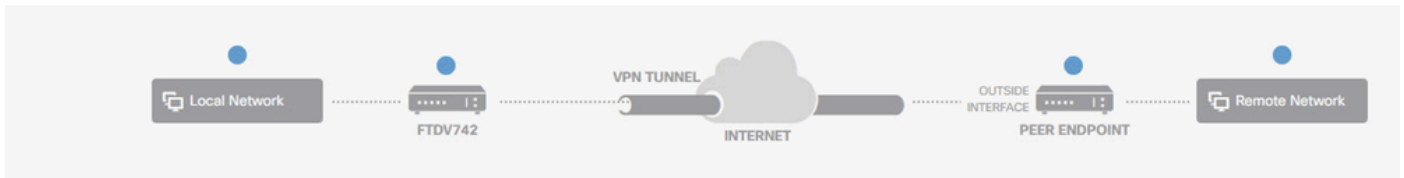
Stap 3.4. Start het maken van een nieuwe site-to-site VPN. Klik op de knop **.CREATE SITE-TO-SITE CONNECTION**



Create_Site-to-Site_Connection

Stap 3.5. Verstrek de nodige informatie.

- Naam verbindingprofiel: Demo_S2S
- Type: routegebaseerd (VTI)
- Lokale VPN-toegangsinterface: klik op de vervolgkeuzelijst en klik vervolgens op **Create new Virtual Tunnel Interface** .



Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name: **Demo_S2S**

Type: **Route Based (VTI)** (selected), Policy Based

Sites Configuration

LOCAL SITE	REMOTE SITE
Local VPN Access Interface Please select Filter Nothing found Create new Virtual Tunnel Interface	Remote IP Address [Empty field] NEXT

Aanmaken_VTI_in_VPN_Wizard

Stap 3.6. Verstrek de nodige informatie om een nieuwe VTI te creëren. Klik op de knop OK.

- Naam: demovti
- Tunnel-id: 1
- Tunnelbron: buiten (Gigabit Ethernet0/0)
- IP-adres en subnetmasker: 169.254.10.1/24
- Status: klik op de schuifschakelaar voor de ingeschakelde positie

Name Status

Most features work with named interfaces only, although some require unnamed interfaces.

Description

Tunnel ID 0 - 10413

Tunnel Source

IP Address and Subnet Mask /

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

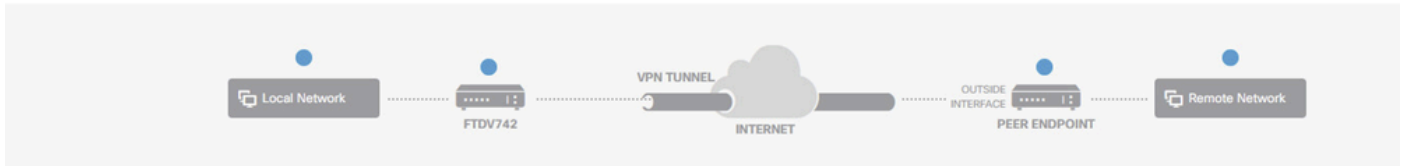
Creëer_VTI_Details

Stap 3.7. Blijf de nodige informatie verstrekken. Klik op de knop VOLGENDE.

- Lokale VPN-toegangsinterface: demovti (gemaakt in stap 3.6.)
- Remote IP-adres: 192.168.10.1

New Site-to-site VPN

1 Endpoints 2 Configuration 3 Summary



Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name: Demo_S2S

Type: Route Based (VTI) Policy Based

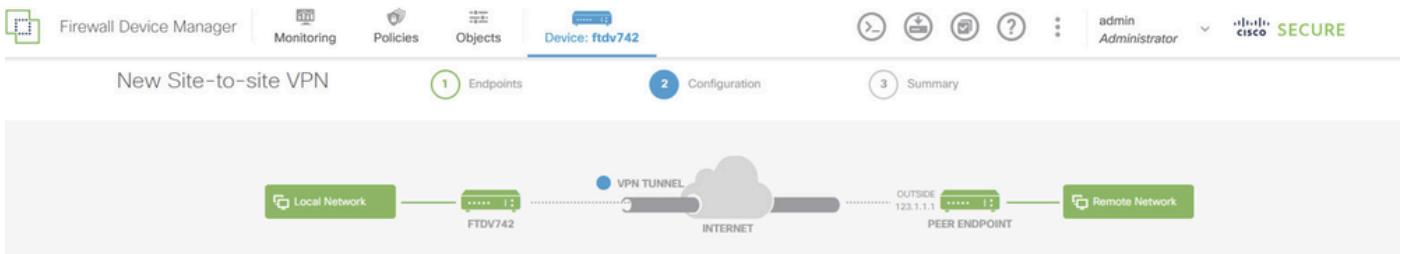
Sites Configuration

LOCAL SITE	REMOTE SITE
Local VPN Access Interface demovti (Tunnel1)	Remote IP Address 192.168.10.1

CANCEL NEXT

VPN_Wizard_Endpoints_Step1

Stap 3.8. Ga naar IKE-beleid. Klik op de knop BEWERKEN.



Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

Info IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2 IKE VERSION 1

IKE Policy

Globally applied

IPSec Proposal

None selected *Warning*

Bewerken_IKE_Policy

Stap 3.9. Voor het IKE-beleid kunt u een vooraf gedefinieerde gebruiken of een nieuwe maken door op Nieuw IKE-beleid maken te klikken.

In dit voorbeeld, schakel een bestaand IKE-beleid AES-SHA-SHA en creëer ook een nieuwe voor

demo doeleinden. Klik op de knop OK om op te slaan.

- Naam: AES256_DH14_SHA256_SHA256
- Versleuteling: AES, AES256
- DH-groep: 14
- Integriteitshash: SHA, SHA256
- PRF-hash: SHA, SHA256
- Levensduur: 86400 (standaard)

The image shows two parts of a software interface. On the left, a list of IKE policies is displayed with a filter. The 'AES-SHA-SHA' policy is selected and highlighted with a red box. Below the list is a 'Create New IKE Policy' button, also highlighted with a red box. An arrow points from this button to the 'Add IKE v2 Policy' dialog box on the right. The dialog box contains the following configuration details:

- Priority: 1
- Name: AES256_DH14_SHA256_SHA256
- State: On (toggle)
- Encryption: AES, AES256
- Diffie-Hellman Group: 14
- Integrity Hash: SHA, SHA256
- Pseudo Random Function (PRF) Hash: SHA, SHA256
- Lifetime (seconds): 86400 (Between 120 and 2147483647 seconds)

At the bottom of the dialog box, there are 'CANCEL' and 'OK' buttons. The 'OK' button is highlighted with a red box.

