

SD-WAN configureren voor site-to-site VPN via beveiligde firewall

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Informatie over functies](#)

[gedekte topologieën](#)

[HUB & Spoke \(één ISP\)](#)

[Dual HUB & Spoke \(één ISP voor redundante HUB via EGBP tussen secundaire HUB en Spokes\)](#)

[Dual HUB & Spoke \(Dual ISP voor redundante HUB en ISP via EGBP tussen secundaire HUB en Spokes\)](#)

[Conclusie](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft routegebaseerde VPN-implementatiescenario's met BGP-overlay-routing met behulp van de SD-WAN-functie op Secure Firewall.

Voorwaarden

Alle hubs en spaken draaien FTD 7.6 of hoger software en worden beheerd via dezelfde FMC, die ook 7.6 of hoger software draait.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- IKEv2
- Routegebaseerde VPN
- Virtual Tunnel Interfaces (VTI)
- IPSEC
- BGP

Gebruikte componenten

De informatie in dit document is gebaseerd op:

- Cisco Secure Firewall Threat Defense 7.7.10
- Cisco Secure Firewall Management Center 7.7.10

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.

Informatie over functies

Het Management Center vereenvoudigt de configuratie van VPN-tunnels en routing tussen gecentraliseerde hoofdkantoren (hubs) en externe vestigingen (spaken) met behulp van de nieuwe SD-WAN-wizard.

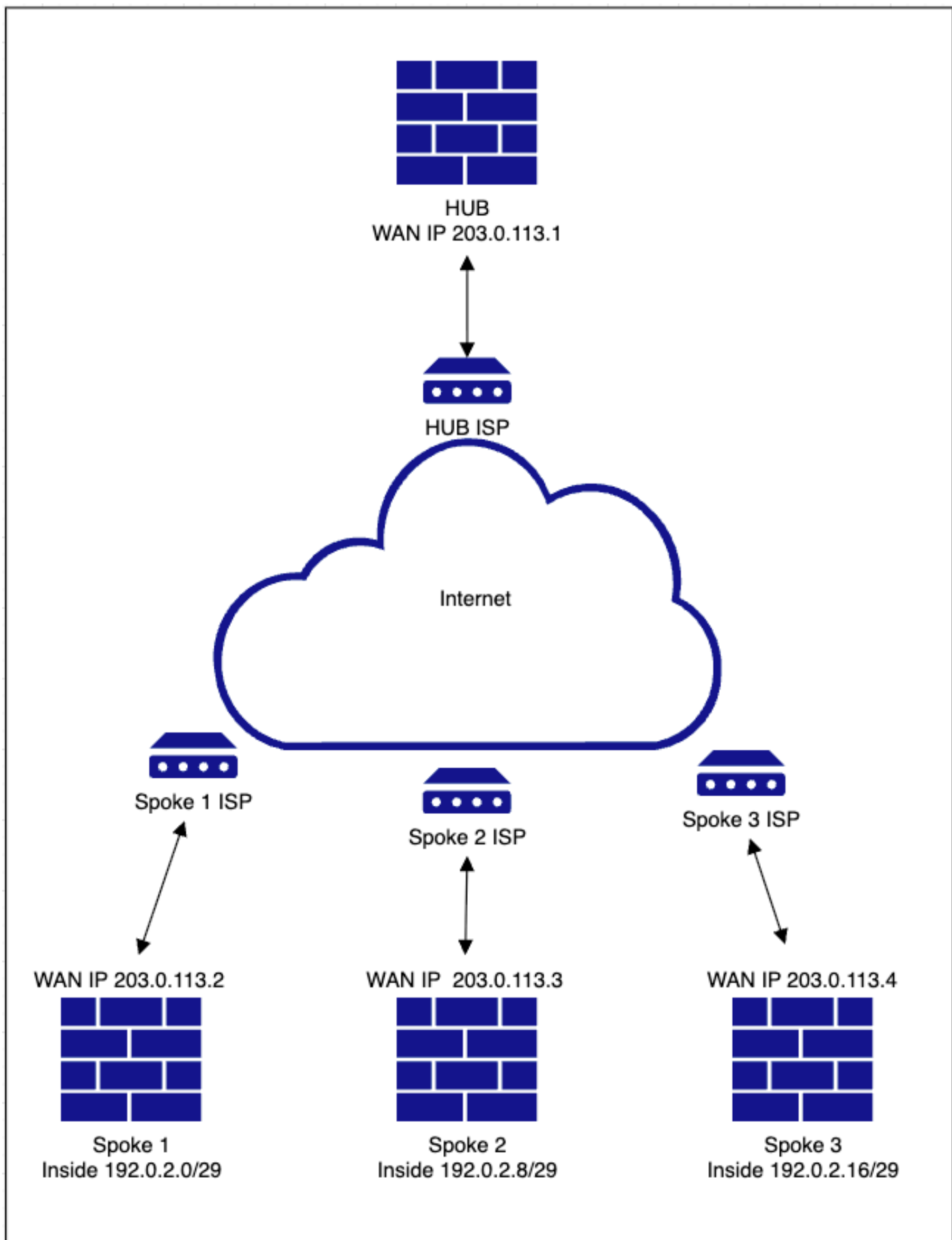
- Automatiseer VPN-configuratie door gebruik te maken van DVTI (Dynamic Virtual Tunnel Interface) op hubs en SVTI (Static Virtual Tunnel Interface) op spaken, met overlay-routing ingeschakeld via BGP.
- Toewijst automatisch SVTI IP-adressen voor spaken en duwt de volledige VTI-configuratie, inclusief crypto-parameters.
- Biedt eenvoudige routeringsconfiguratie in één stap binnen dezelfde wizard om BGP voor overlayrouting mogelijk te maken.
- Maakt schaalbare en optimale routing mogelijk door gebruik te maken van het route-reflectorattribuut voor BGP.
- Meerdere spaken kunnen tegelijkertijd worden toegevoegd met minimale tussenkomst van de gebruiker.

gedekte topologieën

In dit artikel worden meerdere topologieën behandeld om ervoor te zorgen dat gebruikers op de hoogte zijn van verschillende implementatiescenario's.

HUB & Spoke (één ISP)

Netwerkdigram



Configuraties

- Navigeer naar Apparaten > VPN > Site-naar-site > Toevoegen > SD-WAN-topologie > >

Maken.

FMC
Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ? admin

Last Updated: 09:41 AM Refresh NAT Exemptions Add

▼ Select... × Refresh

Create VPN Topology

Topology Name *
HUB-Spoke-VPN-Single-ISP

VPN Type

SD-WAN Topology New
Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.
Select VPN Topology
☒ Hub and Spoke
[Prerequisites](#)

Route-Based VPN
Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.
Select VPN Topology
☐ Hub and Spoke
☐ Peer to Peer

Policy-Based VPN
Secures traffic between peers based on a static policy using protected networks.
Select VPN Topology
☐ Hub and Spoke
☐ Peer to Peer
☐ Full Mesh

SASE Topology
⚠️ SASE Topology cannot be selected because Cisco Umbrella Connection is not configured.
[Prerequisites](#)
[Refresh](#)

[Cancel](#) [Create](#)

- Voeg een hub toe en maak een DVTI aan het einde van de hub. Als onderdeel van de DVTI-configuratie moet u ervoor zorgen dat u de juiste tunnelbroninterface selecteert volgens de topologie.

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy admin

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

2 Spokes

3 Authentication

4 SD-WAN Setup

Next

Add Hub

Device * ftd1

Dynamic Virtual Tunnel Interface (DVTI) * VPN-OUT-1_dynamic_vti_1
Tunnel Source: VPN-OUT-1 (IP Address: 203.0.113.1)

Hub Gateway IP Address 203.0.113.1

Spoke Tunnel IP Address Pool * Select...

Cancel Add

Edit Virtual Tunnel Interface

General

Tunnel Type
☐ Static ☒ Dynamic

Name: * VPN-OUT-1_dynamic_vti_1

☒ Enabled

Description:

Security Zone: VPN-OUT-1

Virtual Tunnel Interface Details
An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Template ID: * 1 (1 - 10413)

Tunnel Source: GigabitEthernet0/0 (VPN-OUT-1) 203.0.113.1

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
☒ Borrow IP (IP unnumbered) Loopback1 (VPN-Loopback-IB...)

VPN Topology Usage

Cancel OK

- Maak een Spoke Tunnel IP-adressengroep aan en klik op Opslaan en vervolgens op Toevoegen. De IP-adrespool wordt gebruikt om VTI-tunnel IP-adressen toe te wijzen aan de spaken.

