

# Configure SD-WAN for Site-to-Site VPN over Secure Firewall

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

#### [Requirements](#)

#### [Components Used](#)

### [Feature Information](#)

### [Topologies Covered](#)

#### [HUB & Spoke \(Single ISP\)](#)

#### [Dual HUB & Spoke \(Single ISP for Redundant HUB via EBGP Between Secondary HUB and Spokes\)](#)

#### [Dual HUB & Spoke \(Dual ISP for Redundant HUB and ISP via EBGP Between Secondary HUB and Spokes\)](#)

### [Conclusion](#)

### [Related Information](#)

---

## Introduction

This document describes route-based VPN deployment scenarios with BGP overlay routing using the SD-WAN feature on Secure Firewall.

## Prerequisites

All the hubs and spokes are running FTD 7.6 or later software and are managed via the same FMC, which is also running 7.6 or later software.

## Requirements

Cisco recommends that you have knowledge of these topics:

- IKEv2
- Route-based VPN
- Virtual Tunnel Interfaces (VTI)
- IPsec
- BGP

## Components Used

The information in this document is based on:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure

that you understand the potential impact of any command.

## Feature Information

The Management Center simplifies the configuration of VPN tunnels and routing between centralized headquarters (hubs) and remote branch sites (spokes) by using the new SD-WAN wizard.

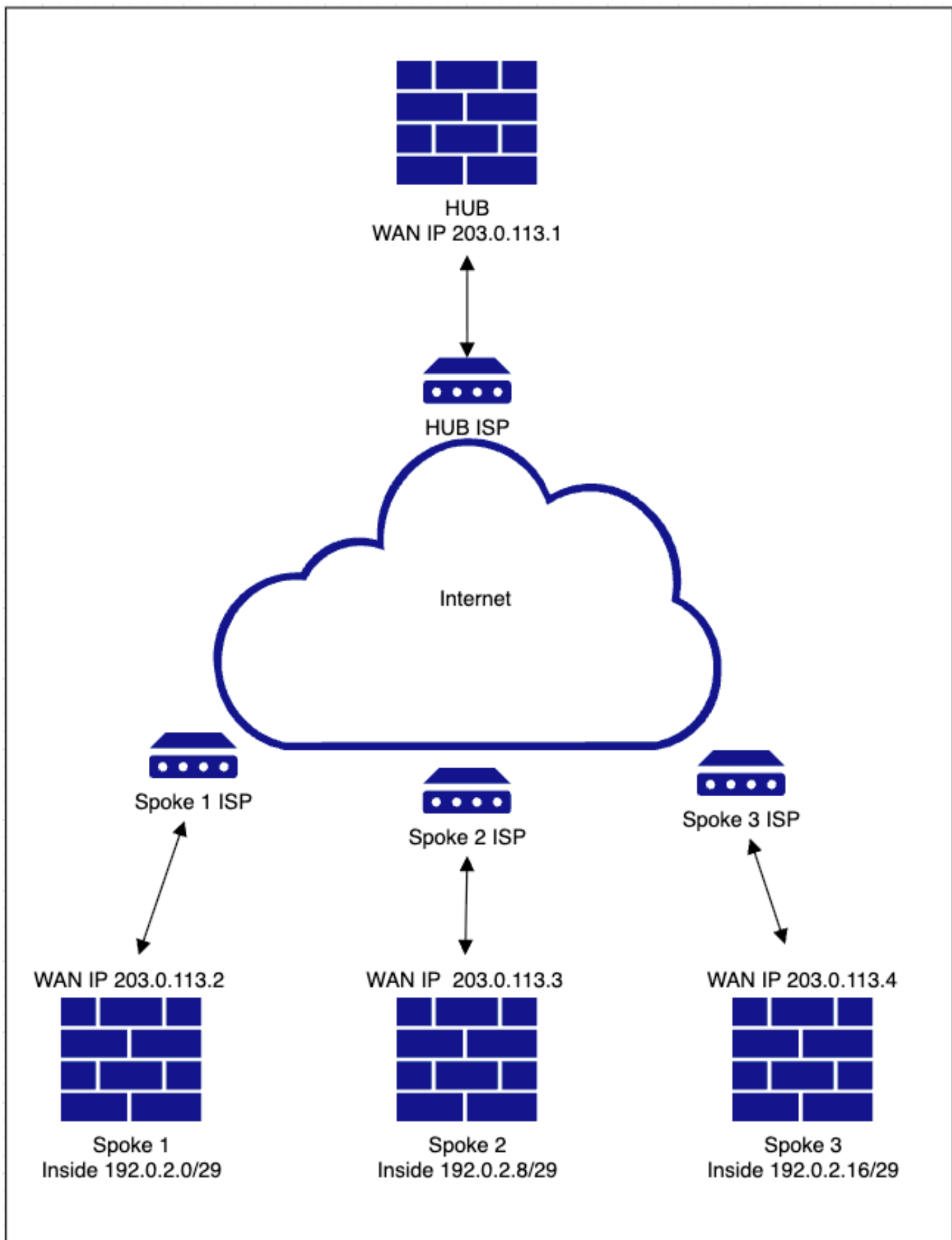
- Automates VPN configuration by leveraging DVTI (Dynamic Virtual Tunnel Interface) on hubs and SVTI (Static Virtual Tunnel Interface) on spokes, with overlay routing enabled through BGP.
- Automatically assigns SVTI IP addresses for spokes and pushes the complete VTI configuration, including crypto parameters.
- Provides easy, one-step routing configuration within the same wizard to enable BGP for overlay routing.
- Enables scalable and optimal routing by leveraging the route-reflector attribute for BGP.
- Allows multiple spokes to be added simultaneously with minimal user intervention.