Add_New_IKE_Policy

Filter

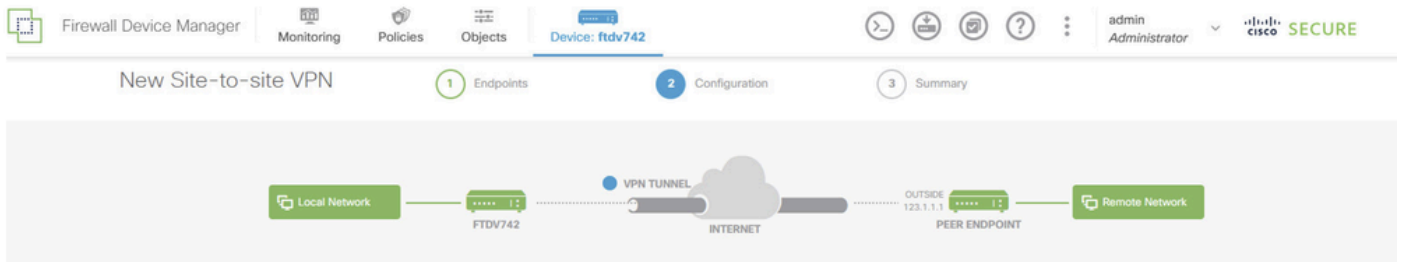
<input type="checkbox"/>	AES-GCM-NULL-SHA	i
<input checked="" type="checkbox"/>	AES-SHA-SHA	i
<input type="checkbox"/>	DES-SHA-SHA	i
<input checked="" type="checkbox"/>	AES256_DH14_SHA256_SHA256	i

Create New IKE Policy

OK

Inschakelen_Nieuw_IKE_Beleid

Stap 3.10. Ga naar het IPSec-voorstel. Klik op de knop BEWERKEN.



Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

1 IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2 IKE VERSION 1

IKE Policy

Globally applied

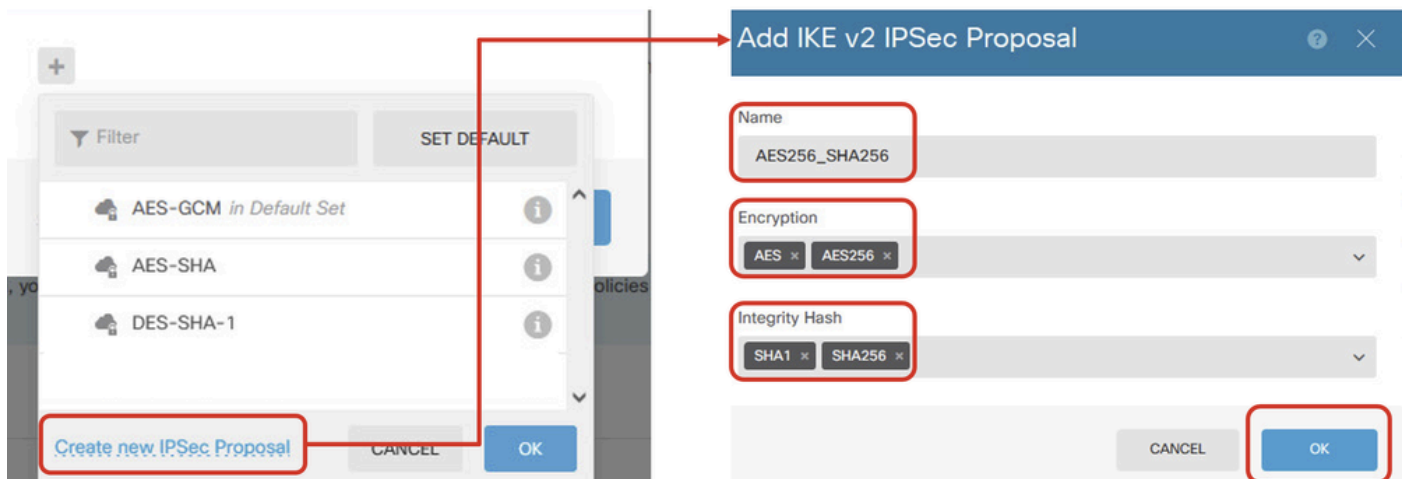
IPSec Proposal

None selected !

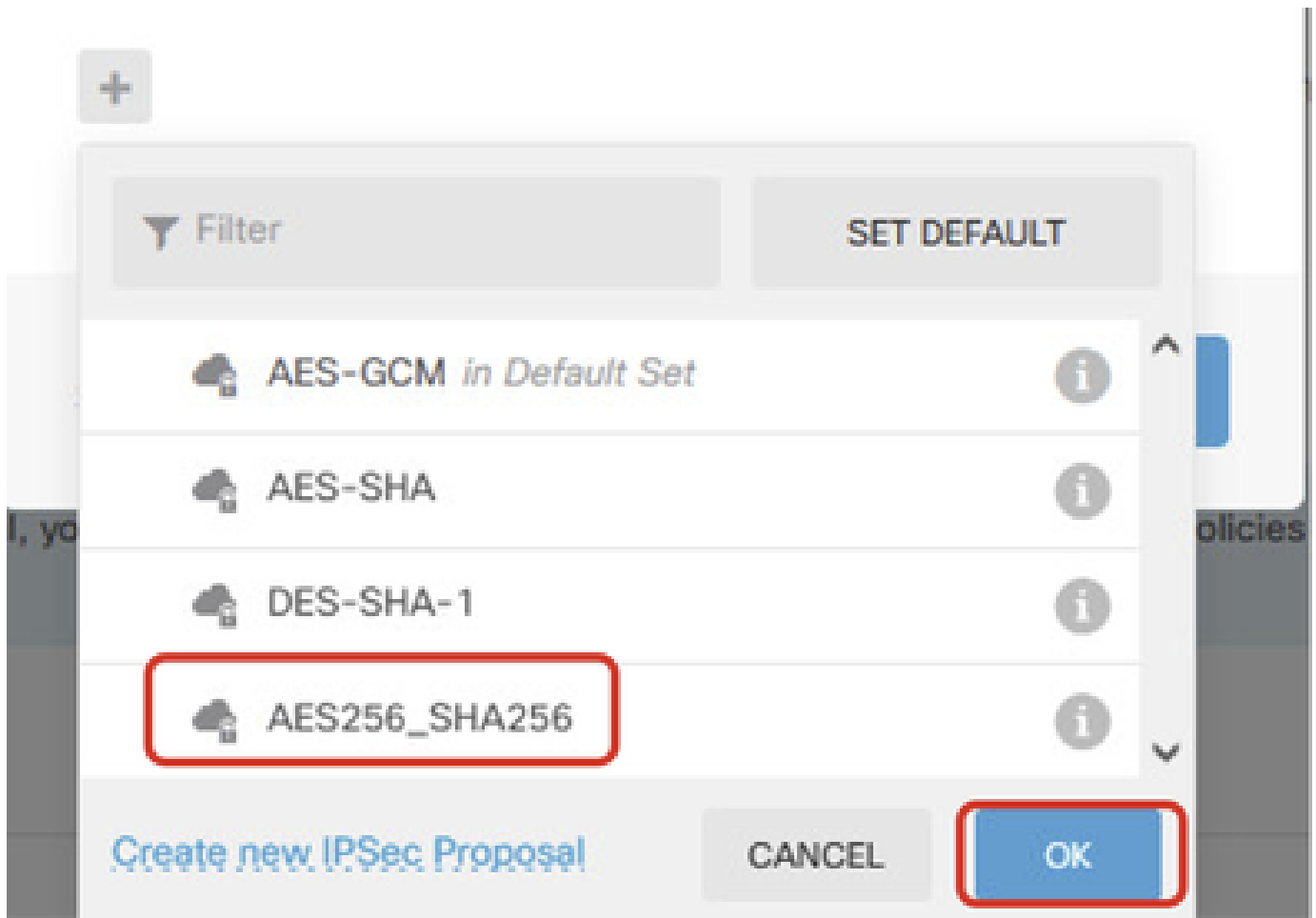
Bewerken_IKE_voorstel

Stap 3.11. Voor het IPSec-voorstel kunt u een vooraf gedefinieerde interface gebruiken of u kunt een nieuwe maken door op Nieuw IPSec-voorstel maken te klikken. In dit voorbeeld, maak een nieuwe voor demo doeleinden. Verstrek de nodige informatie. Klik op de knop OK om op te slaan.

