

Konfiguration von SD-WAN für Site-to-Site-VPN über sichere Firewall

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Informationen zu Funktionen](#)

[Behandelte Topologien](#)

[HUB und Spoke \(einzelner ISP\)](#)

[Dual-HUB und -Spoke \(Single-ISP für redundanten HUB über EBGP zwischen sekundären HUB und Spokes\)](#)

[Dual-HUB und -Spoke \(Dual-ISP für redundante HUBs und ISPs über EBGP zwischen sekundären HUBs und Spokes\)](#)

[Schlussfolgerung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden routenbasierte VPN-Bereitstellungsszenarien mit BGP-Overlay-Routing unter Verwendung der SD-WAN-Funktion der sicheren Firewall beschrieben.

Voraussetzungen

Auf allen Hubs und Stationen wird FTD 7.6 oder höher ausgeführt, und die Verwaltung erfolgt über dasselbe FMC, auf dem auch Software der Version 7.6 oder höher ausgeführt wird.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- IKEv2
- Routenbasiertes VPN
- Virtuelle Tunnelschnittstellen (VTI)
- IPsec
- BGP

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Informationen zu Funktionen

Das Management Center vereinfacht die Konfiguration von VPN-Tunneln und das Routing zwischen zentralisierten Hauptgeschäftsstellen (Hubs) und Außenstellen (Spokes) mithilfe des neuen SD-WAN-Assistenten.

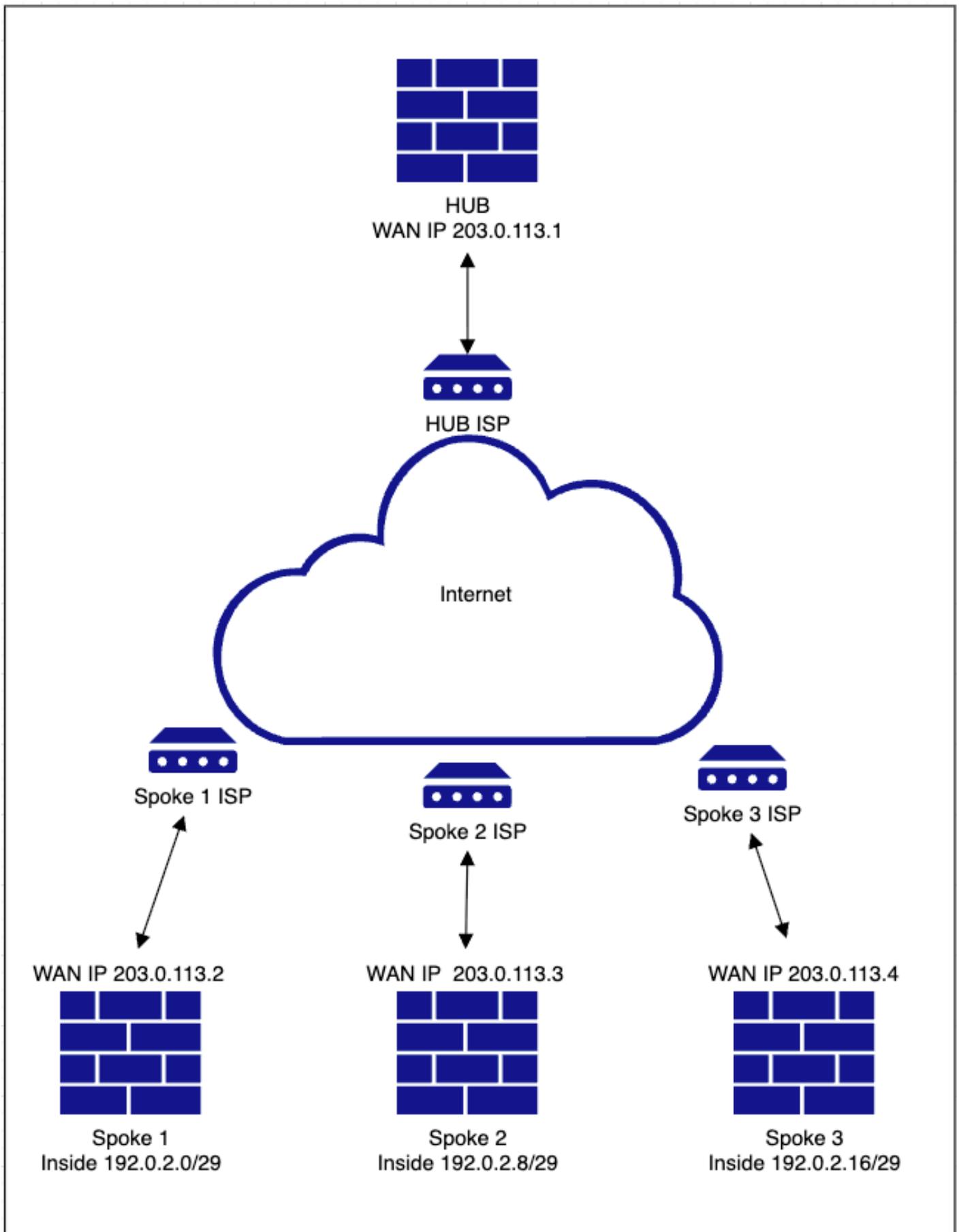
- Automatisiert die VPN-Konfiguration durch die Nutzung von DVTI (Dynamic Virtual Tunnel Interface) auf Hubs und SVTI (Static Virtual Tunnel Interface) auf Stationen, wobei das Overlay-Routing über BGP aktiviert wird.
- Automatische Zuweisung von SVTI-IP-Adressen für Stationen und Übertragung der gesamten VTI-Konfiguration, einschließlich Verschlüsselungsparametern.
- Einfache Routing-Konfiguration in einem Schritt mit demselben Assistenten zur Aktivierung von BGP für Overlay-Routing
- Skalierbares und optimales Routing durch Nutzung des Route-Reflector-Attributs für BGP
- Gleichzeitiges Hinzufügen mehrerer Speichen bei minimalem Benutzereingriff

Behandelte Topologien

In diesem Artikel werden mehrere Topologien behandelt, um sicherzustellen, dass Benutzer die verschiedenen Bereitstellungsszenarien kennen.