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 11 ⚙️ ? admin ▾

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

Add Hub

Device * 📘
ftd1

Dynamic Virtual Tunnel Interface (DVTI) * 📘
VPN-OUT-1_dynamic_vti_1
Tunnel Source: VPN-OUT-1 (IP Address: 203.0.113.1)

Hub Gateway IP Address 📘
203.0.113.1

Spoke Tunnel IP Address Pool *
Select... ▾

Cancel Add

Add IPv4 Pool

Name*
VPN-POOL-198.51.100.0

Description

IPv4 Address Range*
198.51.100.10-198.51.100.20
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*
255.255.255.0

☐ Allow Overrides

📘 Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

Cancel Save

3 Authentication Settings 📘

4 SD-WAN Settings

Cancel Finish

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 11 ⚙️ ? admin ▾

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs 📘

Device	Dynamic Virtual Tunnel Interface (DVTI)	Hub Gateway IP Address	Spoke Tunnel IP Address Pool	
ftd1 Threat Defense	Virtual-Template1 (VPN-OUT-1_dynamic_vti_1) Source:GigabitEthernet0/0 (VPN-OUT-1)	203.0.113.1	VPN-POOL-198.51.100.0 Range: 198.51.100.10-198.51.100.20	Add Hub

Next

2 Spokes 📘 Edit

3 Authentication Settings 📘 Edit

4 SD-WAN Settings Edit

Cancel Finish

- Klik op Volgende om verder te gaan en de spaken toe te voegen. U kunt gebruikmaken van beide opties voor bulkopvoeging als u gemeenschappelijke interface- / zonenamen hebt of

spaken afzonderlijk toevoegt.

FMC
Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 13 ⚙️ ? | admin ▾

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs ⓘ
Device ftd1 DVTI VPN-OUT-1_dynamic_vti_1 Gateway IP Address 203.0.113.1 Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.0
2 Spokes ⓘ
View Generated Tunnel Interfaces **Add Spokes (Bulk Addition)** Add Spoke
No spokes are configured. Add a spoke.

Next
3 Authentication Settings ⓘ
4 SD-WAN Settings

Cancel Finish

- Selecteer de apparaten en geef een naamgevingspatroon op voor de WAN/outside-interface. Als de apparaten dezelfde interfacenaam delen, volstaat het gebruik van initialen. Klik op Volgende en klik op Toevoegen als de validatie is geslaagd. Voor bulktoevoegingen kunt u de zonenaam ook op dezelfde manier gebruiken.

FMC
Site To Site

OverviewAnalysisPolicies**Devices**ObjectsIntegration

Deploy 🔍 11 ⚙️ ? admin ▾

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device ftd1 DVTI VPN-OUT-1_dynamic_vti_1 Gateway IP Address 203.0.113.1 Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.0

2 Spokes

Next

3 Authentication Settings

4 SD-WAN Settings

Spokes (Bulk Addition)

Add Spoke

Edit

Edit

Cancel

Finish

1 Add Devices

2 Validate Devices

Available Devices *

Add

Remove

Selected Devices *

ftd2

ftd3

ftd4

Select VPN Interface Using *

☒ Interface Name Pattern

☐ Security Zone

Select...

+

Cancel

Next

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 1 2 3 4 admin

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs Edit

Device ftd1 DVTI VPN-OUT-1_dynamic_vti_1 Gateway IP Address 203.0.113.1 Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.0

2 Spokes

1 Add Devices

2 Validate Devices

✓ Device Name: ftd2, Interface Name: VPN-OUT-1

✓ Device Name: ftd3, Interface Name: VPN-OUT-1

✓ Device Name: ftd4, Interface Name: VPN-OUT-4

Spokes (Bulk Addition) Add Spoke

Next

3 Authentication Settings Edit

4 SD-WAN Settings Edit

Cancel Back Add

Cancel Finish

- Controleer de spaken en de details van de overlay-interface om er zeker van te zijn dat de juiste interfaces zijn geselecteerd en klik vervolgens op Volgende.

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Edit

Device ftd1 DVTI VPN-OUT-1_dynamic_vti_1 Gateway IP Address 203.0.113.1 Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.0

2 Spokes

View Generated Tunnel Interfaces

Add Spokes (Bulk Addition)

Add Spoke

Device	VPN Interface	Local Tunnel (IKE) Identity	
ftd2 Threat Defense	VPN-OUT-1 (GigabitEthernet0/0) IP Address:203.0.113.2	Type: Key ID Value: HUB-Spoke-VPN-Single-ISP_ftd2	 
ftd3 Threat Defense	VPN-OUT-1 (GigabitEthernet0/0) IP Address:203.0.113.3	Type: Key ID Value: HUB-Spoke-VPN-Single-ISP_ftd3	 
ftd4 Threat Defense	VPN-OUT-4 (GigabitEthernet0/0) IP Address:203.0.113.4	Type: Key ID Value: HUB-Spoke-VPN-Single-ISP_ftd4	 

Next

<<

Viewing 1-3 of 3

>>

3 Authentication Settings

Edit

4 SD-WAN Settings

Edit

Cancel

Finish

- U kunt de standaardparameters voor de IPsec-configuratie behouden of aangepaste cijfers opgeven zoals vereist. Klik op Volgende om verder te gaan. In dit document gebruikt u de standaardparameters.

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

[Edit](#)

Device	ftd1	DVTI	VPN-OUT-1_dynamic_vti_1	Gateway IP Address	203.0.113.1	Spoke Tunnel IP Address Pool	VPN-POOL-198.51.100.0
--------	------	------	-------------------------	--------------------	-------------	------------------------------	-----------------------

2 Spokes

[Edit](#)

Device	ftd2	VPN Interface	VPN-OUT-1	Local Tunnel (IKE) Identity	Key ID: HUB-Spoke-VPN-Single-ISP_ftd2
	ftd3	VPN Interface	VPN-OUT-1		Key ID: HUB-Spoke-VPN-Single-ISP_ftd3
	ftd4	VPN Interface	VPN-OUT-4		Key ID: HUB-Spoke-VPN-Single-ISP_ftd4

3 Authentication Settings

Authentication Type*

Pre-shared Automatic Key

Transform Sets (IPsec Proposals)*

AES-GCM x

[Show Details](#)

IKEv2 Policies*

AES-GCM-NUL-SSH-LATEST x

[Show Details](#)

Pre-shared Key Length*

24 The range is 1 to 127.

Next

4 SD-WAN Settings

[Edit](#)

Cancel

Finish

- Ten slotte kunt u overlay-routing configureren binnen dezelfde wizard voor deze topologie door de juiste BGP-parameters op te geven, zoals het AS-nummer, interfacereclame en communitytags voor prefix-filtering. Beveiligingszone kan helpen bij het filteren van verkeer via toegangscontrolebeleid, terwijl u ook een object voor interfaces kunt maken en deze kunt gebruiken in gekoppelde interfaces voor herverdeling als de naam anders is dan binnen of niet symmetrisch is tussen apparaten in de topologie.

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device ftd1 DVTI VPN-OUT-1_dynamic_vti_1 Gateway IP Address 203.0.113.1 Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.32

Edit

2 Spokes

ftd2 VPN-OUT-1

ftd3 VPN-OUT-1

ftd4 VPN-OUT-4

VPN Interface

Local Tunnel (IKE) Identity

Key ID: HUB-Spoke-VPN-Single-ISP_ftd2

Key ID: HUB-Spoke-VPN-Single-ISP_ftd3

Key ID: HUB-Spoke-VPN-Single-ISP_ftd4

Edit

3 Authentication Settings

Authentication Pre-shared Automatic Key Pre-shared Key Length 24

Edit

4 SD-WAN Settings

Spoke Tunnel Interface Auto Generation

Static Virtual Tunnel Interfaces (SVTIs) are auto generated on each spoke using the spoke's VPN interface as tunnel source to establish a VPN to the DVTI on each of the hubs. [View more](#)

Spoke Tunnel Interface Security Zone

VPN-OUT-1

+

Overlay Routing Configuration

BGP can be enabled on the VPN overlay topology for seamless VPN connectivity from the spokes to the hub, and for spoke-to-spoke connectivity via the hub. [View more](#)

☒ Enable BGP on the VPN Overlay Topology

Autonomous System Number *

65500

Community Tag for Local Routes *

101010

☒ Redistribute Connected Interfaces

Default inside*

+

☒ Enable Multiple Paths for BGP

Allows multiple BGP routes to be used at the same time to reach the same destination. Enables BGP to load-balance traffic across multiple links.

Next

You have unsaved changes

Cancel

Finish

- Klik op Volgende, vervolgens op Voltooien en ten slotte op Implementeren om het proces te voltooien.

Verificatie

- U kunt de tunnelstatus controleren door te navigeren naar Apparaten > VPN > Site to Site.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ? admin ▾

Last Updated: 12:06 PM Refresh NAT Exemptions Add

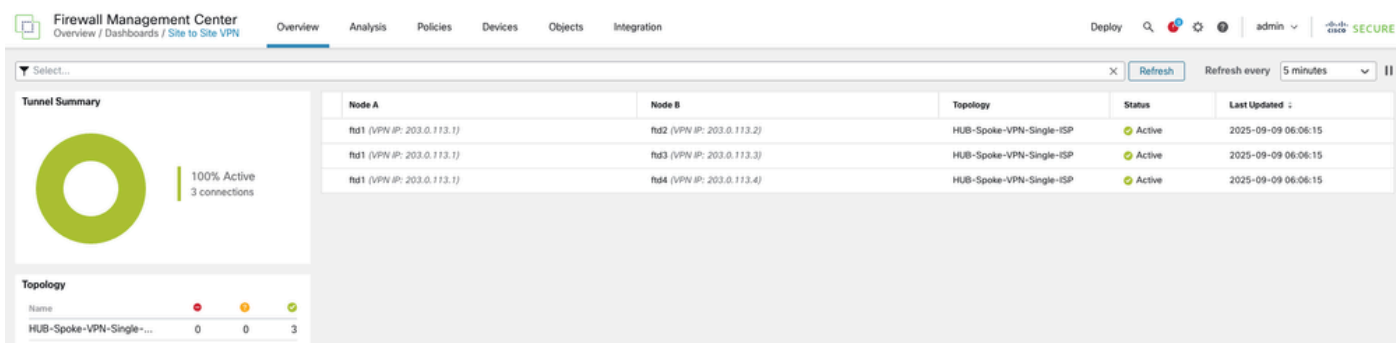
Select...