- Naam: AES256_SHA256
- Versleuteling: AES, AES256
- Integriteitshash: SHA1, SHA256



Add_New_IPSec_voorstel



Enable_New_IPSec_voorstel

Stap 3.12. Configureer de voorgedeelde sleutel. Klik op de knop VOLGENDE.

Noteer deze vooraf gedeelde sleutel en configureer deze later op de Site2 FTD.

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftdv742 | admin Administrator | CISCO SECURI

FTDV742 | INTERNET | PEER ENDPOINT

Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

i IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2 | IKE VERSION 1

IKE Policy
Globally applied

IPSec Proposal
Custom set selected

Authentication Type
 Pre-shared Manual Key Certificate

Local Pre-shared Key

Remote Peer Pre-shared Key

Configuratie_Vooraf_Gedeeld_Sleutel

Stap 3.13. Herzie de VPN-configuratie. Als er iets moet worden gewijzigd, klikt u op de knop TERUG. Als alles goed is, klikt u op de knop VOLTOOIEN.

Demo_S2S Connection Profile

i Peer endpoint needs to be configured according to specified below configuration.

VPN Access Interface

demovti (169.254.10.1)



Peer IP Address

192.168.10.1

IKE V2

IKE Policy

aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14, aes,aes-256-sha,sha256-sha,sha256-14

IPSec Proposal

aes,aes-256-sha-1,sha-256

Authentication Type

Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration

28800 seconds

Lifetime Size

4608000 kilobytes

ADDITIONAL OPTIONS

Diffie-Hellman Null (not selected)

i Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

BACK

FINISH

VPN_Wizard_Compleet

Stap 3.14. Maak een toegangscontroleregel om verkeer door de FTD te laten passeren. In dit voorbeeld, sta allen voor demodoeleinden toe. Wijzig uw beleid op basis van uw werkelijke behoeften.

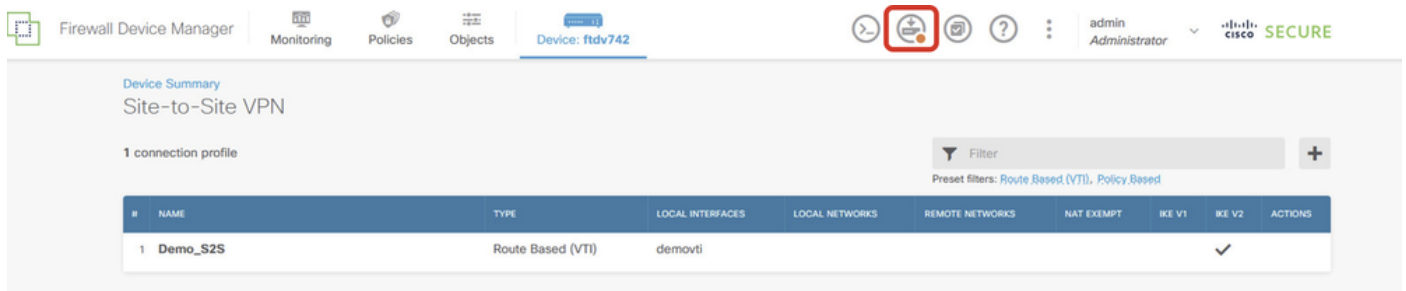
The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes "Firewall Device Manager", "Monitoring", "Policies", "Objects", and "Device: ftdv742". The user is logged in as "admin Administrator". The main content area is titled "Security Policies" and shows a breadcrumb trail: "SSL Decryption" → "Identity" → "Security Intelligence" → "NAT" → "Access Control" → "Intrusion". Under "Access Control", there is one rule named "Demo_allow". The rule configuration table is as follows:

#	NAME	ACTION	SOURCE			DESTINATION			APPLICATIONS	URLS	USERS	ACTIONS
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS				
1	Demo_allow	Allow	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY		

At the bottom, the "Default Action" is set to "Access Control" with a "Block" button.

Stap 3.15. (Optioneel) Configureer NAT-vrijstellingsregel voor het clientverkeer op FTD als dynamische NAT is geconfigureerd voor de client om toegang tot internet te krijgen. In dit voorbeeld is het niet nodig om een NAT-vrijgestelde regel te configureren omdat er op elke FTD geen dynamische NAT is geconfigureerd.

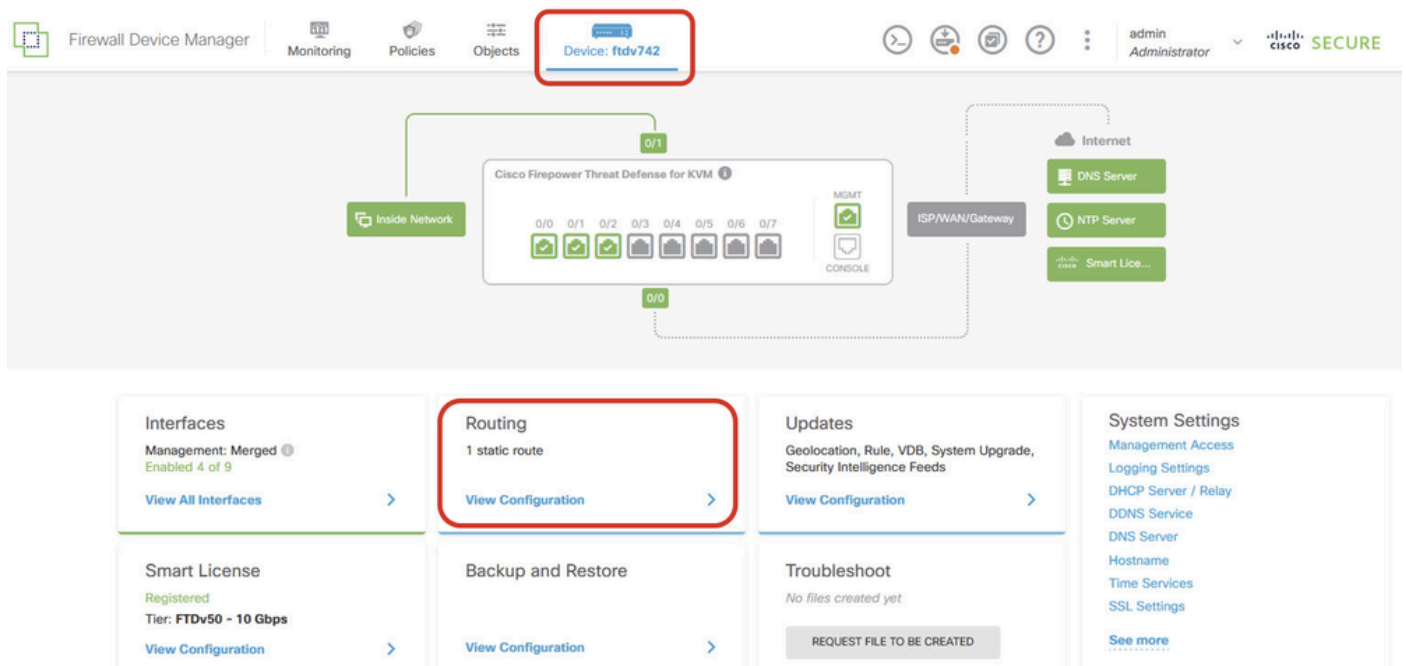
Stap 3.16. Stel de configuratieveranderingen op.