HUB und Spoke (einzelner ISP)

Netzwerkdiagramm



Konfigurationen

- Navigieren Sie zu Devices > VPN > Site to Site > Add > SD-WAN Topology > > Create.

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy Search Settings Help 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](#)

- Hinzufügen eines Hubs und Erstellen einer DVTI am Hub-Ende Stellen Sie im Rahmen der DVTI-Konfiguration sicher, dass Sie die richtige Tunnel-Quellschnittstelle entsprechend der Topologie auswählen.

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 Settings

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

- Erstellen Sie einen IP-Adresspool für den Spoke-Tunnel, und klicken Sie auf Speichern und dann auf Hinzufügen. Der IP-Adresspool wird verwendet, um den Stationen IP-Adressen des VTI-Tunnels zuzuweisen.

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy Search 11 Settings Help admin

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

Add Hub

Device *

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

Hub Gateway IP Address

Spoke Tunnel IP Address Pool *

Cancel **Add**

Add IPv4 Pool

Name*

Description

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

Mask*

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**

Cancel **Finish**

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy Search 11 Settings Help 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	<input type="text" value="Add Hub"/> <input type="text" value="Edit"/>

Next

2 Spokes Edit

3 Authentication Settings Edit

4 SD-WAN Settings Edit

Cancel **Finish**

- Klicken Sie auf Weiter, um fortzufahren und die Speicher hinzuzufügen. Sie können entweder eine Bulk-Hinzufügungsoption nutzen, wenn Sie allgemeine Schnittstellen-

/Zonennamen haben, oder Stationen einzeln hinzufügen.

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 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

View Generated Tunnel Interfaces Add Spokes (Bulk Addition) Add Spoke

No spokes are configured. Add a spoke.

Next

3 Authentication Settings Edit

4 SD-WAN Settings Edit

Cancel Finish

- Wählen Sie die Geräte aus, und geben Sie ein Namensmuster für die WAN-/externe Schnittstelle an. Wenn die Geräte denselben Schnittstellennamen verwenden, ist die Verwendung von Initialen ausreichend. Klicken Sie auf Weiter, und wenn die Validierung erfolgreich ist, klicken Sie auf Hinzufügen. Bei Massenadditionen können Sie den Zonennamen auf die gleiche Weise verwenden.

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

Add Bulk Spokes

1 Add Devices 2 Validate Devices

Available Devices *

Selected Devices *

ftd2

ftd3

ftd4

Select VPN Interface Using *

Interface Name Pattern ?

Security Zone ?

Select... ▾ +

3 Authentication Settings Edit

4 SD-WAN Settings Edit

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 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 Spokes (Bulk Addition) Add Spoke

Add Bulk 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

Cancel Back **Add**

Next

3 Authentication Settings Edit

4 SD-WAN Settings Edit

Cancel **Finish**

- Überprüfen Sie die Speicher- und Overlay-Schnittstellendetails, um sicherzustellen, dass die richtigen Schnittstellen ausgewählt sind, und klicken Sie dann auf Weiter.

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](#)

- Sie können entweder die Standardparameter für die IPsec-Konfiguration beibehalten oder nach Bedarf benutzerdefinierte Chiffren angeben. Klicken Sie auf Weiter, um fortzufahren. In diesem Dokument werden die Standardparameter verwendet.

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
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 Edit

Authentication Type*
Pre-shared Automatic Key

Pre-shared Key Length*
24 The range is 1 to 127.

Transform Sets (IPsec Proposals)*
AES-GCM x Show Details

IKEv2 Policies*
AES-GCM-NULL-SHA-LATEST x Show Details

Next

4 SD-WAN Settings Edit

Cancel Finish

- Schließlich können Sie das Overlay-Routing im selben Assistenten für diese Topologie konfigurieren, indem Sie die entsprechenden BGP-Parameter wie die AS-Nummer, die interne Schnittstellenankündigung und Community-Tags für die Präfixfilterung angeben. Die Sicherheitszone kann bei der Filterung des Datenverkehrs mithilfe von Zugriffskontrollrichtlinien helfen. Sie können außerdem ein Objekt für Schnittstellen erstellen und diese bei der Neuverteilung verbundener Schnittstellen verwenden, wenn der Name nicht der interne Name ist oder nicht symmetrisch zu den Geräten in der Topologie ist.

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-198.51.100.32
- 2 **Spokes** Edit
 - Device ftd2 VPN Interface VPN-OUT-1 Key ID: HUB-Spoke-VPN-Single-ISP_ftd2
 - 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 Key ID: HUB-Spoke-VPN-Single-ISP_ftd4
- 3 **Authentication Settings** Edit
 - Authentication Pre-shared Automatic Key Pre-shared Key Length 24
- 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 +
 - 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

- Klicken Sie auf Weiter, dann auf Fertig stellen und schließlich auf Bereitstellen, um den Prozess abzuschließen.

Verifizierung

- Sie können den Tunnelstatus überprüfen, indem Sie zu Devices (Geräte) > VPN (VPN) > Site to Site (Site-to-Site) navigieren.

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

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
▼ HUB-Spoke-VPN-Single-ISP	Route Based (VTI)	SD-WAN Topology	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_dynam... (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_dynam... (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

- Weitere Details können unter Übersicht > Dashboards > Site-to-Site-VPN überprüft werden.

Firewall Management Center
Overview / Dashboards / Site to Site VPN

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Select... Refresh Refresh every 5 minutes

Tunnel Summary

100% Active
3 connections

Node A	Node B	Topology	Status	Last Updated :
fd1 (VPN IP: 203.0.113.1)	fd2 (VPN IP: 203.0.113.2)	HUB-Spoke-VPN-Single-ISP	Active	2025-09-09 06:06:15
fd1 (VPN IP: 203.0.113.1)	fd3 (VPN IP: 203.0.113.3)	HUB-Spoke-VPN-Single-ISP	Active	2025-09-09 06:06:15
fd1 (VPN IP: 203.0.113.1)	fd4 (VPN IP: 203.0.113.4)	HUB-Spoke-VPN-Single-ISP	Active	2025-09-09 06:06:15

Topology

Name	🔴	🟡	🟢
HUB-Spoke-VPN-Single-...	0	0	3

- Um weitere Einblicke zu erhalten, wählen Sie den Tunnel aus, und klicken Sie auf Vollständige Informationen anzeigen.