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
HUB-Spoke-VPN-Single-ISP	Route Based (VTI)	SD-WAN Topology	3 Tunnels	✓	

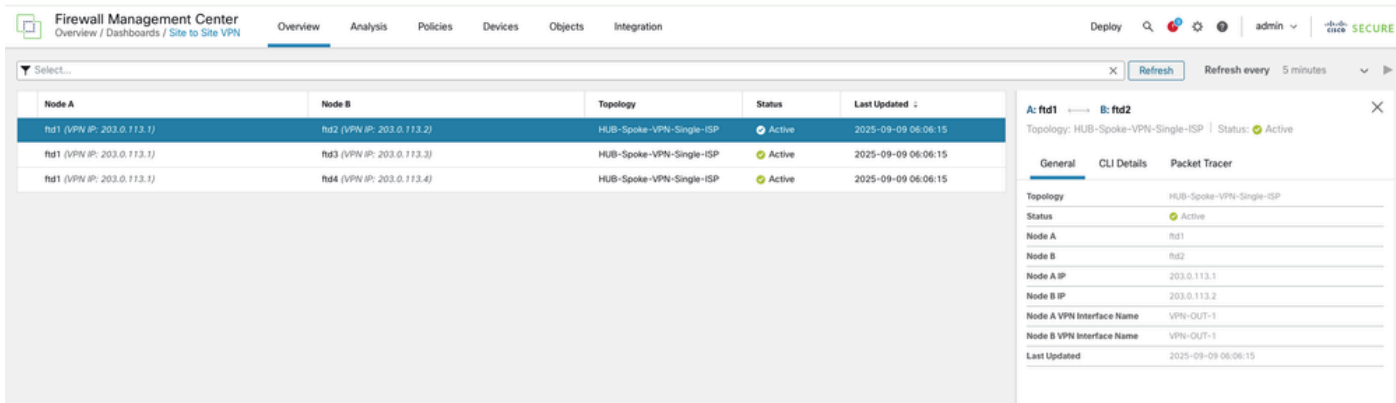
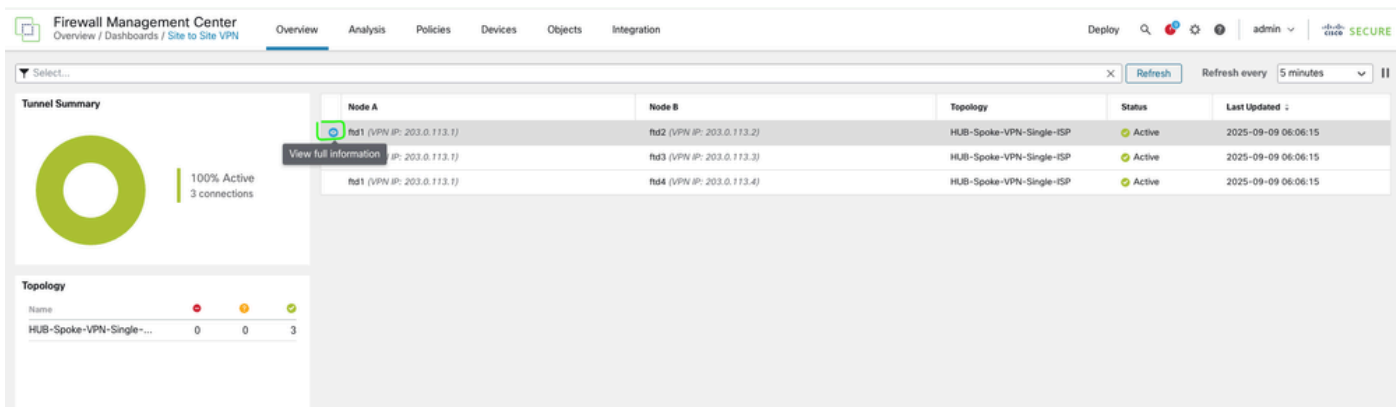
Hub			Spoke		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynamic... (10.18.89.254)	ftd2	VPN-OUT-1 (203.0.113.2)	VPN-OUT-1_static... (198.51.100.10)
ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynamic... (10.18.89.254)	ftd3	VPN-OUT-1 (203.0.113.3)	VPN-OUT-1_static... (198.51.100.11)
ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynamic... (10.18.89.254)	ftd4	VPN-OUT-4 (203.0.113.4)	VPN-OUT-4_static... (198.51.100.12)

Viewing 1-3 of 3

- Aanvullende details kunnen worden geverifieerd door te navigeren naar Overzicht > Dashboards > Site to Site VPN.



- Selecteer de tunnel en klik op Volledige informatie bekijken voor meer informatie.



Firewall Management Center
Overview / Dashboards / Site to Site VPN

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Select...

Node A	Node B	Topology	Status	Last Updated
ftd1 (VPN IP: 203.0.113.1)	ftd2 (VPN IP: 203.0.113.2)	HUB-Spoke-VPN-Singl...	Active	2025-09-09 06:06:15
ftd1 (VPN IP: 203.0.113.1)	ftd3 (VPN IP: 203.0.113.3)	HUB-Spoke-VPN-Singl...	Active	2025-09-09 06:06:15
ftd1 (VPN IP: 203.0.113.1)	ftd4 (VPN IP: 203.0.113.4)	HUB-Spoke-VPN-Singl...	Active	2025-09-09 06:06:15

Refresh Refresh every 5 minutes

A: ftd1 ↔ B: ftd2
Topology: HUB-Spoke-VPN-Single-ISP | Status: Active

General CLI Details Packet Tracer

Refresh Maximize view

Summary

Node A (203.0.113.1/500)	Node B (203.0.113.2/500)
Transmitted: 9.52 KB (9744 B)	Transmitted: 9.26 KB (9481 B)
Received: 12.33 KB (12628 B)	Received: 12.61 KB (12912 B)

IPsec Security Associations (1)

0.0.0.0/0.0.0.0/0 0.0.0.0/0.0.0.0/0

```

ftd1 (VPN Interface IP: 203.0.113.1)
show crypto ipsec sa peer 203.0.113.2
peer address: 203.0.113.2
interface: VPN-OUT-1_dynamic_vti_1_va9
Crypto map tag: VPN-OUT-1_dynamic_vti_1_vtemplate_dyn_map, seq num: 1, local addr: 203.0.113.1

Protected vrf (jvrf): 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: 203.0.113.2

#pkts encaps: 155, #pkts encrypt: 155, #pkts digest: 155
#pkts decaps: 154, #pkts decrypt: 154, #pkts verify: 154
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 155, #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 not offload decrypted: 154

ftd2 (VPN Interface IP: 203.0.113.2)
show crypto ipsec sa peer 203.0.113.1
peer address: 203.0.113.1
interface: VPN-OUT-1_static_vti_1
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 203.0.113.2

Protected vrf (jvrf): 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: 203.0.113.1

```

Viewing 1-3 of 3

- De uitvoer wordt rechtstreeks weergegeven vanuit de FTD CLI en kan worden vernieuwd om bijgewerkte tellers en belangrijke informatie weer te geven, zoals details van de Security Parameter Index (SPI).