Implementatie_VPN_configuratie

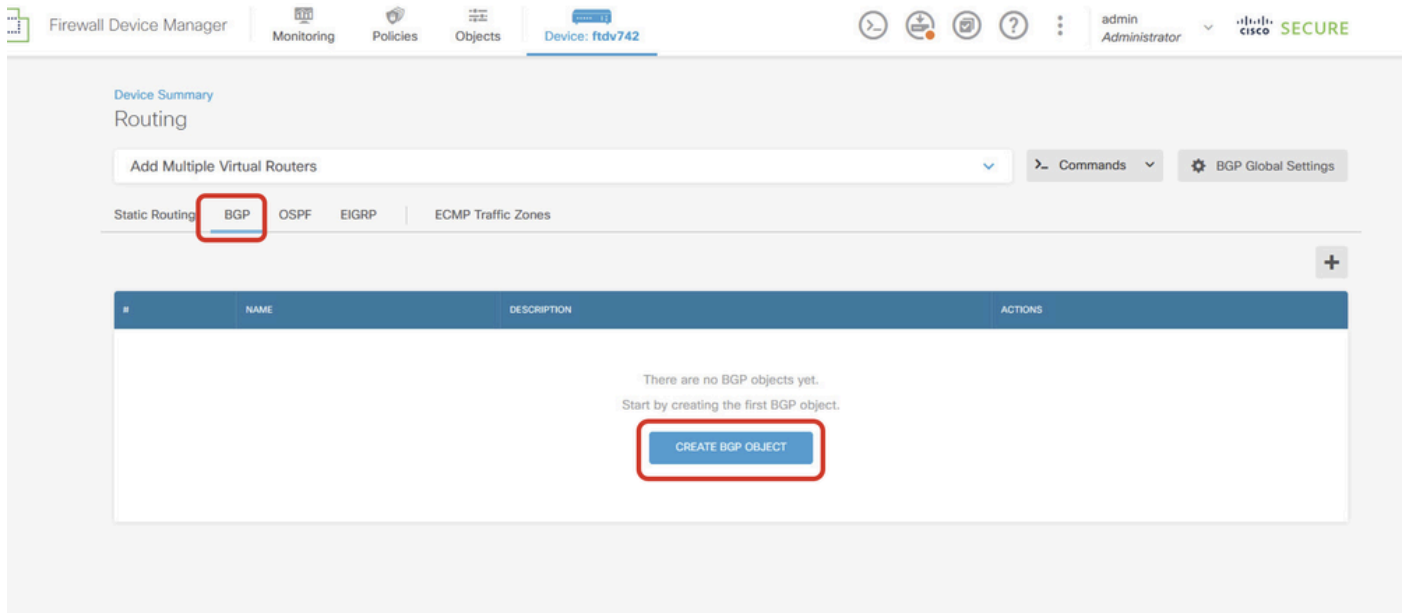
Configuraties op BGP

Stap 4. Navigeer naar apparaat > routing. Klik op Configuratie weergeven.



View_Routing_Configuration

Stap 5. Klik op het tabblad BGP en klik vervolgens op CREATE BGP OBJECT.



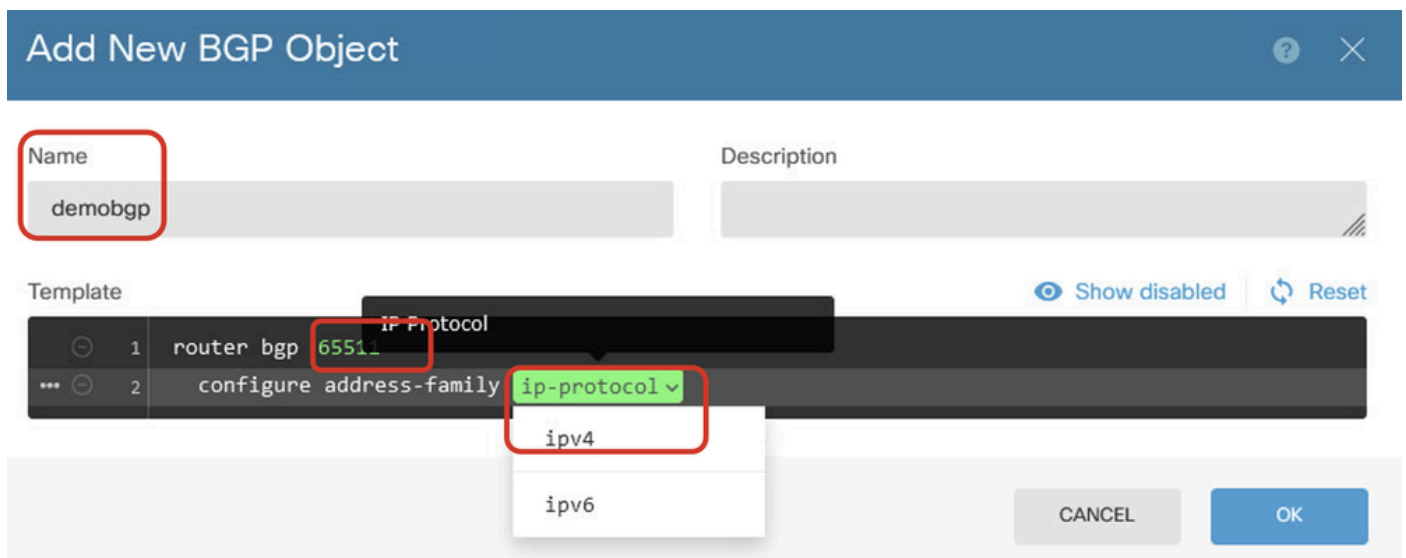
Maken_BGP_Object

Stap 6. Geef de naam van het object op. Navigeren naar Sjabloon en configureren. Klik op de knop OK om op te slaan.

Naam: demobgp

Lijn 1: Als nummer instellen. Klik op als nummer. Handmatige invoer lokaal AS-nummer. In dit voorbeeld, AS-nummer 65511 voor Site1 FTD.

Lijn 2: IP-protocol configureren. Klik op IP-protocol. Selecteer ipv4.



Maken_BGP_Object_ASNumber_Protocol

Lijn 4: Meer instellingen configureren. Klik op Instellingen, kies algemeen en klik vervolgens op Uitgeschakeld tonen.

Add New BGP Object

Name: demobgp

Description:

Template: Show disabled Reset

```

1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4     configure address-family ipv4 settings

```

Address Family IPv4 Settings

- general
- advanced

CANCEL OK

Creëer_BGP_Object_AddressSetting

Lijn 6: Klik op het pictogram + om de lijn in staat te stellen het BGP-netwerk te configureren. Klik op het netwerkobject. U kunt de bestaande beschikbare objecten zien en er een kiezen. Kies in dit voorbeeld de objectnaam `inside_192.168.70.0` (gemaakt in Stap 3.2.).