Firewall Management Center
Overview / Dashboards / Site to Site VPN

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Select... Refresh Refresh every 5 minutes

Tunnel Summary

100% Active
3 connections

Node A	Node B	Topology	Status	Last Updated :
fd1 (VPN IP: 203.0.113.1)	fd2 (VPN IP: 203.0.113.2)	HUB-Spoke-VPN-Single-ISP	Active	2025-09-09 06:06:15
fd1 (VPN IP: 203.0.113.1)	fd3 (VPN IP: 203.0.113.3)	HUB-Spoke-VPN-Single-ISP	Active	2025-09-09 06:06:15
fd1 (VPN IP: 203.0.113.1)	fd4 (VPN IP: 203.0.113.4)	HUB-Spoke-VPN-Single-ISP	Active	2025-09-09 06:06:15

Topology

Name	🔴	🟡	🟢
HUB-Spoke-VPN-Single-...	0	0	3

Firewall Management Center
Overview / Dashboards / Site to Site VPN

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Select... Refresh Refresh every 5 minutes

Node A	Node B	Topology	Status	Last Updated :
fd1 (VPN IP: 203.0.113.1)	fd2 (VPN IP: 203.0.113.2)	HUB-Spoke-VPN-Single-ISP	Active	2025-09-09 06:06:15
fd1 (VPN IP: 203.0.113.1)	fd3 (VPN IP: 203.0.113.3)	HUB-Spoke-VPN-Single-ISP	Active	2025-09-09 06:06:15
fd1 (VPN IP: 203.0.113.1)	fd4 (VPN IP: 203.0.113.4)	HUB-Spoke-VPN-Single-ISP	Active	2025-09-09 06:06:15

A: fd1 ↔ B: fd2
Topology: HUB-Spoke-VPN-Single-ISP | Status: Active

General	CLI Details	Packet Tracer
Topology	HUB-Spoke-VPN-Single-ISP	
Status	Active	
Node A	fd1	
Node B	fd2	
Node A IP	203.0.113.1	
Node B IP	203.0.113.2	
Node A VPN Interface Name	VPN-OUT-1	
Node B VPN Interface Name	VPN-OUT-1	
Last Updated	2025-09-09 06:06:15	

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 (203.0.113.1/30)	Node B (203.0.113.2/30)
Transmitted: 9.52 KB (9744 B)	Transmitted: 9.26 KB (9481 B)
Received: 12.33 KB (12628 B)	Received: 12.61 KB (12912 B)