Tunnel Details	
Summary	
Node A (203.0.113.1/500)	Node B (203.0.113.2/500)
Transmitted: 9.52 KB (9744 B)	Transmitted: 9.26 KB (9481 B)
Received: 12.33 KB (12628 B)	Received: 12.61 KB (12912 B)
IPsec Security Associations (1)	
0.0.0.0/0.0.0.0/0/0	0.0.0.0/0.0.0.0/0/0
ftd1 (VPN Interface IP: 203.0.113.1) show crypto ipsec sa peer 203.0.113.2 peer address: 203.0.113.2 interface: VPN-OUT-1_dynamic_vti_1_va9 Crypto map tag: VPN-OUT-1_dynamic_vti_1_vtemplate_dyn_map, seq num: 1 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: 203.0.113.2 #pkts encaps: 155, #pkts encrypt: 155, #pkts digest: 155 #pkts decaps: 154, #pkts decrypt: 154, #pkts verify: 154 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 155, #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 not offload decrypted: 154 #send errors: 0, #recv errors: 0 local crypto endpt.: 203.0.113.1/500, remote crypto endpt.: 203.0.113.2/500 path mtu 1500, ipsec overhead 55(36), media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: 3EE69843 current inbound spi : D113FBF4 inbound esp sas: spi: 0xD113FBF4 (3507747828) SA State: active transform: esp-aes-gcm-256 esp-null-hmac no compression in use settings = {L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 9, crypto-map: VPN-OUT-1_dynamic_vti_1_vtemplate_dyn_map sa timing: remaining key lifetime (sec): 24309	ftd2 (VPN Interface IP: 203.0.113.2) show crypto ipsec sa peer 203.0.113.1 peer address: 203.0.113.1 interface: VPN-OUT-1_static_vti_1 Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) 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: 203.0.113.1 #pkts encaps: 154, #pkts encrypt: 154, #pkts digest: 154 #pkts decaps: 155, #pkts decrypt: 155, #pkts verify: 155 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 154, #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 not offload decrypted: 155 #send errors: 0, #recv errors: 0 local crypto endpt.: 203.0.113.2/500, remote crypto endpt.: 203.0.113.1/500 path mtu 1500, ipsec overhead 55(36), media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: D113FBF4 current inbound spi : 3EE69843 inbound esp sas: spi: 0x3EE69843 (1055299651) SA State: active transform: esp-aes-gcm-256 esp-null-hmac no compression in use settings = {L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa timing: remaining key lifetime (sec): 24308

Close Refresh

- De FTD CLI kan ook worden gebruikt om routeringsinformatie en de BGP-peering-status te controleren.

Aan de HUB-zijde

</root>

HUB1# show bgp summary

```
BGP router identifier 198.51.100.3, local AS number 65500
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
```

1/1 BGP path/bestpath attribute entries using 208 bytes of memory
 1 BGP community entries using 24 bytes of memory
 1 BGP route-map cache entries using 64 bytes of memory
 0 BGP filter-list cache entries using 0 bytes of memory
 BGP using 856 total bytes of memory
 BGP activity 2/0 prefixes, 4/2 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
198.51.100.10	4	65500	4	6	7	0	0	00:00:45	0

<<<< spoke 1 bgp peering

198.51.100.11	4	65500	5	5	7	0	0	00:00:44	1
---------------	---	-------	---	---	---	---	---	----------	---

<<<< spoke 2 bgp peering

198.51.100.12	4	65500	5	5	7	0	0	00:00:52	1
---------------	---	-------	---	---	---	---	---	----------	---

<<<< spoke 3 bgp peering

<#root>

HUB1# 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 not set

B 192.0.2.0 255.255.255.248 [200/1] via 198.51.100.10, 00:00:18

<<<<<<< spoke 1 inside network

B 192.0.2.8 255.255.255.248 [200/1] via 198.51.100.11, 00:08:08

<<<<<<< spoke 2 inside network

B 192.0.2.16 255.255.255.248 [200/1] via 198.51.100.12, 00:08:16

<<<<<<< spoke 3 inside network

<#root>

HUB1#show bgp ipv4 unicast neighbors 198.51.100.10 routes

<<<< to check only prefix received from specific peer

BGP table version is 14, local router ID is 198.51.100.3
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
 r RIB-failure, S Stale, m multipath

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i192.0.2.0/29	198.51.100.10	1	100	0	?

<<<<<<<< routes received from spoke 1

Total number of prefixes 1

<#root>

HUB1#show bgp ipv4 unicast neighbors 198.51.100.11 routes

<<<<< to check only prefix received from specific peer

BGP table version is 14, local router ID is 198.51.100.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i192.0.2.8/29	198.51.100.11	1	100	0	?

<<<<<<<< routes received from spoke 2

Total number of prefixes 1

<#root>

HUB1#show bgp ipv4 unicast neighbors 198.51.100.12 routes

<<<<< to check only prefix received from specific peer

BGP table version is 14, local router ID is 198.51.100.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i192.0.2.16/29	198.51.100.12	1	100	0	?

<<<<<<<< routes received from spoke 3

Total number of prefixes 1

aan de spraakzijde

Dezelfde verificatie kan ook worden uitgevoerd op de spaakapparaten. Hier is een voorbeeld van een van de sprekers.

<#root>

Spoke1# show bgp summary

BGP router identifier 198.51.100.4, local AS number 65500
BGP table version is 12, main routing table version 12
3 network entries using 600 bytes of memory
3 path entries using 240 bytes of memory
2/2 BGP path/bestpath attribute entries using 416 bytes of memory
2 BGP rrinfo entries using 80 bytes of memory
1 BGP community entries using 24 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 1360 total bytes of memory
BGP activity 5/2 prefixes, 7/4 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
198.51.100.1	4	65500	12	11	12	0	0	00:07:11	2

<<<<<<<< BGP peering with HUB

<#root>

Spoke1# show bgp ipv4 unicast neighbors 198.51.100.1 routes

BGP table version is 12, local router ID is 198.51.100.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i192.0.2.8/29	198.51.100.1	1	100	0	?

<<<<<<< route received from HUB for spoke 2

*>i192.0.2.16/29	198.51.100.1	1	100	0	?
------------------	--------------	---	-----	---	---

<<<<<<< route received from HUB for spoke 3

Total number of prefixes 2

<#root>

Spoke1# show bgp ipv4 unicast neighbors 198.51.100.1 advertised-routes

BGP table version is 12, local router ID is 198.51.100.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 192.0.2.0/29	0.0.0.0	0		32768	?

<<<<<<< route advertised by this spoke into BGP

Total number of prefixes 1

<#root>

Spoke1# 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 not set

B 192.0.2.8 255.255.255.248 [200/1] via 198.51.100.1, 00:13:42

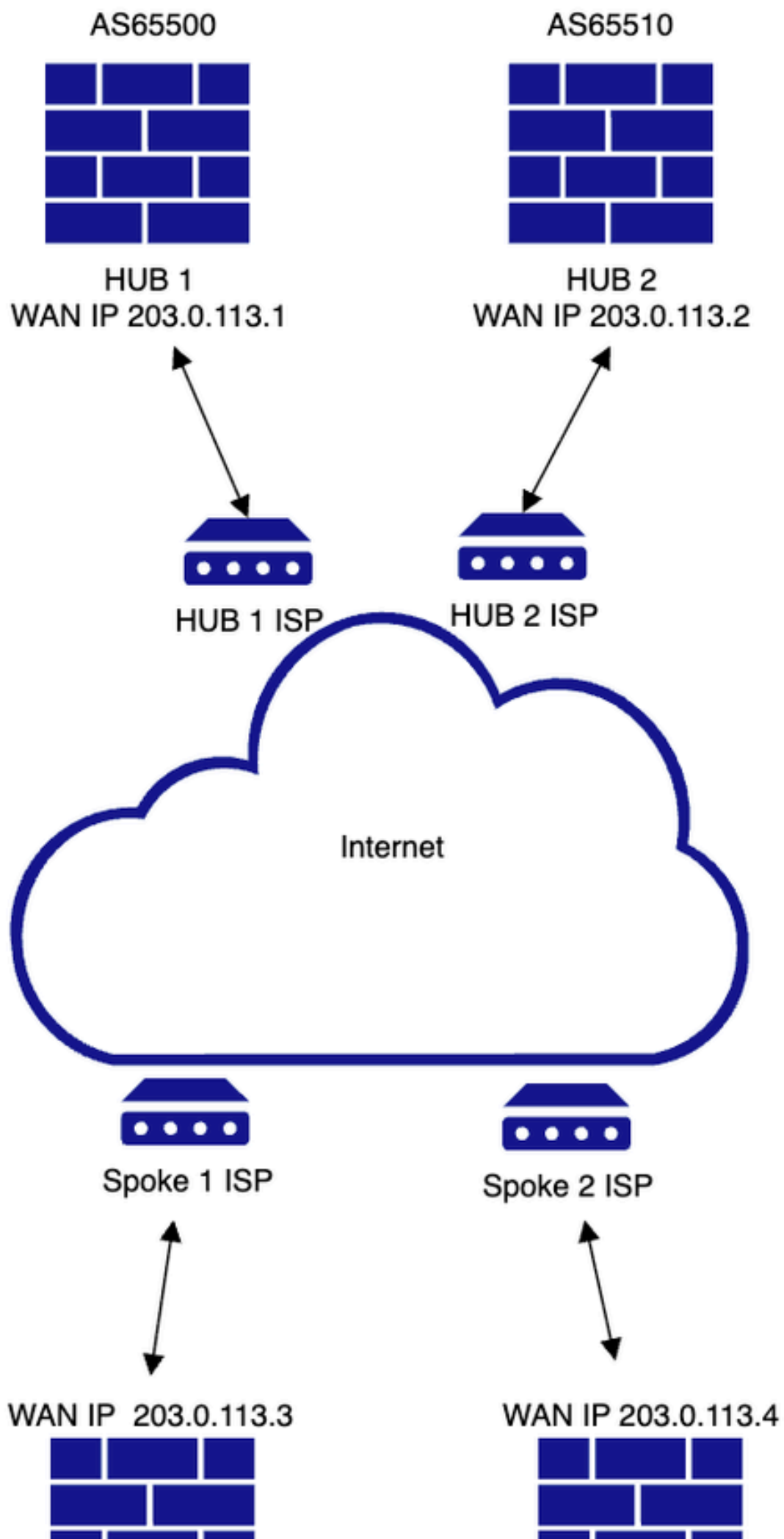
<<<<<<< spoke 2 inside network

B 192.0.2.16 255.255.255.248 [200/1] via 198.51.100.1, 00:13:42

<<<<<<< spoke 3 inside network

Dual HUB & Spoke (één ISP voor redundante HUB via EBGP tussen secundaire HUB en Spokes)

Netwerkdigram



Nadat u de eerste HUB hebt toegevoegd, gaat u verder met het toevoegen van de tweede HUB met behulp van dezelfde stappen die eerder voor HUB1 zijn gebruikt.