Add New BGP Object

Name: demobgp

Description:

Template: Hide disabled Reset

```

1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4     configure address-family ipv4 general
5     distance bgp 20 200 200
6     network network-object
7     network network-object route-map map-tag
8     bgp inject-map inject-map exist-map exist-map options
9     configure aggregate-address map-type
10    configure filter-rules direction
11    configure neighbor neighbor-address remote-as as-number config-options
12    configure ipv4 redistribution protocol identifier none
13    bgp router-id router-id

```

Aanmaken_BGP_Object_Add_Network

Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

The screenshot shows a configuration editor with a list of lines (1-13) and a dropdown menu. The configuration lines are:

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4     configure address-family ipv4 general
5     distance bgp 20 200 200
6   network
7   network
8   bgp inje
9   configur
10  configur
11  configur
12  configur
13  bgp router-i
```

The dropdown menu is open, showing several network options:

- OutsidelPv4DefaultRoute Network
- OutsidelPv4Gateway Host
- any-ipv4 Network
- any-ipv6 Network
- inside_192.168.70.0 Network (highlighted with a red box)

The selected option is "inside_192.168.70.0 Network".

Maken_BGP_Object_Add_Network2

Lijn 11: Klik op het pictogram + om de lijn in staat te stellen om de BGP-buurinformatie te configureren. Klik op buuradres en voer handmatig het peer-BGP buuradres in. In dit voorbeeld is het 169.254.10.2 (VTI IP-adres van Site2 FTD). Klik op as-number en voer handmatig het peer AS-nummer in. In dit voorbeeld is 65510 voor Site2 FTD. Klik op Config-opties en kies eigenschappen.

Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6         network inside_192.168.70.0
7         network network-object route-map map-tag
8         bgp inject-map inject-map exist-map exist-map options
9         configure aggregate-address map-type
10        configure filter-rules direction
11        configure neighbor 169.254.10.2 remote-as 65510 config-options
12        configure ipv4 redistribution protocol identifier
13        bgp router-id router-id
```

Select Configuration Option

config-options

properties

Creëer_BGP_Object_NeighbourSetting

Lijn 14: Klik op het pictogram + om de lijn in staat te stellen bepaalde eigenschappen van de buur te configureren. Klik op activeringsopties en kies eigenschappen.

Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6         network inside_192.168.70.0
7         network network-object route-map map-tag
8         bgp inject-map inject-map exist-map exist-map options
9         configure aggregate-address map-type
10        configure filter-rules direction
11        configure neighbor 169.254.10.2 remote-as 65510 properties
12          neighbor 169.254.10.2 remote-as 65510
13          configure neighbor 169.254.10.2 activate activate-options
14            activate-options
15          configure ipv4 redistribution protocol id
16          bgp router-id router-id
```

Maken_BGP_Object_NeighborSetting_Properties

Lijn 13: Klik op het pictogram + om de lijn in staat te stellen geavanceerde opties weer te geven. Klik op Instellingen en kies Geavanceerd.

Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6         network inside_192.168.70.0
7         network network-object route-map map-tag
8         bgp inject-map inject-map exist-map exist-map options
9         configure aggregate-address map-type
10        configure filter-rules direction
11        configure neighbor 169.254.10.2 remote-as 65511 properties
12        neighbor 169.254.10.2 remote-as 65511
13        configure neighbor 169.254.10.2 remote-as 65511 settings
14        configure neighbor 169.254.10.2 activate
15        neighbor 169.254.10.2 activate
16        configure neighbor 169.254.10.2 activate
17        configure ipv4 redistribution protocol identifier
18        bgp router-id router-id
```

Select Neighbor Settings

settings

general

advanced

migration

ha-mode

CANCEL

OK

Maken_BGP_Object_NeighborSetting_Properties_Advanced

Lijn 18: Klik op opties en kies uitschakelen om MTU-detectie van pad uit te schakelen.

Add New BGP Object



Name

Description

demobgp

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3   address-family ipv4 unicast
4     configure address-family ipv4 general
5     distance bgp 20 200 200
6     network inside_192.168.70.0
7     network network-object route-map map-tag
8     bgp inject-map inject-map exist-map exist-map options
9     configure aggregate-address map-type
10    configure filter-rules direction
11    configure neighbor 169.254.10.2 remote-as 65510 properties
12    neighbor 169.254.10.2 remote-as 65510
13    configure neighbor 169.254.10.2 remote-as advanced
14    neighbor 169.254.10.2 password secret
15    configure neighbor 169.254.10.2 hops options
16    neighbor 169.254.10.2 version version-number options (optional)
17    neighbor 169.254.10.2 transport connection-mode options
18    neighbor 169.254.10.2 transport path-mtu-discovery options
19    configure neighbor 169.254.10.2 activate properties
20    neighbor 169.254.10.2 activate
21    configure neighbor 169.254.10.2 activate settings
22    configure ipv4 redistribution protocol identifier none
23    bgp router-id router-id
```

Maken_BGP_Object_NeighborSetting_Properties_Advanced_PMD

Lijn 14, 15, 16, 17: Klik op de -toets om de lijnen uit te schakelen. Klik vervolgens op de knop OK om het BGP-object op te slaan.

Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6       network inside_192.168.70.0
7       network network-object route-map map-tag
8     bgp inject-map inject-map exist-map exist-map options
9     configure aggregate-address map-type
10    configure filter-rules direction
11    configure neighbor 169.254.10.2 remote-as 65510 properties
12    neighbor 169.254.10.2 remote-as 65510
13    configure neighbor 169.254.10.2 remote-as advanced
14    neighbor 169.254.10.2 password secret
15    configure neighbor 169.254.10.2 hops options
16    neighbor 169.254.10.2 version version-number
17    neighbor 169.254.10.2 transport connection-mode options
18    neighbor 169.254.10.2 transport path-mtu-discovery disable
19    configure neighbor 169.254.10.2 activate properties
20    neighbor 169.254.10.2 activate
21    configure neighbor 169.254.10.2 activate settings
22    configure ipv4 redistribution protocol identifier none
23  bgp router-id router-id
```

CANCEL

OK

Creëer_BGP_Object_DisableLines

Dit is een overzicht van de BGP-instelling in dit voorbeeld. U kunt de andere BGP-instellingen configureren op basis van uw werkelijke behoeften.

Name	Description
demobgp	

Template

Hide disabled

Reset

```

1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5       distance bgp 20 200 200
6       network inside_192.168.70.0
7       network network-object route-map map-tag
8       bgp inject-map inject-map exist-map exist-map options
9       configure aggregate-address map-type
10      configure filter-rules direction
11      configure neighbor 169.254.10.2 remote-as 65510 properties
12      neighbor 169.254.10.2 remote-as 65510
13      configure neighbor 169.254.10.2 remote-as advanced
14      neighbor 169.254.10.2 password secret
15      configure neighbor 169.254.10.2 hops options
16      neighbor 169.254.10.2 version version-number
17      neighbor 169.254.10.2 transport connection-mode options
18      neighbor 169.254.10.2 transport path-mtu-discovery disable
19      configure neighbor 169.254.10.2 activate properties
20      neighbor 169.254.10.2 activate
21      configure neighbor 169.254.10.2 activate settings
22      configure ipv4 redistribution protocol identifier none
23      bgp router-id router-id
  
```

CANCEL

OK

Maken_BGP_Object_Final_Overview

Stap 7. Implementeer de BGP-configuratie wijzigingen.

The screenshot shows the Cisco Firewall Device Manager interface. At the top, there are navigation tabs: Firewall Device Manager, Monitoring, Policies, Objects, and Device: ftdv742. The 'Device: ftdv742' tab is active. Below the navigation, there are icons for navigation and help, and a user profile for 'admin Administrator'. The main content area is titled 'Device Summary Routing'. It features a search bar 'Add Multiple Virtual Routers' and a 'Commands' dropdown. Below this, there are tabs for 'Static Routing', 'BGP', 'OSPF', 'EIGRP', and 'ECMP Traffic Zones'. The 'BGP' tab is selected. A table shows '1 object' with the following details:

#	NAME	DESCRIPTION	ACTIONS
1	demobgp		

Implementatie_BGP_configuratie

Stap 8. De configuratie voor Site1 FTD is nu voltooid.

Herhaal stap 3 tot en met stap 7 om Site2 FTD VPN en BGP te configureren met de bijbehorende parameters van Site2 FTD.

Configuratieoverzicht van Site1 FTD en Site2 FTD in CLI.