Ipssec 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)	ftd2 (VPN Interface IP: 203.0.113.2)

```

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

- Die Ausgabe wird direkt über die FTD-CLI angezeigt und kann aktualisiert werden, um aktualisierte Zähler und wichtige Informationen anzuzeigen, z. B. Details zum Sicherheitsparameterindex (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 reas: 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_vt
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, loc

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 reas: 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

- Die FTD-CLI kann auch verwendet werden, um Routing-Informationen und den BGP-Peering-Status zu überprüfen.

HUB-seitig

<#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

auf Spoke-Seite

Die gleiche Überprüfung kann auch an den Spoke-Geräten durchgeführt werden. Hier ist ein Beispiel aus einer der Speichen.

<#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

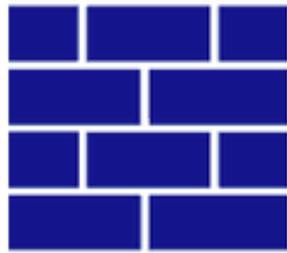
B 192.0.2.16 255.255.255.248 [200/1] via 198.51.100.1, 00:13:42

<<<<<< spoke 3 inside network

Dual-HUB und -Spoke (Single-ISP für redundanten HUB über EBGP zwischen sekundären HUB und Spokes)

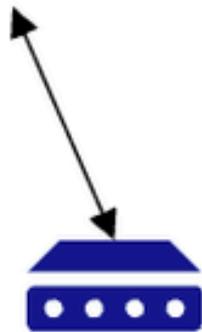
Netzwerkdigramm

AS65500



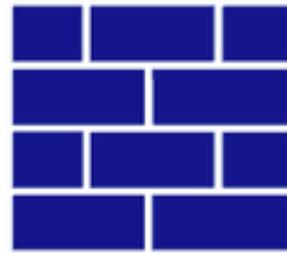
HUB 1

WAN IP 203.0.113.1



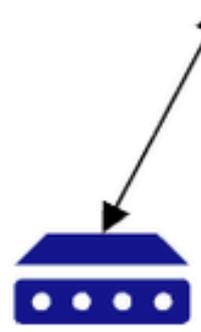
HUB 1 ISP

AS65510

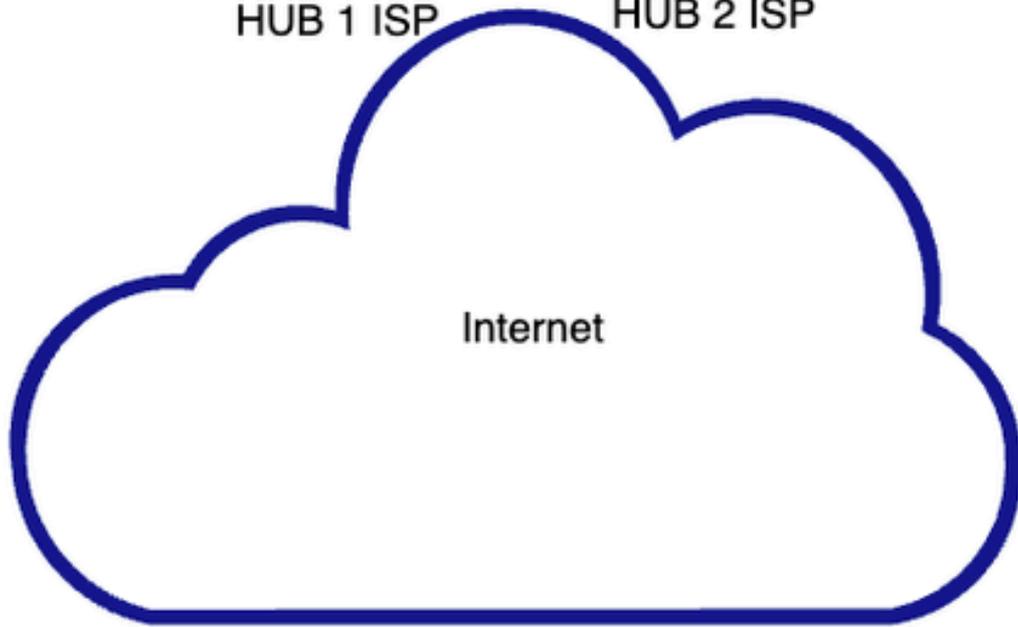


HUB 2

WAN IP 203.0.113.2



HUB 2 ISP



Internet



Spoke 1 ISP



Spoke 2 ISP

WAN IP 203.0.113.3



WAN IP 203.0.113.4



Fahren Sie nach dem Hinzufügen des ersten HUB mit dem Hinzufügen des zweiten HUB fort. Gehen Sie dabei wie zuvor für HUB1 beschrieben vor.

FMC Site To Site Overview Analysis Policies Devices Objects Integration Deploy Search 3 Settings Help admin