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 3 ⚙️ ? admin ▾

Dual-HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Add Hub

Device	Dynamic Virtual Tunnel Interface (DVTI)	Hub Gateway IP Address	Spoke Tunnel IP Address Pool
ftd1 Threat Defense	Virtual-Template1 (VPN-OUT-1_dynamic_vti_1) Source:GigabitEthernet0/0 (VPN-OUT-1)	203.0.113.1	VPN-POOL-198.51.100.0 Range: 198.51.100.10-198.51.100.1

Next

- Ga verder met het maken van de Dynamic Virtual Tunnel Interface (DVTI).

Firewall Management Center Devices / VPN / Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 3 ⚙️ ? admin ▾

Dual-HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Add Hub

Add Virtual Tunnel Interface

Add Loopback Interface

- Voor HUB 2 VTI-tunnels aan de spaakzijde is een nieuwe IP-adrespool vereist. Maak en configureer de nieuwe groep en sla de wijzigingen vervolgens op.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⌂ admin ✓ cisco SECURE

Dual-HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device	Dynamic Virtual Tunnel Interface (DVTI)	Hub Gateway IP Address	Spoke Tunnel IP Address Pool
ftd1 Threat Defense	Virtual-Template1 (VPN-OUT-1_dynamic_vti_1) Source: GigabitEthernet0/0 (VPN-OUT-1)	203.0.113.1	VPN-POOL-198.51.100.0 Range: 198.51.100.10-198.51.100.20

Next

2 Spokes

Device ftd3 VPN Interface VPN-OUT-1 Local Tunnel (IKE Identity

3 Authentication Settings

Authentication Pre-shared Automatic Key Pre-shared Key Length

4 SD-WAN Settings

BGP on Overlay Enabled
Hubs and spokes are configured with internal BGP and AS number

Add Hub

Device *
ftd2

Dynamic Virtual Tunnel Interface (DVTI) *
VPN-OUT-1_dynamic_vti_1
Tunnel Source: VPN-OUT-1 (IP Address: 203.0.113.2)

Hub Gateway IP Address
203.0.113.2

Spoke Tunnel IP Address Pool *
VPN-POOL-198.51.100.32

Cancel Add

Cancel Finish

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⌂ admin ✓ cisco SECURE

Dual-HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device	Dynamic Virtual Tunnel Interface (DVTI)	Hub Gateway IP Address	Spoke Tunnel IP Address Pool
ftd1 Threat Defense	Virtual-Template1 (VPN-OUT-1_dynamic_vti_1) Source: GigabitEthernet0/0 (VPN-OUT-1)	203.0.113.1	VPN-POOL-198.51.100.0 Range: 198.51.100.10-198.51.100.20
ftd2 Threat Defense	Virtual-Template1 (VPN-OUT-1_dynamic_vti_1) Source: GigabitEthernet0/0 (VPN-OUT-1)	203.0.113.2	VPN-POOL-198.51.100.32 Range: 198.51.100.40-198.51.100.50

Next

2 Spokes

Device ftd3 VPN Interface VPN-OUT-1 Local Tunnel (IKE Identity Key ID: HUB-Spoke-VPN-Single-ISP_ftd3

Device ftd4 VPN Interface VPN-OUT-4 Local Tunnel (IKE Identity Key ID: HUB-Spoke-VPN-Single-ISP_ftd4

3 Authentication Settings

Authentication Pre-shared Automatic Key Pre-shared Key Length 24

4 SD-WAN Settings

BGP on Overlay Enabled
Hubs and spokes are configured with internal BGP and AS number 65500.

Cancel Finish

- Als u eBGP-peering tussen de tweede HUB en de spaken wilt configureren, wijzigt u de SD-WAN-instellingen in de laatste stap. Schakel de optie Secundaire HUB is in een ander autonoom systeem en geef het nummer van het autonome systeem (AS) voor de secundaire HUB. IBGP kan ook worden gebruikt als er geen beperking is voor het gebruik van een ander AS-nummer in uw omgeving door de optie Secundaire HUB in een ander autonoom systeem niet aan te vinken. Hierdoor worden dezelfde communitytag en hetzelfde AS-nummer ook voor secundaire HUB gebruikt. Het artikel richt zich op eBGP voor de huidige setup.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⚙️ admin ▾ **SECURE**

Dual-HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device ftd1 ftd2
DVTI VPN-OUT-1_dynamic_vti_1
Gateway IP Address 203.0.113.1 203.0.113.2
Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.0 VPN-POOL-198.51.100.32

Edit

2 Spokes

Device ftd3 ftd4
VPN Interface VPN-OUT-1 VPN-OUT-4
Local Tunnel (IKE) Identity Key ID: HUB-Spoke-VPN-Single-ISP_ftd3
Key ID: HUB-Spoke-VPN-Single-ISP_ftd4

Edit

3 Authentication Settings

Authentication Pre-shared Automatic Key Pre-shared Key Length 24

Edit

4 SD-WAN Settings

Spoke Tunnel Interface Auto Generation

Static Virtual Tunnel Interfaces (SVTIs) are auto generated on each spoke using the spoke's VPN interface as tunnel source to establish a VPN to the DVTI on each of the hubs. [View more](#)

Spoke Tunnel Interface Security Zone

VPN-OUT-1 x v +

Overlay Routing Configuration

BGP can be enabled on the VPN overlay topology for seamless VPN connectivity from the spokes to the hub, and for spoke-to-spoke connectivity via the hub. [View more](#)

☒ Enable BGP on the VPN Overlay Topology

Autonomous System Number * 65500 Community Tag for Local Routes * 101010

☒ Redistribute Connected Interfaces

Default inside* v +

☒ Secondary Hub is in different Autonomous System

Autonomous System Number * 65510 Community Tag for Learned Routes * 010101

☒ Enable Multiple Paths for BGP

Allows multiple BGP routes to be used at the same time to reach the same destination. Enables BGP to load-balance traffic across multiple links.