## Topologies Covered

In this article, multiple topologies are covered to ensure that users are aware of various deployment scenarios.

### HUB & Spoke (Single ISP)

Network Diagram



## Configurations

- Navigate to **Devices > VPN > Site to Site > Add > SD-WAN Topology > > Create**.

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](#)

- Add a **hub** and create a **DVTI** at the hub end. As part of DVTI configuration, please ensure to select correct tunnel source interface as per the topology.

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

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

- Create a **Spoke Tunnel IP address pool** and click **Save** and then **Add**. The ip address pool is used to assign VTI tunnel IP addresses to the spokes.

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	

Next

2 Spokes 📘 Edit

3 Authentication Settings 📘 Edit

4 SD-WAN Settings Edit

Cancel Finish

- Click **Next** to proceed and add the spokes. You can leverage either bulk addition option if you have common interface / zone names or add spokes individually.

## 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

No spokes are configured. Add a spoke.

Next

## 3 Authentication Settings

Edit

## 4 SD-WAN Settings

Edit

Cancel

Finish

- Select the **devices** and specify a naming pattern for the WAN/outside interface. If the devices share the same interface name, using initials is sufficient. Click **Next**, and if the validation is successful, click **Add**. For bulk additions, you can also use the zone name in the same way.

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

Add Bulk Spokes

1 Add Devices

2 Validate Devices

Available Devices \*

🔍 Search

Add

Remove

Selected Devices \*

ftd2

ftd3

ftd4

Select VPN Interface Using \*

Interface Name Pattern

out

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

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

Next

3 Authentication Settings

4 SD-WAN Settings

Cancel Back Add

Cancel Finish

- Verify the spokes and overlay interface details to ensure that the correct interfaces are selected, then click **Next**.

## 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](#)

&lt;&lt;

Viewing 1-3 of 3

&gt;&gt;

## 3 Authentication Settings

Edit

## 4 SD-WAN Settings

Edit

Cancel

Finish

- You can either retain the default parameters for the IPsec configuration or specify custom ciphers as required. Click **Next** to proceed. In this document, you are using the default parameters.

## 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

ftd2	VPN Interface	VPN-OUT-1	Key ID: HUB-Spoke-VPN-Single-ISP_ftd2
ftd3	VPN-OUT-1	Key ID: HUB-Spoke-VPN-Single-ISP_ftd3	
ftd4	VPN-OUT-4	Key ID: HUB-Spoke-VPN-Single-ISP_ftd4	

## 3 Authentication Settings

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-NUL-LSHA-LATEST x ▾

[Show Details](#)[Next](#)

## 4 SD-WAN Settings

Edit

Cancel

Finish

- Finally, you can configure overlay routing within the same wizard for this topology by specifying the appropriate BGP parameters, such as the AS number, inside interface advertisement, and community tags for prefix filtering. Security zone can assist in traffic filtering via access control policies while you can also create an object for interfaces and use them in connected interfaces redistribution if the name is different than inside or is not symmetric across devices in the topology.

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

- 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
--------	------	------	-------------------------	--------------------	-------------	------------------------------	------------------------
- Spokes** [Edit](#)

Device	ftd2	VPN Interface	VPN-OUT-1	Local Tunnel (IKE) Identity	Key ID: HUB-Spoke-VPN-Single-ISP_ftd2
ftd3	VPN-OUT-1		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 (S VTIs) 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 *	Community Tag for Local Routes *
65500	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](#)

- Click **Next**, then **Finish**, and finally **Deploy** to complete the process.

## Verification

- You can verify the tunnel status by navigating to **Devices > VPN > Site to Site**.

Firewall Management Center  
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin 🔒 **SECURE**

Last Updated: 12:06 PM Refresh NAT Exemptions Add

Select...

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEx1	IKEx2
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
fd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynam... (10.18.89.254)	fd2	VPN-OUT-1 (203.0.113.2)	VPN-OUT-1_static... (198.51.100.10)
fd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynam... (10.18.89.254)	fd3	VPN-OUT-1 (203.0.113.3)	VPN-OUT-1_static... (198.51.100.11)
fd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynam... (10.18.89.254)	fd4	VPN-OUT-4 (203.0.113.4)	VPN-OUT-4_static... (198.51.100.12)

Viewing 1-3 of 3

- Additional details can be verified by navigating to **Overview > Dashboards > Site to Site VPN**.


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-ISP

0 0 3

- For further insights, select the tunnel and click **View Full Information**.


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-ISP

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
<b>Topology</b>		
HUB-Spoke-VPN-Single-ISP		
<b>Status</b>		
Active		
<b>Node A</b>		
fd1		
<b>Node B</b>		
fd2		
<b>Node A IP</b>		
203.0.113.1		
<b>Node B IP</b>		
203.0.113.2		
<b>Node A VPN Interface Name</b>		
VPN-OUT-1		
<b>Node B VPN Interface Name</b>		
VPN-OUT-1		
<b>Last Updated</b>		
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 (203.0.113.1/500)	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

- The output is shown directly from the FTD CLI and can be refreshed to display updated counters and important information, such as Security Parameter Index (SPI) details.

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

- The FTD CLI can also be used to check routing information and BGP peering status.

On HUB side

```
<#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

## On Spoke Side

The same verification can be performed on the spoke devices as well. Here is an example from one of the spokes.





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 (Single ISP for Redundant HUB via EBGp Between Secondary HUB and Spokes)**

Network Diagram