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: 198.51.100.10-198.51.100.1

Next

Add Hub

- Fahren Sie mit der Erstellung des DVTI (Dynamic Virtual Tunnel Interface) fort.

Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy Search 3 Settings Help admin

Dual-HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Add Virtual Tunnel Interface

General Path Monitoring

Tunnel Type
 Static Dynamic

Name:*
VPN-OUT-1_dynamic_vti_1

Enabled

Description:

Security Zone:

Priority:
0 (0 - 65535)

Virtual Tunnel Interface Details
An interface named TunnelID* 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) 203.0.113.2

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) Select Interface

Add Loopback Interface

General IPv4 IPv6

Name:
VPN-OUT-LOOPBACK

Enabled

Loopback ID:*
1 (1-1024)

Description

Add Hub

Device *
ftd2

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

Hub Gateway IP Address *

Cancel Add

Cancel OK

Cancel OK

Cancel Finish

- Für HUB 2 VTI-Tunnel auf der Spoke-Seite ist ein neuer IP-Adresspool erforderlich. Erstellen und konfigurieren Sie den neuen Pool, und speichern Sie die Änderungen.

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 ftd4 VPN Interface VPN-OUT-1 VPN-OUT-4 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 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

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

- Ändern Sie im letzten Schritt die SD-WAN-Einstellungen, um das eBGP-Peering zwischen dem zweiten HUB und den Stationen zu konfigurieren. Aktivieren Sie die Option Sekundärer HUB befindet sich in einem anderen autonomen System, und geben Sie die AS-Nummer (Autonomous System) für den sekundären HUB an. IBGP kann auch verwendet werden, wenn die Verwendung unterschiedlicher AS-Nummern in Ihrer Umgebung nicht eingeschränkt ist, indem die Option "Sekundärer HUB" in einem anderen autonomen System deaktiviert wird. Dadurch werden dieselbe Community-Tag- und AS-Nummer auch für das sekundäre HUB verwendet. Der Schwerpunkt dieses Artikels liegt auf eBGP für die aktuelle