Next You have unsaved changes

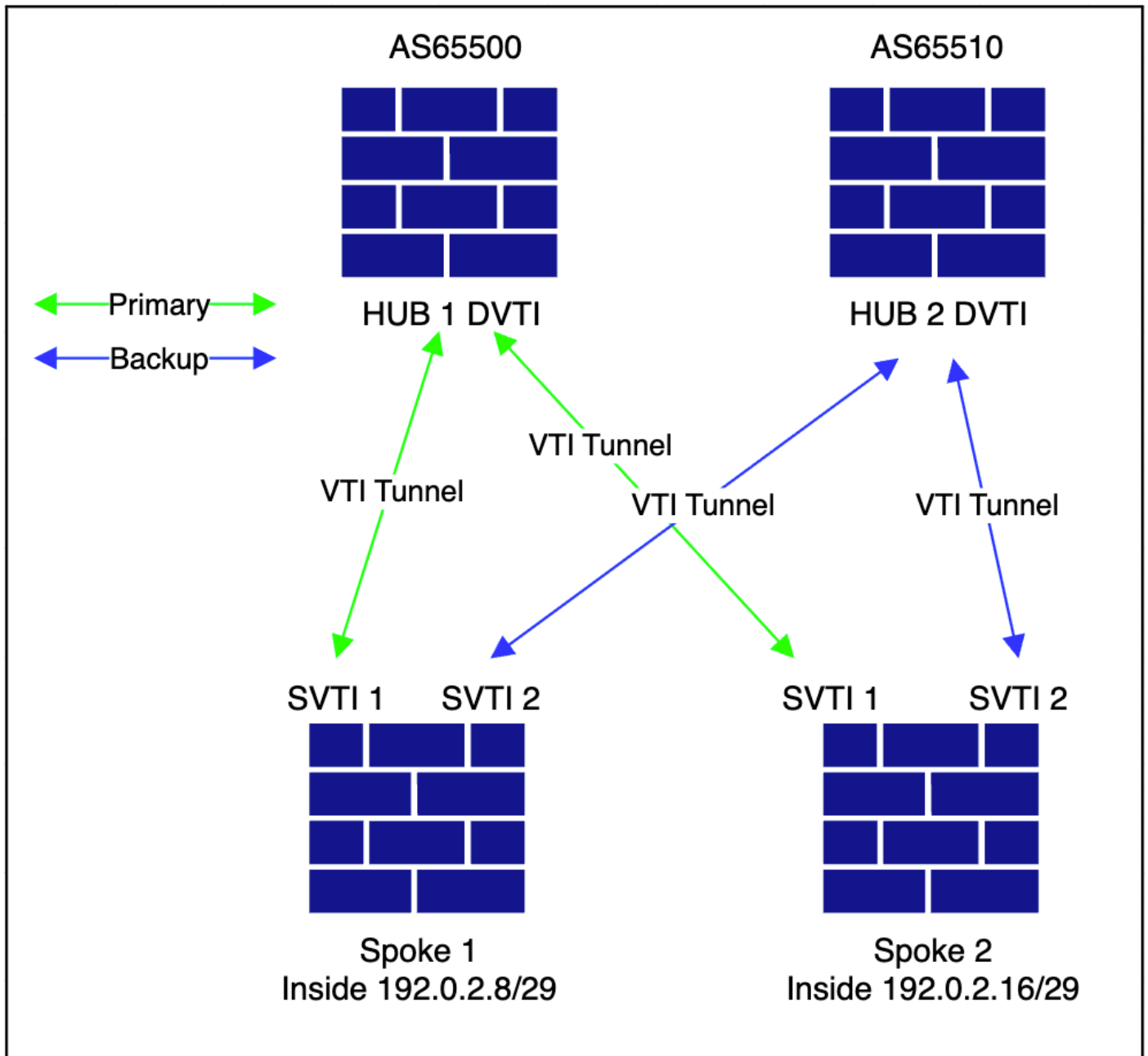
Cancel

Finish

Zorg ervoor dat zowel het AS-nummer (Autonomous System) als het communitylabel uniek zijn in deze configuratie.

Verificatie

Dit diagram illustreert de overlay-topologie.



- Navigeer in de FMC naar Apparaten > VPN > Site to Site.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾ secure

Last Updated: 02:20 PM Refresh NAT Exemptions Add

Select... X Refresh

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
Dual-HUB-Spoke-VPN-Single-ISP	Route Based (VTI)	SD-WAN Topology	4 Tunnels	✓	

Hub			Spoke		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
FTD ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynam... (198.51.100.1)	FTD ftd3	VPN-OUT-1 (203.0.113.3)	VPN-OUT-1_static... (198.51.100.10)
FTD ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynam... (198.51.100.1)	FTD ftd4	VPN-OUT-4 (203.0.113.4)	VPN-OUT-4_static... (198.51.100.11)
FTD ftd2	VPN-OUT-1 (203.0.113.2)	VPN-OUT-1_dynam... (198.51.100.2)	FTD ftd3	VPN-OUT-1 (203.0.113.3)	VPN-OUT-1_static... (198.51.100.40)
FTD ftd2	VPN-OUT-1 (203.0.113.2)	VPN-OUT-1_dynam... (198.51.100.2)	FTD ftd4	VPN-OUT-4 (203.0.113.4)	VPN-OUT-4_static... (198.51.100.41)

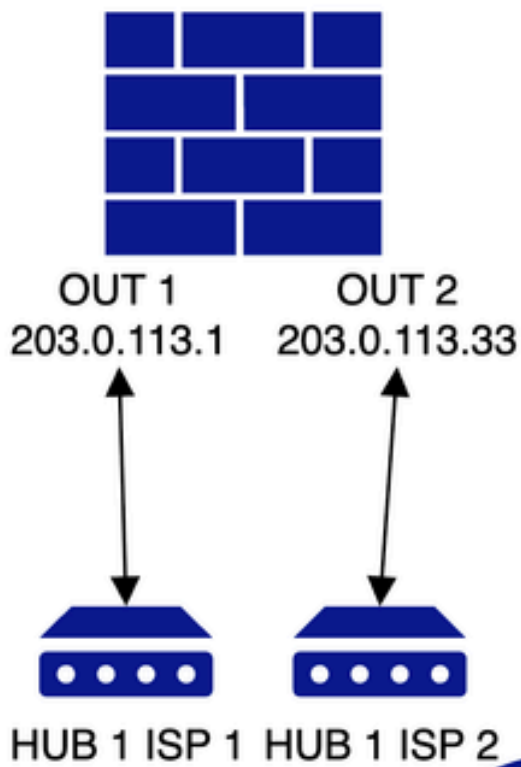
Viewing 1-4 of 4

- Alle andere stappen blijven ongewijzigd.

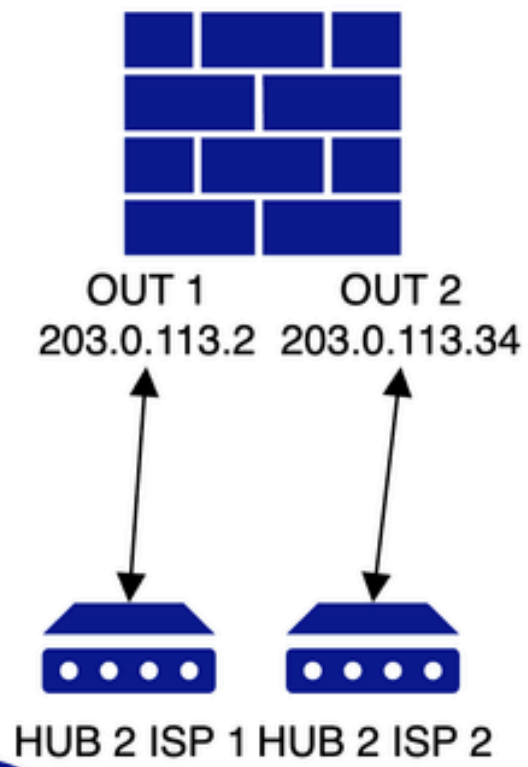
Dual HUB & Spoke (Dual ISP voor redundante HUB en ISP via EBGP tussen
secundaire HUB en Spokes)

Netwerkdigram

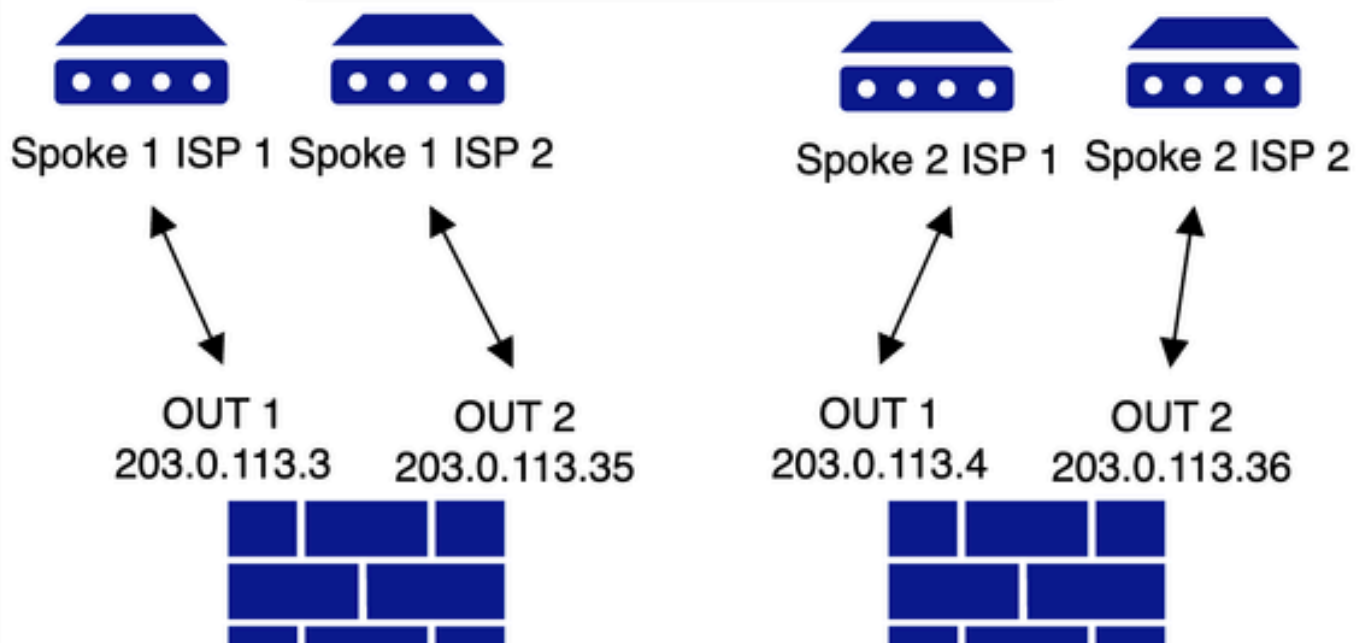
AS65500



AS65510



Internet



De implementatie voor deze topologie wordt overgeslagen met behulp van de eerste ISP. omdat dat wordt behandeld in de vorige topologie.