Site1 FTD	Site2 FTD
<pre> NGFW versie 7.4.2 interface Gigabit Ethernet0/0 nameif buiten cts-handleiding propagate sgt-conservatie-untag beleid statisch zicht uitgeschakeld vertrouwd veiligheidsniveau 0 IP-adres 192.168.30.1 255.255.255.0 interface Gigabit Ethernet0/2 nameif inside veiligheidsniveau 0 IP-adres 192.168.70.1 255.255.255.0 interfacetunnel 1 nameif demovti IP-adres 169.254.10.1 255.255.255.0 tunnelbroninterface buiten tunnelbestemming 192.168.10.1 tunnelmodus ipsec ipv4 tunnelbeveiliging ipsec-profiel ipsec_profile e4084d322d objectnetwerk OutsideIPv4Gateway host 192.168.30.3 objectnetwerk inside_192.168.70.0 subnetnummer 192.168.70.0 255.255.255.0 algemene toegangsgroep NGFW_ONBOX_ACL toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 268435457: TOEGANGSBELEID: NGFW_Access_Policy toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 268435457: L5 REGEL: Inside_Outside_Rule access-list NGFW_ONBOX_ACL geavanceerde trust object-groep acSvcbg-268435457 ifc in elke ifc buiten elk regel-id 268435457 gebeurtenislogboek, beide toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 268435458: TOEGANGSBELEID: NGFW_Access_Policy toegangslijst NGFW_ONBOX_ACL-opmerking regel-id </pre>	<pre> NGFW versie 7.4.2 interface Gigabit Ethernet0/0 nameif buiten cts-handleiding propagate sgt-conservatie-untag beleid statisch zicht uitgeschakeld vertrouwd veiligheidsniveau 0 IP-adres 192.168.10.1 255.255.255.0 interface Gigabit Ethernet0/2 nameif inside veiligheidsniveau 0 IP-adres 192 168 50 1255 255 255 00 interfacetunnel 1 nameif-demovti25 IP-adres 169.254.10.2 255.255.255.0 tunnelbroninterface buiten tunnelbestemming 192.168.30.1 tunnelmodus ipsec ipv4 tunnelbeveiliging ipsec-profiel ipsec_profile e4084d322d objectnetwerk OutsideIPv4Gateway host 192.168.10.3 objectnetwerk inside_192.168.50.0 subnetnummer 192.168.50.0 255.255.255.0 algemene toegangsgroep NGFW_ONBOX_ACL toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 268435457: TOEGANGSBELEID: NGFW_Access_Policy toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 268435457: L5 REGEL: Inside_Outside_Rule access-list NGFW_ONBOX_ACL geavanceerde trust object-groep acSvcbg-268435457 ifc in elke ifc buiten elk regel-id 268435457 gebeurtenislogboek, beide toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 268435458: TOEGANGSBELEID: NGFW_Access_Policy toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 268435458: L5 REGEL: Demo_allow </pre>

<p>268435458: L5 REGEL: Demo_allow toegangslijst NGFW_ONBOX_ACL geavanceerde vergunningsobject-groep lacSvcg-268435458 elk regel-id 268435458-gebeurtenislogboek, zowel toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 1: TOEGANGSBELEID: NGFW_Access_Policy toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 1: L5 REGEL: DefaultActionRule toegangslijst Geavanceerd NGFW_ONBOX_ACL ontkennen ip elke regel-id 1</p> <p>router bgp 65511 bgp log-buurwijzigingen bgp router-id vrf automatisch toewijzen IPv4-unicast voor adresfamilie buur 169.254.10.2 op afstand 65510 buur 169.254.10.2 transportpad-mtu-discovery uitschakelen buur 169.254.10.2 activeren netwerk 192.168.70.0 geen automatische samenvatting geen synchronisatie exit-address-family</p> <p>route buiten 0.0.0.0 0.0.0 192.168.30.3 1</p> <p>crypto ipsec ikev2 ipsec-voorstel AES256_SHA256 ESP-encryptie protocol aes-256 aes protocol ESP-integriteit sha-256 sha-1</p> <p>crypto ipsec-profiel ipsec_profile e4084d322d set ikev2 ipsec-voorstel AES256_SHA256 instellen security-associatie-levensduur kilobytes 4608000 instellen security-associatielevensduur seconden 28800</p> <p>crypto ipsec security-association pmtu-aging oneindig</p> <p>crypto ikev2-beleid 1 encryptie aes-256 aes integriteit sha256 sha groep 14 prf sha256 sha levenslange 86400</p> <p>crypto ikev2-beleid 20 encryptie aes-256 aes-192 aes integriteit sha512 sha384 sha256 sha groep 21 20 16 15 14</p>	<p>toegangslijst NGFW_ONBOX_ACL geavanceerde vergunningsobject-groep lacSvcg-268435458 elk regel-id 268435458-gebeurtenislogboek, zowel toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 1: TOEGANGSBELEID: NGFW_Access_Policy toegangslijst NGFW_ONBOX_ACL-opmerking regel-id 1: L5 REGEL: DefaultActionRule toegangslijst Geavanceerd NGFW_ONBOX_ACL ontkennen ip elke regel-id 1</p> <p>router bgp 65510 bgp log-buurwijzigingen bgp router-id vrf automatisch toewijzen IPv4-unicast voor adresfamilie buur 169.254.10.1 op afstand 65511 buur 169.254.10.1 transportpad-mtu-discovery uitschakelen buur 169.254.10.1 activeren netwerk 192.168.50.0 geen automatische samenvatting geen synchronisatie exit-address-family</p> <p>route buiten 0.0.0.0 0.0.0 192.168.10.3 1</p> <p>crypto ipsec ikev2 ipsec-voorstel AES256_SHA256 ESP-encryptie protocol aes-256 aes protocol ESP-integriteit sha-256 sha-1</p> <p>crypto ipsec-profiel ipsec_profile e4084d322d set ikev2 ipsec-voorstel AES256_SHA256 instellen security-associatie-levensduur kilobytes 4608000 instellen security-associatielevensduur seconden 28800</p> <p>crypto ipsec security-association pmtu-aging oneindig</p> <p>crypto ikev2-beleid 1 encryptie aes-256 aes integriteit sha256 sha groep 14 prf sha256 sha levenslange 86400</p> <p>crypto ikev2-beleid 20 encryptie aes-256 aes-192 aes integriteit sha512 sha384 sha256 sha groep 21 20 16 15 14</p>
---	--

prf sha512 sha384 sha256 sha levenslange 86400	prf sha512 sha384 sha256 sha levenslange 86400
crypto ikev2 activeren buiten	crypto ikev2 activeren buiten
groepsbeleid s2sGP 192.168.10.1 intern groepsbeleid s2sGP 192.168.10.1 eigenschappen VPN-tunnelprotocol ikev2	groepsbeleid s2sGP 192.168.30.1 intern groepsbeleid s2sGP 192.168.30.1 eigenschappen VPN-tunnelprotocol ikev2
tunnelgroep 192.168.10.1 type ipsec-l2l tunnelgroep 192.168.10.1 algemene kenmerken standaardgroepsbeleid s2sGP 192.168.10.1	tunnel-groep 192.168.30.1 type ipsec-l2l tunnelgroep 192.168.30.1 algemene kenmerken standaardgroepsbeleid s2sGP 192.168.30.1
tunnel-groep 192.168.10.1 ipsec-eigenschappen ikev2-***** voor verificatie op afstand vooraf met gedeelde sleutel ikev2-***** voor lokale verificatie met gedeelde sleutel	tunnel-groep 192.168.30.1 ipsec-eigenschappen ikev2-***** voor verificatie op afstand vooraf met gedeelde sleutel ikev2-***** voor lokale verificatie met gedeelde sleutel

Verifiëren

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

Stap 1. Navigeer naar de CLI van elk FTD via console of SSH om de VPN-status van fase 1 en fase 2 te verifiëren via de opdrachten tonen crypto ikev2 sa en tonen crypto ipsec sa.