Konfiguration.

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

- 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
	ftd2		VPN-OUT-1_dynamic_vti_1		203.0.113.2		VPN-POOL-198.51.100.32
- Spokes** Edit

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

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.

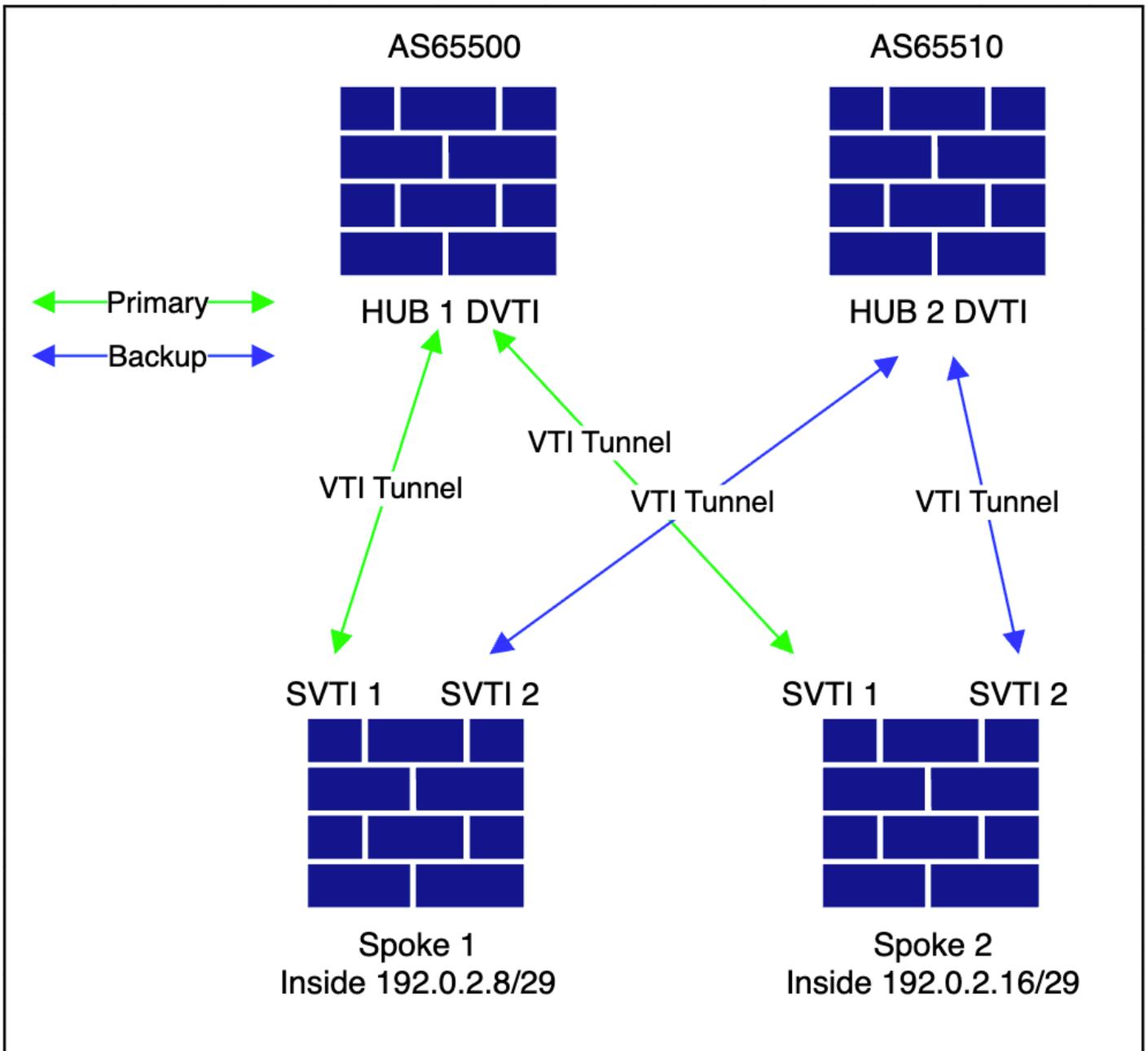
[Next](#) You have unsaved changes

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

Stellen Sie sicher, dass sowohl die AS-Nummer (Autonomous System) als auch das Community-Tag in dieser Konfiguration eindeutig sind.

Verifizierung

Dieses Diagramm zeigt die Overlay-Topologie.



- Navigieren Sie im FMC zu Devices > VPN > Site to Site.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 Cisco SECURE

Last Updated: 02:20 PM Refresh NAT Exemptions Add

Select... Refresh

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

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

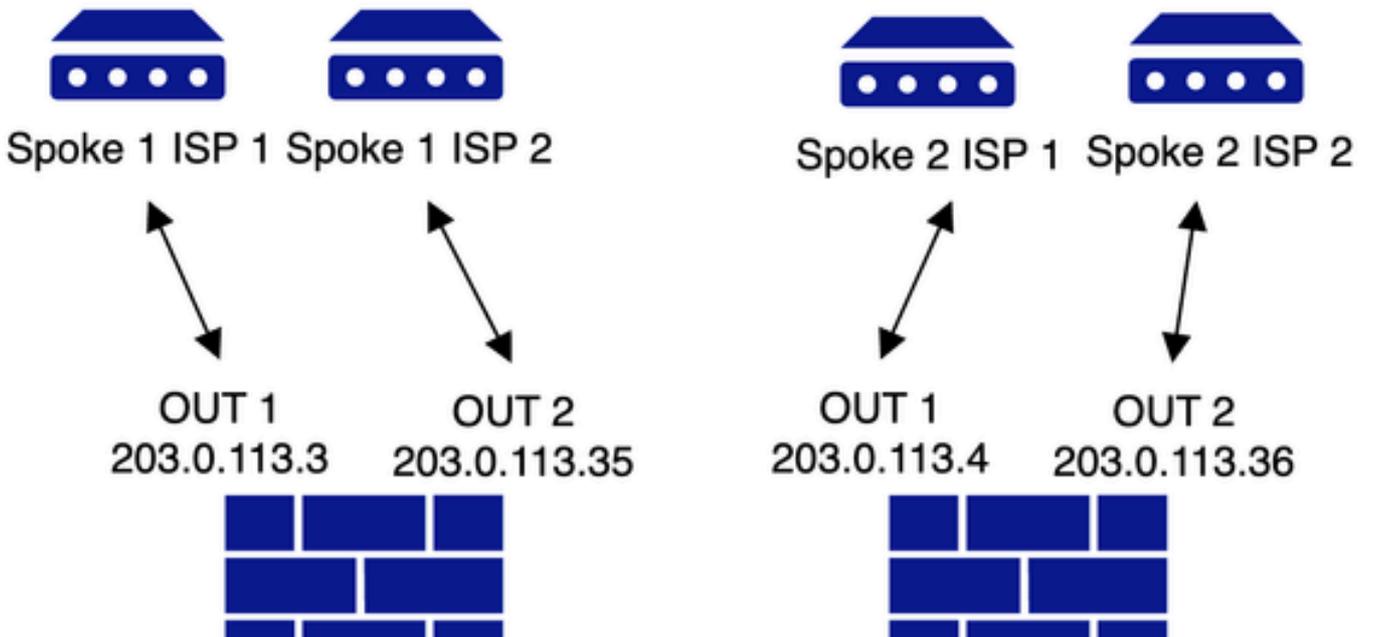
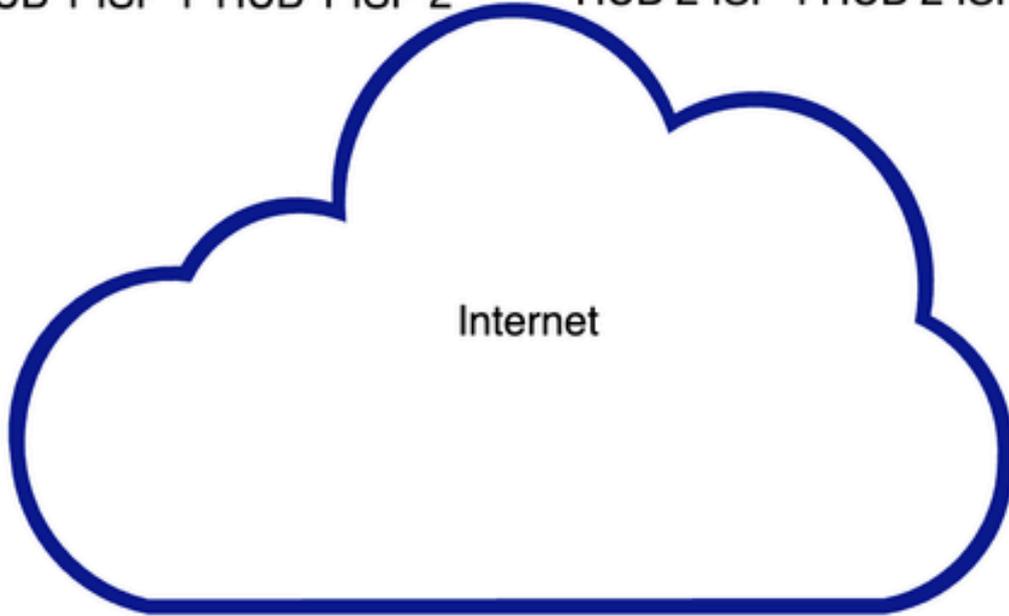
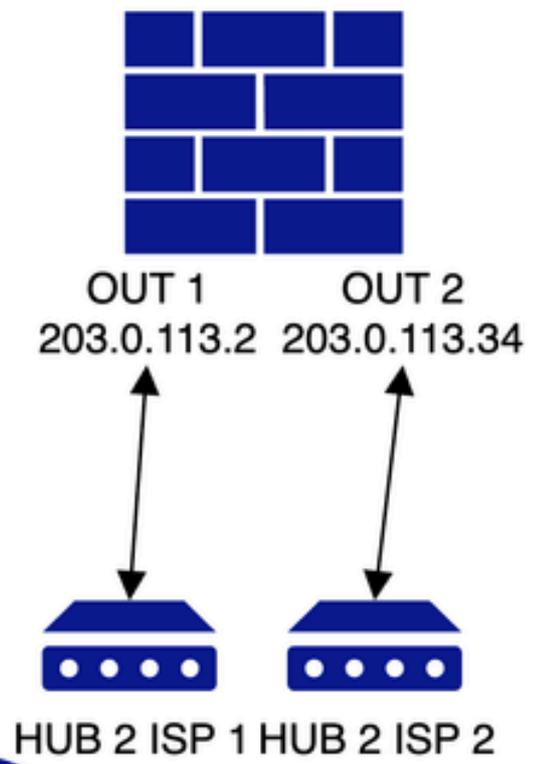
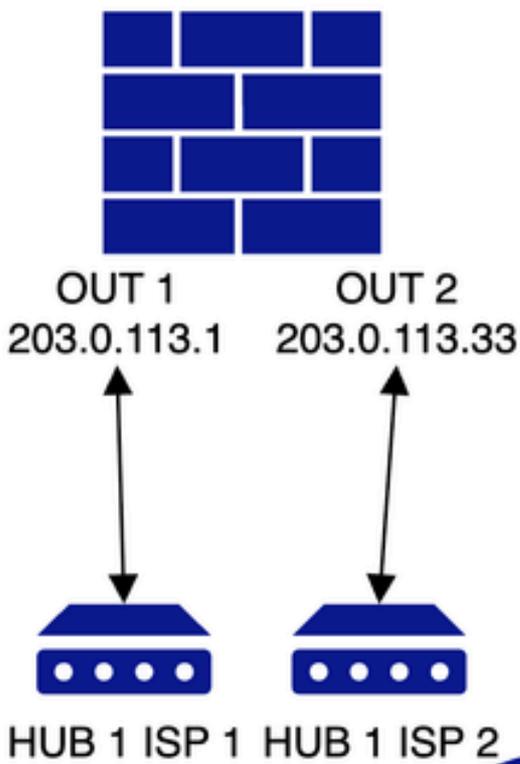
- Alle anderen Schritte bleiben unverändert.

Dual-HUB und -Spoke (Dual-ISP für redundante HUBs und ISPs über EBGP zwischen sekundären HUBs und Spokes)

Netzwerkdigramm

AS65500

AS65510



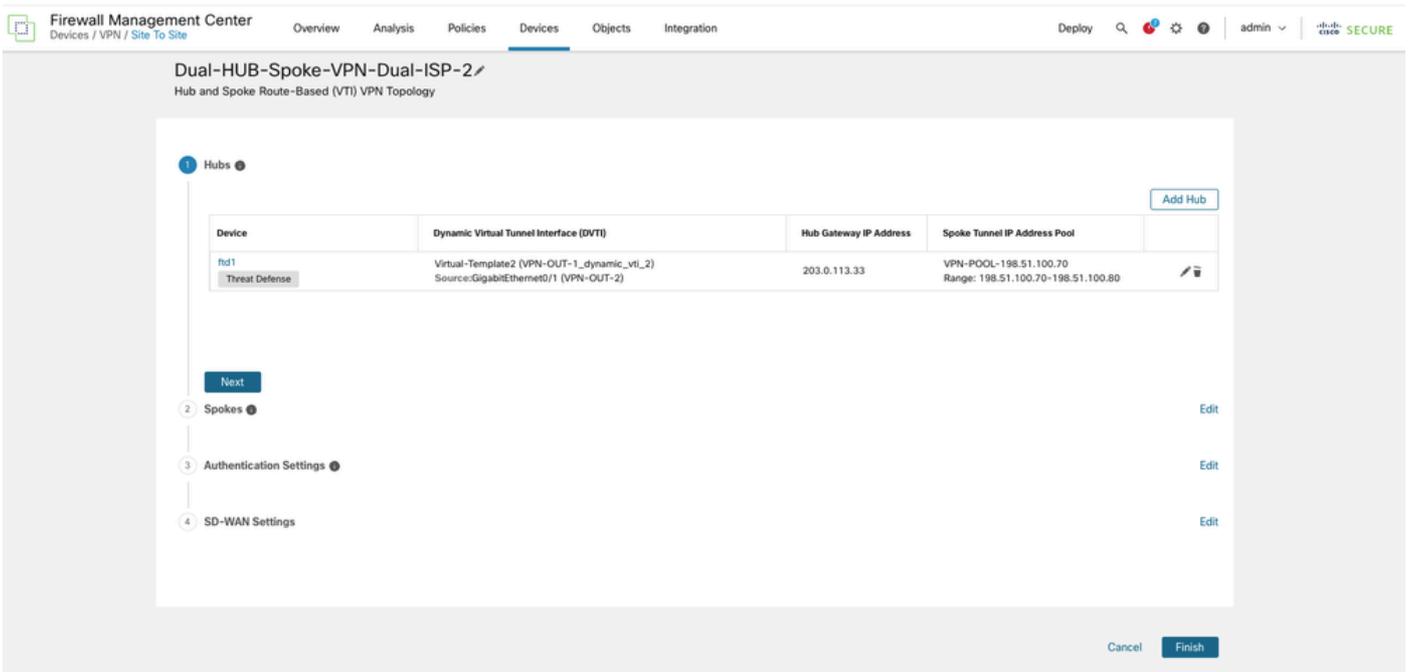
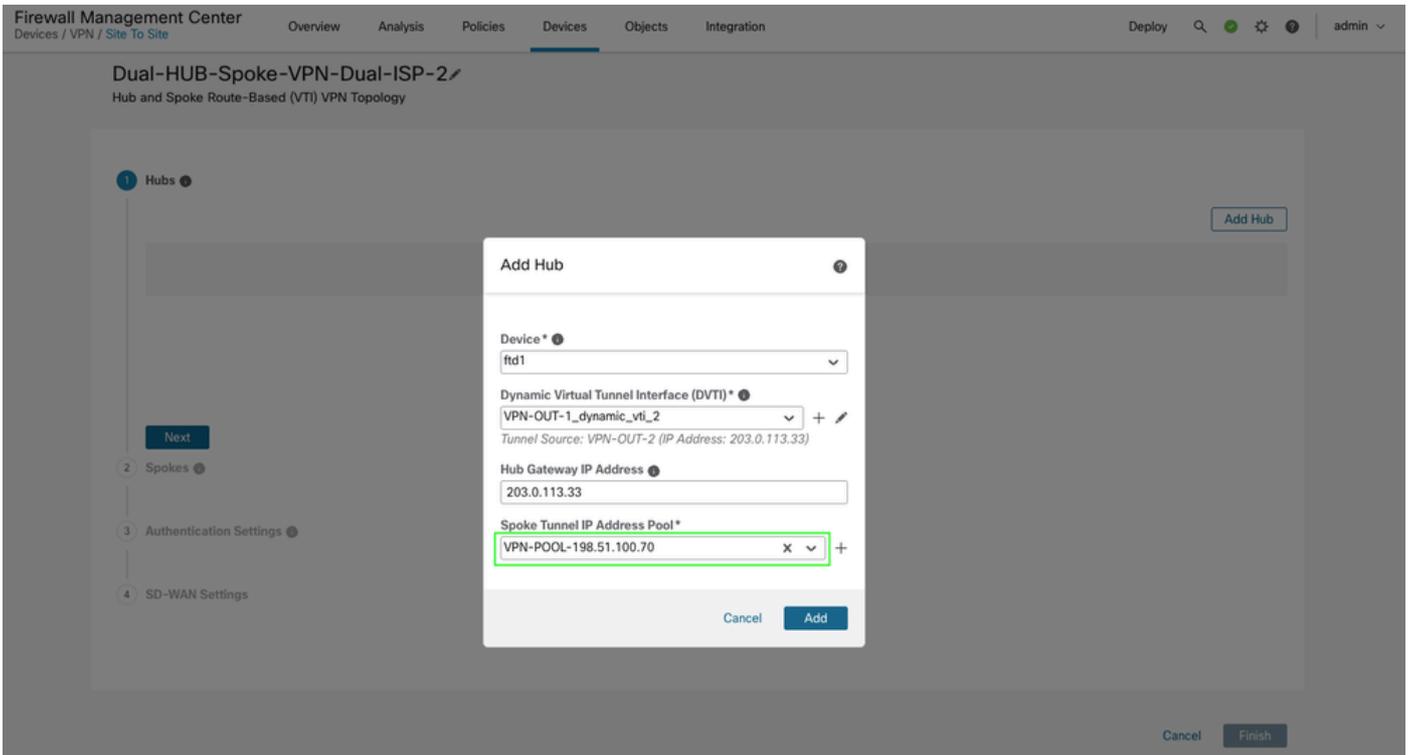
Die Bereitstellung für diese Topologie wird mit dem ersten ISP übersprungen, da dies in der vorherigen Topologie behandelt wurde.

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_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)		