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
Dual-HUB-Spoke-VPN-Dual-ISP-1	Route Based (VTI)	SD-WAN Topology	4 - Tunnels	✓	
Hub			Spoke		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
FTD ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynamic... (198.51.100.1)	FTD ftd3	VPN-OUT-1 (203.0.113.3)	VPN-OUT-1_static... (198.51.100.10)
FTD ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynamic... (198.51.100.1)	FTD ftd4	VPN-OUT-4 (203.0.113.4)	VPN-OUT-4_static... (198.51.100.11)
FTD ftd2	VPN-OUT-1 (203.0.113.2)	VPN-OUT-1_dynamic... (198.51.100.2)	FTD ftd3	VPN-OUT-1 (203.0.113.3)	VPN-OUT-1_static... (198.51.100.40)
FTD ftd2	VPN-OUT-1 (203.0.113.2)	VPN-OUT-1_dynamic... (198.51.100.2)	FTD ftd4	VPN-OUT-4 (203.0.113.4)	VPN-OUT-4_static... (198.51.100.41)

- Vervolgens gaat u verder met het toevoegen van de tweede topologie door twee extra DVTI-interfaces per HUB te maken, elk met behulp van de onderliggende interface voor ISP 2 (VPN-OUT-2).

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾

Dual-HUB-Spoke-VPN-Dual-ISP-2

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Add Hub

Device * ▾
ftd1

Dynamic Virtual Tunnel Interface (DVTI) * ▾
Select... **+**

Hub Gateway IP Address

Cancel Add

Add Virtual Tunnel Interface

General Path Monitoring

Tunnel Type
☐ Static ☒ Dynamic

Name: *
VPN-OUT-1_dynamic_vti_2

☒ Enabled

Description:

Security 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 VTI.

Template ID: * 2 (1 - 10413)

Tunnel Source:
GigabitEthernet0/1 (VPN-OUT-2) 203.0.113.33

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 169.254.2.1/30 ⓘ
☒ Borrow IP (IP unnumbered) Loopback2 (VPN-2-LOOPBACK...) +

Cancel OK

- Er is een extra VPN IP-adressenpool beschikbaar die specifiek is bedoeld voor gesproken Virtual Tunnel Interface (VTI)-adressen.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾

Dual-HUB-Spoke-VPN-Dual-ISP-2

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs ⓘ

2 Spokes ⓘ

3 Authentication Settings ⓘ

4 SD-WAN Settings

Next

Add Hub

Add Hub ⓘ

Device* ⓘ
ftd1

Dynamic Virtual Tunnel Interface (DVTI)* ⓘ
VPN-OUT-1_dynamic_vti_2
Tunnel Source: VPN-OUT-2 (IP Address: 203.0.113.33)

Hub Gateway IP Address ⓘ
203.0.113.33

Spoke Tunnel IP Address Pool*
VPN-POOL-198.51.100.70

Cancel Add

Cancel Finish

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾

Dual-HUB-Spoke-VPN-Dual-ISP-2

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs ⓘ

2 Spokes ⓘ

3 Authentication Settings ⓘ

4 SD-WAN Settings

Next

Add Hub

Device	Dynamic Virtual Tunnel Interface (DVTI)	Hub Gateway IP Address	Spoke Tunnel IP Address Pool
ftd1 Threat Defense	Virtual-Template2 (VPN-OUT-1_dynamic_vti_2) Source: GigabitEthernet0/1 (VPN-OUT-2)	203.0.113.33	VPN-POOL-198.51.100.70 Range: 198.51.100.70-198.51.100.80

Edit

Edit

Edit

Cancel Finish

- Als u een secundaire hub wilt toevoegen, herhaalt u het proces door DVTI 2 te maken met behulp van de secundaire ISP-interface (VPN-OUT-2) en een extra IP-pool voor gesproken VTI-adressen te configureren.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ⓘ admin

Dual-HUB-Spoke-VPN-Dual-ISP-2

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device	Dynamic Virtual Tunnel Interface (DVTI)
ftd1	Virtual-Template2 (VPN-OUT-1_dynamic_vti_2) Source:GigabitEthernet0/1 (VPN-OUT-2)

2 Spokes

3 Authentication Settings

4 SD-WAN Settings

Add Hub

Device *
ftd2

Dynamic Virtual Tunnel Interface (DVTI) *
Select... +

Hub Gateway IP Address

Cancel Add

Add Virtual Tunnel Interface

General Path Monitoring

Tunnel Type
☐ Static ☒ Dynamic

Name:*
VPN-OUT-1_dynamic_vti_2

☒ Enabled

Description:

Security Zone:
VPN-OUT-2

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 VTI.

Template ID:*
2 (1 - 10413)

Tunnel Source:
GigabitEthernet0/1 (VPN-OUT-2) 203.0.113.34

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 169.254.2.1/30 ⓘ
☒ Borrow IP (IP unnumbered) Loopback2 (VPN-2-LOOPBACK) +

Cancel OK

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ⓘ admin

Dual-HUB-Spoke-VPN-Dual-ISP-2

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device	Dynamic Virtual Tunnel Interface (DVTI)	Hub Gateway IP Address	Spoke Tunnel IP Address Pool
ftd1	Virtual-Template2 (VPN-OUT-1_dynamic_vti_2) Source:GigabitEthernet0/1 (VPN-OUT-2)	203.0.113.34	VPN-POOL-198.51.100.70 Range: 198.51.100.70-198.51.100.80

2 Spokes

3 Authentication Settings

4 SD-WAN Settings

Next

Add Hub

Device *
ftd2

Dynamic Virtual Tunnel Interface (DVTI) *
VPN-OUT-1_dynamic_vti_2 +

Tunnel Source: VPN-OUT-2 (IP Address: 203.0.113.34)

Hub Gateway IP Address
203.0.113.34

Spoke Tunnel IP Address Pool*
VPN-POOL-198.51.100.100 x +

Cancel Add

Cancel Finish

- Zorg er bij het toevoegen van een spaak voor dat de juiste ondervloer / WAN-interface is opgegeven voor de VTI-tunnels. Deze topologie maakt gebruik van de secundaire ISP-

interface VPN-OUT-2.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ? admin

Dual-HUB-Spoke-VPN-Dual-ISP-2

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device ftd1
ftd2 DVTI VPN-OUT-1_dynamic_vti_2
VPN-OUT-1_dynamic_vti_2 Gateway IP Address 203.0.113.33
203.0.113.34 Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.70
VPN-POOL-198.51.100.100

2 Spokes

Add Bulk Spokes

1 Add Devices

2 Validate Devices

✓ Device Name: ftd3, Interface Name: VPN-OUT-2
✓ Device Name: ftd4, Interface Name: VPN-OUT-2

Cancel Back Add

Spokes (Bulk Addition) Add Spoke

Next

3 Authentication Settings

4 SD-WAN Settings

Edit Edit

Cancel Finish

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ? admin

Dual-HUB-Spoke-VPN-Dual-ISP-2

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device ftd1
ftd2 DVTI VPN-OUT-1_dynamic_vti_2
VPN-OUT-1_dynamic_vti_2 Gateway IP Address 203.0.113.33
203.0.113.34 Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.70
VPN-POOL-198.51.100.100

2 Spokes

View Generated Tunnel Interfaces

Add Spokes (Bulk Addition) Add Spoke

Device	VPN Interface	Local Tunnel (IKE) Identity
ftd3 Threat Defense	VPN-OUT-2 (GigabitEthernet0/1) IP Address:203.0.113.35	Type: Key ID Value: Dual-HUB-Spoke-VPN-Dual-ISP-2_ftd3
ftd4 Threat Defense	VPN-OUT-2 (GigabitEthernet0/1) IP Address:203.0.113.36	Type: Key ID Value: Dual-HUB-Spoke-VPN-Dual-ISP-2_ftd4

Next

3 Authentication Settings

4 SD-WAN Settings

Edit Edit

Cancel Finish

Viewing 1-2 of 2

- Zorg er bij het configureren van routing voor dat de communitytags en AS-nummers voor beide HUB's in deze topologie consistent zijn met de tags en AS-nummers die in de vorige ISP1-topologie zijn gebruikt. De topologie gebruikt verschillende beveiligingszones, maar de resterende configuraties zoals AS-nummers voor primaire en secundaire HUB's en community-tags zijn hetzelfde. Dit is verplicht voor de gebruikersinterface om de topologievalidatie te voltooien.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾

Dual-HUB-Spoke-VPN-Dual-ISP-2

Hub and Spoke Route-Based (VTI) VPN Topology

- Hubs** Edit

Device	DVTI	Gateway IP Address	Spoke Tunnel IP Address Pool
ftd1	VPN-OUT-1_dynamic_vti_2	203.0.113.33	VPN-POOL-198.51.100.70
ftd2	VPN-OUT-1_dynamic_vti_2	203.0.113.34	VPN-POOL-198.51.100.100
- Spokes** Edit

Device	VPN Interface	Local Tunnel (IKE) Identity	Key ID
ftd3	VPN-OUT-2	VPN-OUT-2	Dual-HUB-Spoke-VPN-Dual-ISP-2_ftd3
ftd4	VPN-OUT-2	VPN-OUT-2	Dual-HUB-Spoke-VPN-Dual-ISP-2_ftd4
- Authentication Settings** Edit

Authentication: Pre-shared Automatic Key Pre-shared Key Length: 24
- SD-WAN Settings**

Spoke Tunnel Interface Auto Generation
Static Virtual Tunnel Interfaces (SVTIs) are auto generated on each spoke using the spoke's VPN interface as tunnel source to establish a VPN to the DVTI on each of the hubs. [View more](#)

Spoke Tunnel Interface Security Zone
VPN-OUT-2

Overlay Routing Configuration
BGP can be enabled on the VPN overlay topology for seamless VPN connectivity from the spokes to the hub, and for spoke-to-spoke connectivity via the hub. [View more](#)

☒ **Enable BGP on the VPN Overlay Topology**

Autonomous System Number * 65500 Community Tag for Local Routes * 101010

☒ **Redistribute Connected Interfaces**
Default inside*

☒ **Secondary Hub is in different Autonomous System**

Autonomous System Number * 65510 Community Tag for Learned Routes * 010101

☒ **Enable Multiple Paths for BGP**
Allows multiple BGP routes to be used at the same time to reach the same destination. Enables BGP to load-balance traffic across multiple links.