Site1 FTD	Site2 FTD
ftdv742# toont crypto ikev2 sa	ftdv742# toont crypto ikev2 sa
IKEv2 SA's:	IKEv2 SA's:
Session-id:134, status:UP-ACTIVE, IKE-telling:1, KINDERTELLING:1	Session-id:13, status:UP-ACTIVE, IKE-telling:1, KINDERTELLING:1
Tunnel-id lokale externe FVRF/ivrf-statusrol 563984431 192.168.30.1/500 192.168.10.1/500 Global/Global Ready-responder	Tunnel-id lokale externe FVRF/ivrf-statusrol 339797985 192.168.10.1/500 192.168.30.1/500 Initiator voor wereldwijde/wereldwijde voorbereiding
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK	Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Leven/actieve tijd: 86400/5145 sec	Leven/actieve tijd: 86400/74099 sec
Kinderslot: lokale keuzeschakelaar 0.0.0.0/0 - 25.255.255.255/65535	Kinderslot: lokale keuzeschakelaar 0.0.0.0/0 - 25.255.255.255/65535
externe selector 0.0.0.0/0 - 25.255.255.255/65535	externe selector 0.0.0.0/0 - 25.255.255.255/65535
	ESP spi in/uit: 0xb7b5b38b/0xf0c4239d

<p>ESP spi in/uit: 0xf0c4239d/0xb7b5b38b</p> <p>ftdv742# toont crypto ipsec sa</p> <p>interface: demovti Crypto map tag: __vti-crypto-map-Tunnel1-0-1, volgnummer: 65280, lokaal adres: 192.168.30.1</p> <p>Protected vrf (ivrf): Wereldwijd lokaal nummer (adres/masker/poort/poort): (0.0.0.0/0.0.0.0/0/0) afstandsbediening (adres/masker/poort/poort): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.10.1</p> <p>#pkts encaps: 5720, #pkts versleutelen: 5720, #pkts overzicht: 5720 #pkts decaps: 5717, #pkts decrypt: 5717, #pkts verifieer: 5717 #pkts gecomprimeerd: 0, #pkts gedecomprimeerd: 0 #pkts niet gecomprimeerd: 5720, #pkts comp mislukt: 0, #pkts decomp mislukt: 0 #pre-frag successen: 0, #pre-frag mislukkingen: 0, #fragments gecreëerd: 0 #PMTUs verzonden: 0, #PMTUs rcvd: 0, #decapsulated eieren die hermontage nodig hebben: 0 #TFC rcvd: 0, #TFC verzonden: 0 #Valid ICMP-fouten rcvd: 0, #Invalid ICMP-fouten rcvd: 0 #send fouten: 0, #recv fouten: 0</p> <p>lokale crypto-endpt: 192.168.30.1/500, externe crypto-endpt: 192.168.10.1/500 pad mtu 1500, ipsec overhead 78(44), media mtu 1500 PMTU tijd resterend (sec): 0, DF-beleid: copy-df ICMP-foutvalidatie: uitgeschakeld, TFC-pakketten: uitgeschakeld huidige uitgaande spi: B7B5B38B huidige inkomende spi: F0C4239D</p> <p>inkomende esp sas: Centrifugeren: 0xF0C4239D (4039386013)</p>	<p>ftdv742# toont crypto ipsec sa</p> <p>interface: demovti25 Crypto map tag: __vti-crypto-map-Tunnel1-0-1, volgnummer: 65280, lokaal adres: 192.168.10.1</p> <p>Protected vrf (ivrf): Wereldwijd lokaal nummer (adres/masker/poort/poort): (0.0.0.0/0.0.0.0/0/0) afstandsbediening (adres/masker/poort/poort): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.30.1</p> <p>#pkts encaps: 5721, #pkts versleutelen: 5721, #pkts overzicht: 5721 #pkts decaps: 5721, #pkts decrypt: 5721, #pkts verifieer: 5721 #pkts gecomprimeerd: 0, #pkts gedecomprimeerd: 0 #pkts niet gecomprimeerd: 5721, #pkts comp mislukt: 0, #pkts decomp mislukt: 0 #pre-frag successen: 0, #pre-frag mislukkingen: 0, #fragments gecreëerd: 0 #PMTUs verzonden: 0, #PMTUs rcvd: 0, #decapsulated eieren die hermontage nodig hebben: 0 #TFC rcvd: 0, #TFC verzonden: 0 #Valid ICMP-fouten rcvd: 0, #Invalid ICMP-fouten rcvd: 0 #send fouten: 0, #recv fouten: 0</p> <p>lokale crypto-endpt: 192.168.10.1/500, externe crypto-endpt: 192.168.30.1/500 pad mtu 1500, ipsec overhead 78(44), media mtu 1500 PMTU tijd resterend (sec): 0, DF-beleid: copy-df ICMP-foutvalidatie: uitgeschakeld, TFC-pakketten: uitgeschakeld huidige uitgaande spi: F0C4239D actuele inkomende spi: B7B5B38B</p> <p>inkomende esp sas: SPI: 0xB7B5B38B (3082138507)</p>
--	---

<p>SA Staat: actief transformatie: esp-aes-256 esp-sha-256-hmac geen compressie in gebruiksinstellingen = {L2L, Tunnel, IKEv2, VTI} slot: 0, conn_id: 266, crypto-map: __vti-crypto-map-Tunnel1-0-1 als timing: resterende sleutellevensduur (kB/sec): (4285389/3722) IV-grootte: 16 bytes Ondersteuning van replay-detectie: Y Anti-replay bitmap: 0xFFFFFFFF 0xFFFF uitgaande bse: SPI: 0xB7B5B38B (3082138507) SA Staat: actief transformatie: esp-aes-256 esp-sha-256-hmac geen compressie in gebruiksinstellingen = {L2L, Tunnel, IKEv2, VTI} slot: 0, conn_id: 266, crypto-map: __vti-crypto-map-Tunnel1-0-1 als timing: resterende sleutellevensduur (kB/sec): (4147149/3722) IV-grootte: 16 bytes Ondersteuning van replay-detectie: Y Anti-replay bitmap: 0x00000000 0x00000001</p>	<p>SA Staat: actief transformatie: esp-aes-256 esp-sha-256-hmac geen compressie in gebruiksinstellingen = {L2L, Tunnel, IKEv2, VTI} slot: 0, conn_id: 160, crypto-map: __vti-crypto-map-Tunnel1-0-1 als timing: resterende sleutellevensduur (kB/sec): (3962829/3626) IV-grootte: 16 bytes Ondersteuning van replay-detectie: Y Anti-replay bitmap: 0xFFFFFFFF 0xFFFF uitgaande bse: Centrifugeren: 0xF0C4239D (4039386013) SA Staat: actief transformatie: esp-aes-256 esp-sha-256-hmac geen compressie in gebruiksinstellingen = {L2L, Tunnel, IKEv2, VTI} slot: 0, conn_id: 160, crypto-map: __vti-crypto-map-Tunnel1-0-1 als timing: resterende sleutellevensduur (kB/sec): (4101069/3626) IV-grootte: 16 bytes Ondersteuning van replay-detectie: Y Anti-replay bitmap: 0x00000000 0x00000001</p>
---	---

Stap 2. Navigeer naar de CLI van elk FTD via console of SSH om de BGP status te verifiëren met behulp van de opdrachten `tonen bgp buren` en `tonen route bgp`.