- Als Nächstes fügen Sie die zweite Topologie hinzu, indem Sie zwei zusätzliche DVTI-Schnittstellen pro HUB erstellen, die jeweils die Underlay-Schnittstelle für ISP 2 (VPN-OUT-2) nutzen.

The screenshot shows the 'Add Virtual Tunnel Interface' dialog in the Firewall Management Center. The 'General' tab is active. The 'Tunnel Type' is set to 'Dynamic'. The 'Name' field contains 'VPN-OUT-1_dynamic_vti_2'. The 'Enabled' checkbox is checked. The 'Description' field is empty. The 'Security Zone' is set to 'untrust'. The 'Priority' is set to '0'. The 'Virtual Tunnel Interface Details' section shows 'Template ID' as '2' and 'Tunnel Source' as 'GigabitEthernet0/1 (VPN-OUT-2)' with IP address '203.0.113.33'. The 'IPsec Tunnel Mode' is set to 'IPv4'. The 'IP Address' is set to 'Borrow IP (IP unnumbered)' with 'Loopback2 (VPN-2-LOOPBACK...)' selected.

- Speziell für Spoke Virtual Tunnel Interface (VTI)-Adressen wird ein zusätzlicher VPN-IP-Adresspool bereitgestellt.



- Um einen sekundären Hub hinzuzufügen, wiederholen Sie den Vorgang, indem Sie DVTI 2 über die sekundäre ISP-Schnittstelle (VPN-OUT-2) erstellen, und konfigurieren Sie einen zusätzlichen IP-Pool für Spoke-End-VTI-Adressen.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration Deploy

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

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Device	Dynamic Virtual Tunnel Interface (DVTI)
ftd1 Threat Defense	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

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 Threat Defense	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

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

Next

Cancel Finish

- Achten Sie beim Hinzufügen einer Spoke darauf, dass die richtige Underlay-/WAN-Schnittstelle für die VTI-Tunnel festgelegt ist. Diese Topologie verwendet die sekundäre ISP-

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

2 Spokes

Next

3 Authentication Settings

4 SD-WAN Settings