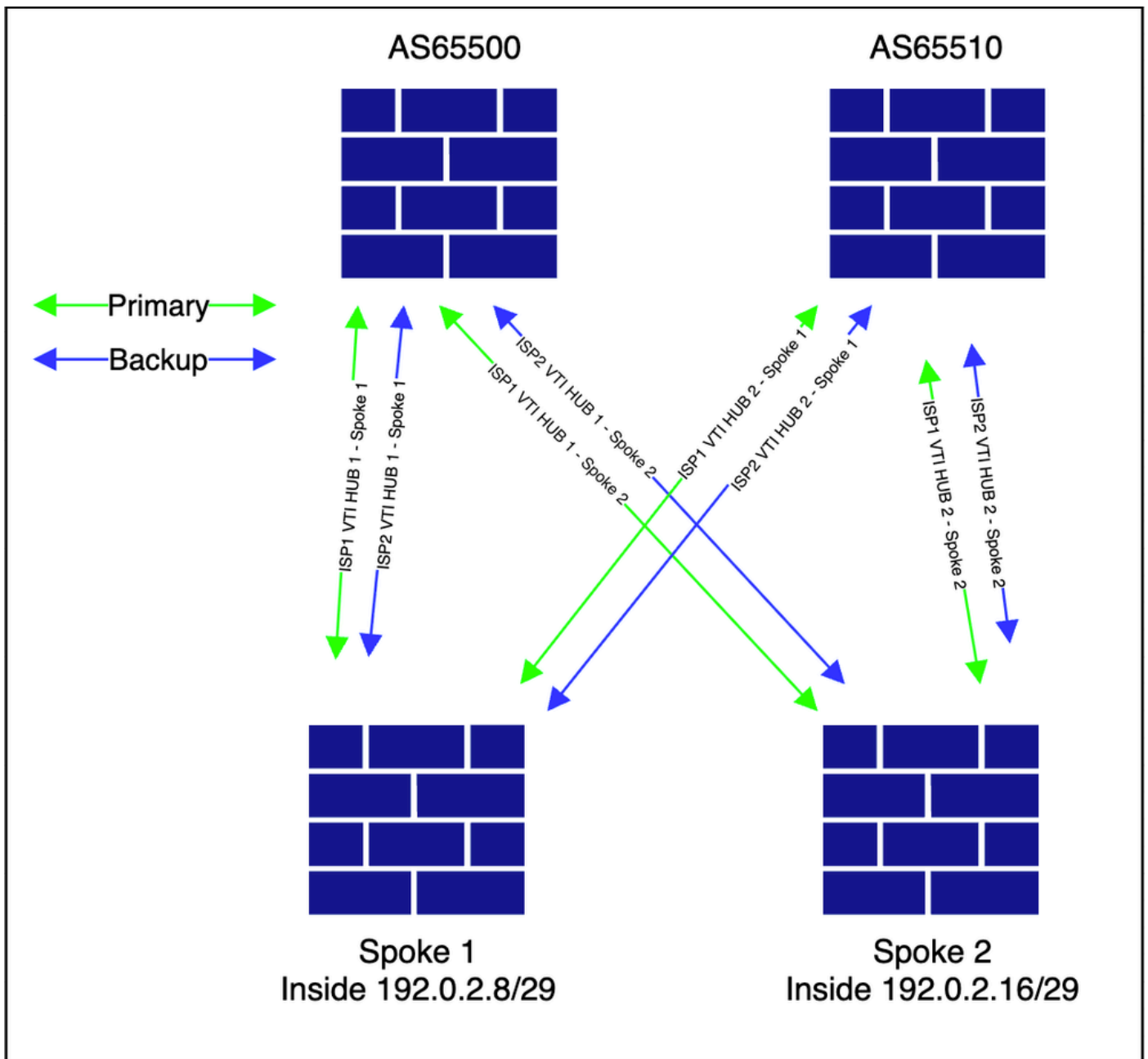
[Next](#) You have unsaved changes

[Cancel](#) [Finish](#)

- Alle andere instellingen blijven ongewijzigd. Voltooi de wizard en ga verder met de implementatie.

Verificatie

- De topologie wordt weergegeven.



- Navigeer naar Apparaten > VPN > Site to Site om de topologie te bekijken.

198.51.100.4 4 65510 183 183 4 0 0 03:16:30 2

<<<<<<<< HUB 2 ISP 2 VTI

<#root>

Spoke1#show bgp ipv4 unicast neighbors 198.51.100.1 routes <<<< check for specific prefixes received via

BGP table version is 4, local router ID is 203.0.113.35

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*>i192.0.2.16/29	198.51.100.1	1	100	0	?

<<<<<<< spoke 2 network received via HUB 1 ISP 1 tunnel

Total number of prefixes 1

<#root>

Spoke1#show bgp ipv4 unicast neighbors 198.51.100.3 routes <<<< check for specific prefixes received via

BGP table version is 4, local router ID is 203.0.113.35

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
*mi192.0.2.16/29	198.51.100.3	1	100	0	?

<<<<<<< spoke 2 network received via HUB 1 ISP 2 tunnel

Total number of prefixes 1

<#root>

Spoke1# show bgp ipv4 unicast neighbors 198.51.100.2 routes <<<< check for specific prefixes received via

BGP table version is 4, local router ID is 203.0.113.35

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* 192.0.2.8/29	198.51.100.2	100		0	65510 65510 ?

<<<<<<< inside network receieved cause we advertised it to HUB 1 from ISP 2 topology

* 192.0.2.16/29	198.51.100.2	100		0	65510 65510 ?
-----------------	--------------	-----	--	---	---------------

<<<<<<< spoke 2 network received via HUB 2 ISP 1 tunnel but not preferred

Total number of prefixes 2

<#root>

Spoke1# show bgp ipv4 unicast neighbors 198.51.100.4 routes <<<< check for specific prefixes received via

BGP table version is 4, local router ID is 203.0.113.35
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
* 192.0.2.8/29	198.51.100.4	100		0	65510 65510 ?

<<<<<<< inside network received cause we advertised it to HUB 2 from ISP 1 topology

* 192.0.2.16/29	198.51.100.4	100		0	65510 65510 ?
-----------------	--------------	-----	--	---	---------------

<<<<<<< spoke 2 network received via HUB 2 ISP 2 tunnel but not preferred

Total number of prefixes 2

De routingstabel wordt weergegeven, wat bevestigt dat het verkeer aan de spaakzijde evenwichtig is verdeeld over beide links.

<#root>

Spoke1#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 not set

B 192.0.2.16 255.255.255.248 [200/1] via 198.51.100.3, 03:23:53

<<<<< multipath for spoke 2 inside network

[200/1] via 198.51.100.1, 03:23:53

<<<<< multipath for spoke 2 inside network

<#root>

Spoke1#show bgp 192.0.2.16

BGP routing table entry for 192.0.2.16/29, version 4

Paths: (4 available, best #4, table default)

Multipath: eBGP iBGP

Advertised to update-groups:

2 4

65510 65510

198.51.100.4 from 198.51.100.4 (198.51.100.4)

<<<< HUB2 ISP2 next-hop

Origin incomplete, metric 100, localpref 100, valid, external

Community: 10101

Local

198.51.100.3 from 198.51.100.3 (198.51.100.3)

<<<< HUB1 ISP2 next-hop

Origin incomplete, metric 1, localpref 100, valid, internal, multipath

Community: 10101

Originator: 203.0.113.36, Cluster list: 198.51.100.3

65510 65510

198.51.100.2 from 198.51.100.2 (198.51.100.4)

<<<< HUB2 ISP1 next-hop

Origin incomplete, metric 100, localpref 100, valid, external

Community: 10101

Local

198.51.100.1 from 198.51.100.1 (198.51.100.3)

<<<< HUB1 ISP1 next-hop

Origin incomplete, metric 1, localpref 100, valid, internal, multipath, best

Community: 10101

Originator: 203.0.113.36, Cluster list: 198.51.100.3

Conclusie

Het doel van dit artikel is om verschillende implementatiescenario's uit te leggen die eenvoudig kunnen worden geïmplementeerd met behulp van één installatiewizard.

Gerelateerde informatie

- Voor aanvullende hulp kunt u contact opnemen met TAC. Een geldig supportcontract is vereist: [Cisco Worldwide Support Contacts](#).
- Je kunt ook de Cisco VPN Community [hier](#) bezoeken.

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.