Site1 FTD	Site2 FTD
<p>ftdv742# toont bgp-buren BGP-buur is 169.254.10.2, vrf single_vf, extern AS-65510, externe link BGP versie 4, externe router-ID 192.168.50.1 BGP-status = ingesteld, tot 1 d20 uur Laatste gelezen 00:00:25, laatste schrijven 00:00:45, de tijd van de greep is 180, keepalive interval is 60 seconden Buursessies: 1 actief, is niet geschikt voor meerdere sessies (uitgeschakeld)</p>	<p>ftdv742# toont bgp-buren BGP-buur is 169.254.10.1, vrf single_vf, extern AS-65511, externe link BGP versie 4, externe router-ID 192.168.70.1 BGP-status = ingesteld, tot 1 d20 uur Laatste gelezen 00:00:11, laatste schrijven 00:00:52, de tijd van de greep is 180, keepalive interval is 60 seconden Buursessies: 1 actief, is niet geschikt voor meerdere sessies (uitgeschakeld)</p>

Buurmogelijkheden:
Routevernieuwing: geadverteerd en ontvangen(nieuw)
Vier-octetten ASN Capability: geadverteerd en ontvangen
IPv4 Unicast-adresfamilie: geadverteerd en ontvangen
Multisessievermogen:
Berichtstatistieken:
InQ diepte is 0
OutQ-diepte is 0

Verzonden RCVD
Opent: 1 1
Kennisgevingen: 0 0
Updates: 2.2
Keepalives: 2423 2427
Routevernieuwing: 0,0
Totaal: 2426 2430
De minimale tijd tussen het maken van een advertentie is 30 seconden.

Voor adresfamilie: IPv4 Unicast
Sessie: 169.254.10.2
BGP-tabelversie 3, buurversie 3/0
Grootte van uitvoerwachtrij : 0
Indexnummer 1
1 lid van de updategroep
Verzonden RCVD
Prefixactiviteit: ---- ----
Huidige prefixes: 1 1 (gebruikt 80 bytes)
Totaal: 1 1
Stilzwijgende intrekking: 0 0
Expliciet terugtrekken: 0 0
Gebruikt als beste pad: n.v.t. 1
Gebruikt als multipath: n/a 0

Uitgaand inkomend
Prefixes bij lokaal beleid geweigerd: -----
Bestpath van deze peer: 1 n/a
Totaal: 1 0
Aantal NLRI's in de verstuurd update: max 1, min 0

Het bijhouden van adressen is ingeschakeld, de RIB heeft een route naar 169.254.10.2

Buurmogelijkheden:
Routevernieuwing: geadverteerd en ontvangen(nieuw)
Vier-octetten ASN Capability: geadverteerd en ontvangen
IPv4 Unicast-adresfamilie: geadverteerd en ontvangen
Multisessievermogen:
Berichtstatistieken:
InQ diepte is 0
OutQ-diepte is 0

Verzonden RCVD
Opent: 1 1
Kennisgevingen: 0 0
Updates: 2.2
Keepalives: 2424 2421
Routevernieuwing: 0,0
Totaal: 2427 2424
De minimale tijd tussen het maken van een advertentie is 30 seconden.

Voor adresfamilie: IPv4 Unicast
Sessie: 169 254 10.1
BGP-tabelversie 9, buurversie 9/0
Grootte van uitvoerwachtrij : 0
Indexnummer 4
4 update-groep lid
Verzonden RCVD
Prefixactiviteit: ---- ----
Huidige prefixes: 1 1 (gebruikt 80 bytes)
Totaal: 1 1
Stilzwijgende intrekking: 0 0
Expliciet terugtrekken: 0 0
Gebruikt als beste pad: n.v.t. 1
Gebruikt als multipath: n/a 0

Uitgaand inkomend
Prefixes bij lokaal beleid geweigerd: -----
Bestpath van deze peer: 1 n/a
Totaal: 1 0
Aantal NLRI's in de verstuurd update: max 1, min 0

Het bijhouden van adressen is ingeschakeld, de RIB heeft een route naar 169.254.10.1

<p>Aansluitingen vastgelegd 1; gevallen 0 Laatste reset nooit Transport (TCP) pad-mtu-detectie is uitgeschakeld Naadloze herstart is uitgeschakeld</p>	<p>Aansluitingen vastgelegd 4; gevallen 3 Laatste gereset 1d21h, vanwege interfaceklep van sessie 1 Transport (TCP) pad-mtu-detectie is uitgeschakeld Naadloze herstart is uitgeschakeld</p>
<p>ftdv742# toont route bgp</p> <p>Codes: L - lokaal, C - aangesloten, S - statisch, R - RIP, M - mobiel, B - BGP D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea N1 - OSPF NSSA extern type 1, N2 - OSPF NSSA extern type 2 E1 - OSPF extern type 1, E2 - OSPF extern type 2, V - VPN i - IS-IS, su - IS-IS-samenvatting, L1 - IS-IS niveau-1, L2 - IS-IS niveau-2 ia - IS-IS interarea, * - kandidaat-standaard, U - statische route per gebruiker o - ODR, P - periodieke gedownloadede statische route, + - replicated route SI - Statische InterVRF, BI - BGP InterVRF Gateway of last resort is 192.168.30.3 naar netwerk 0.0.0.0</p> <p>B 192.168.50.0 255.255.255.0 [20/0] via 169.254.10.2, 1d20h</p>	<p>ftdv742# toont route bgp</p> <p>Codes: L - lokaal, C - aangesloten, S - statisch, R - RIP, M - mobiel, B - BGP D - EIGRP, EX - EIGRP extern, O - OSPF, IA - OSPF interarea N1 - OSPF NSSA extern type 1, N2 - OSPF NSSA extern type 2 E1 - OSPF extern type 1, E2 - OSPF extern type 2, V - VPN i - IS-IS, su - IS-IS-samenvatting, L1 - IS-IS niveau-1, L2 - IS-IS niveau-2 ia - IS-IS interarea, * - kandidaat-standaard, U - statische route per gebruiker o - ODR, P - periodieke gedownloadede statische route, + - replicated route SI - Statische InterVRF, BI - BGP InterVRF Gateway of last resort is 192.168.10.3 naar netwerk 0.0.0.0</p> <p>B 192.168.70.0 255.255.255.0 [20/0] via 169.254.10.1, 1d20h</p>

Stap 3. Site1-client en Site2-client pingen elkaar met succes.

Site1-client:

```
Site1_Client#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/56/90 ms
```

Site2-client:

```
Site2_Client#ping 192.168.70.2
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.70.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/39/71 ms
```

Problemen oplossen

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

U kunt deze debug-opdrachten gebruiken om de VPN-sectie probleemoplossing te bieden.

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug vti 255
```

U kunt deze debug commando's gebruiken om de BGP sectie op te lossen.

```
ftdv742# debug ip bgp ?
```

```
A.B.C.D    BGP neighbor address
all All    address families
events     BGP events
import     BGP path import across topologies, VRFs or AFs in BGP Inbound information
ipv4       Address family
ipv6       Address family
keepalives BGP keepalives
out        BGP Outbound information
range     BGP dynamic range
rib-filter Next hop route watch filter events
updates    BGP updates
vpn4       Address family
vpn6       Address family
vrf        VRF scope
<cr>
```


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.