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

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

Cancel Finish

- Stellen Sie beim Konfigurieren des Routings sicher, dass die Community-Tags und AS-Nummern für beide HUBs in dieser Topologie mit den Tags übereinstimmen, die in der vorherigen ISP1-Topologie verwendet wurden. Die Topologie nutzt unterschiedliche Sicherheitszonen, die verbleibenden Konfigurationen (AS-Nummern für primäre und sekundäre HUBs sowie Community-Tags) sind jedoch identisch. Dies ist erforderlich, damit die Benutzeroberfläche die Topologieprüfung abschließen kann.

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.

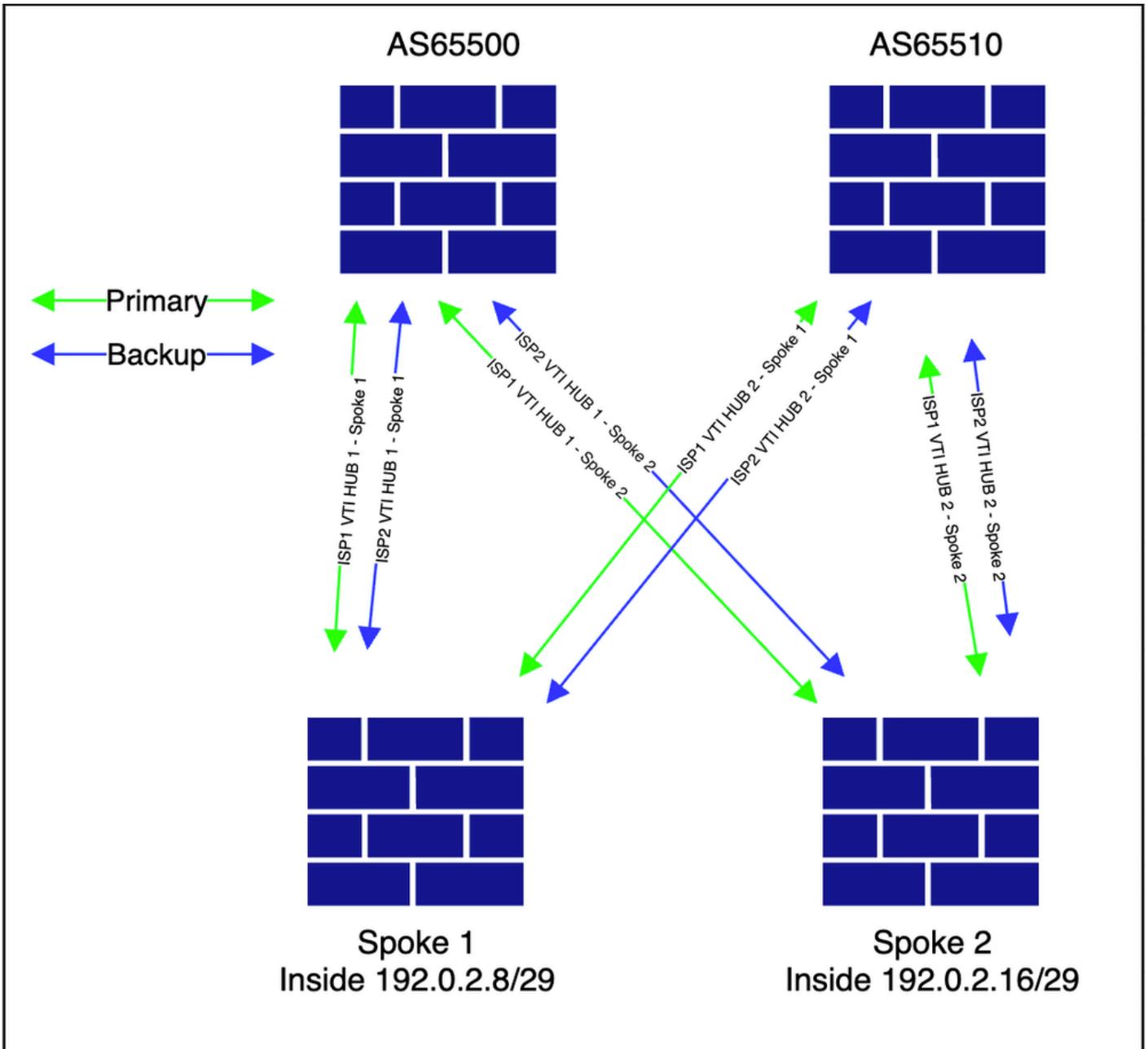
Next You have unsaved changes

Cancel Finish

- Alle anderen Einstellungen bleiben unverändert. Schließen Sie den Assistenten ab, und fahren Sie mit der Bereitstellung fort.

Verifizierung

- Die Topologie wird wie dargestellt angezeigt.



- Navigieren Sie zu Devices > VPN > Site to Site, um die Topologie anzuzeigen.


```
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 received 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 v

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

Die Routing-Tabelle wird wie dargestellt angezeigt. Sie bestätigt, dass ein Load Balancing des Datenverkehrs zwischen den beiden Verbindungen auf der Spoke-Seite stattfindet.

<#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
```

Schlussfolgerung

In diesem Artikel werden verschiedene Bereitstellungsszenarien erläutert, die mit einem einzigen Setup-Assistenten einfach implementiert werden können.

Zugehörige Informationen

- Weitere Unterstützung erhalten Sie beim TAC. Ein gültiger Support-Vertrag ist erforderlich: [Cisco Worldwide Support Contacts](#)
- Sie können [hier](#) auch die Cisco VPN Community besuchen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.