

为通过安全防火墙的站点到站点VPN配置SD-WAN

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[功能信息](#)

[涵盖的拓扑](#)

[集中星型 \(单个ISP\)](#)

[双中心辐射型 \(通过辅助中心辐射和辐射之间的EBGP为冗余中心提供单一ISP\)](#)

[双中心辐射型 \(双ISP通过辅助中心辐射型和辐射型之间的EBGP提供冗余中心和ISP\)](#)

[结论](#)

[相关信息](#)

简介

本文档介绍使用安全防火墙上的SD-WAN功能的BGP重叠路由的基于路由的VPN部署方案。

先决条件

所有集线器和辐条都运行FTD 7.6或更高版本的软件，并通过同样运行7.6或更高版本的软件的FMC进行管理。

要求

Cisco 建议您了解以下主题：

- IKEv2
- 基于路由的VPN
- 虚拟隧道接口(VTI)
- IPsec
- 调试输出中显示“BGP

使用的组件

本文档中的信息基于：

- 思科安全防火墙威胁防御7.7.10
- 思科安全防火墙管理中心7.7.10

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

功能信息

通过使用新的SD-WAN向导，管理中心可简化集中式总部（集线器）和远程分支站点（分支）之间的VPN隧道配置和路由。

- 通过利用集线器上的DVTI（动态虚拟隧道接口）和分支上的SVTI（静态虚拟隧道接口）实现VPN配置自动化，并通过BGP启用重叠路由。

- 自动为分支分配SVTI IP地址并推送完整的VTI配置，包括加密参数。

- 在同一向导内提供简单的一步路由配置，为重叠路由启用BGP。

- 利用BGP的路由反射器属性实现可扩展的最佳路由。

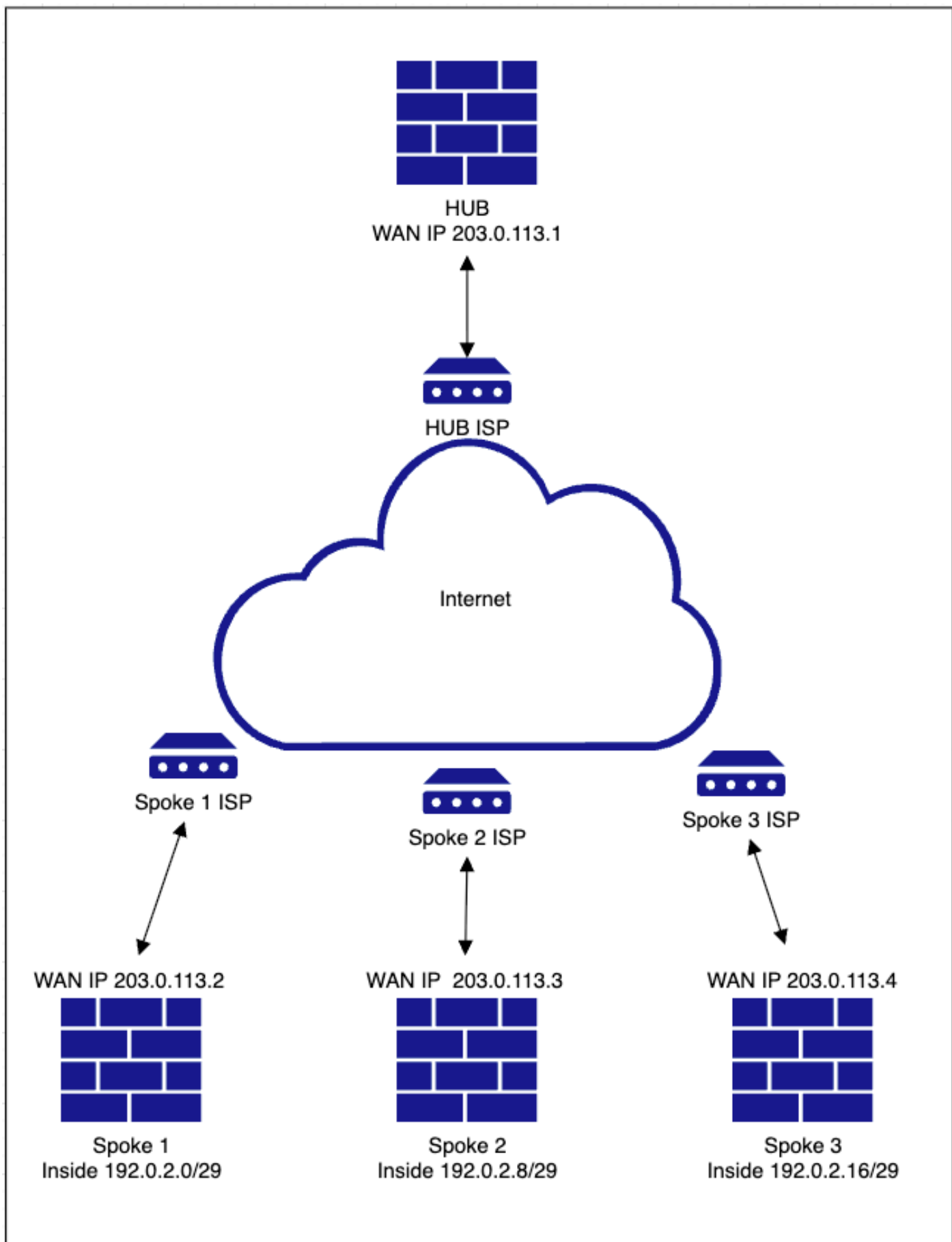
- 允许同时添加多个辐射点，而用户干预最少。

涵盖的拓扑

本文涵盖多个拓扑，以确保用户了解各种部署方案。

集中星型（单个ISP）

网络图



配置

- 导航到设备> VPN > 站点到站点>添加> SD-WAN拓扑> >创建。

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](#)

·添加中心并在中心端创建一个DVTI。作为DVTI配置的一部分，请确保根据拓扑选择正确的隧道源接口。

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.

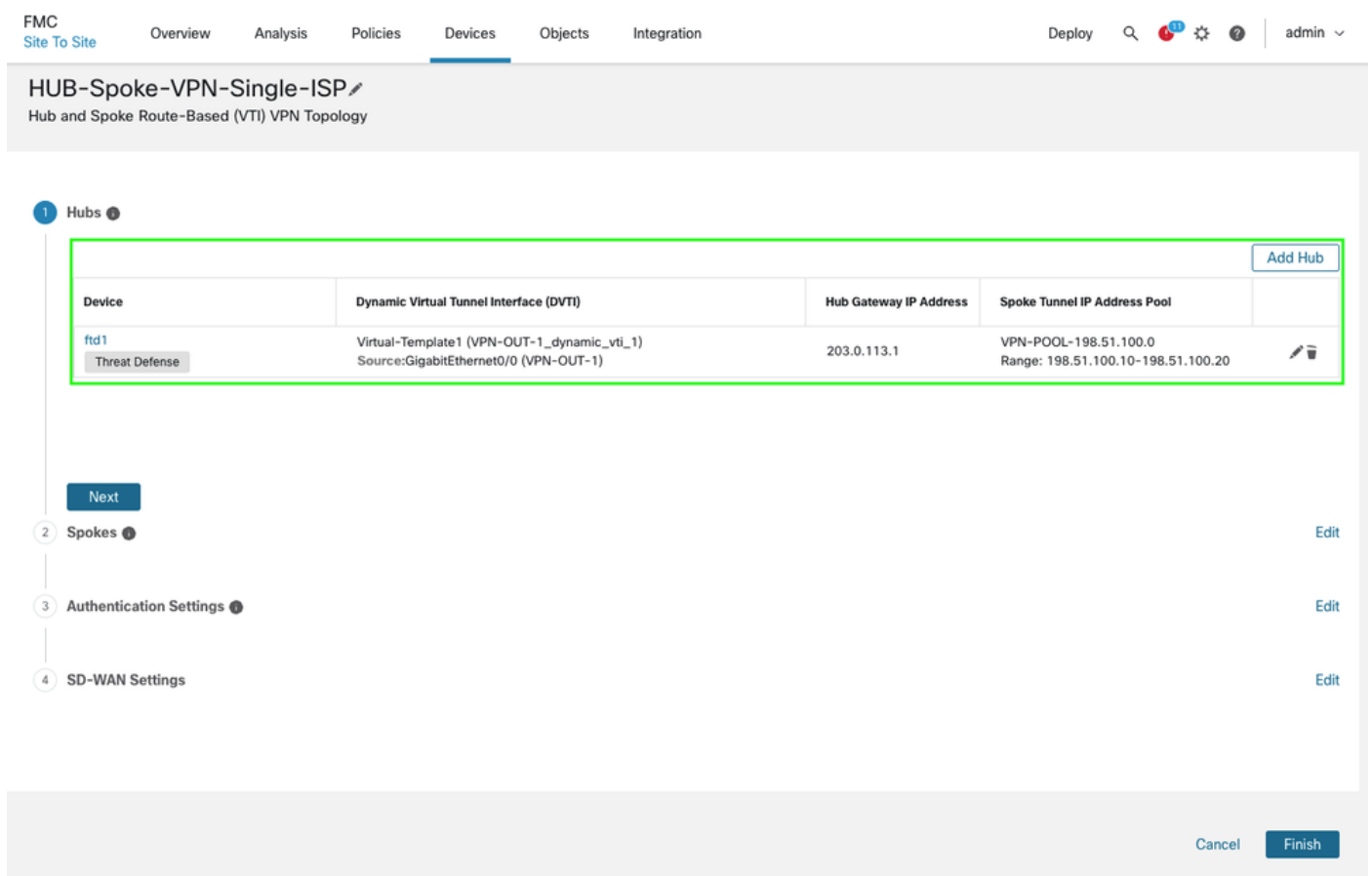
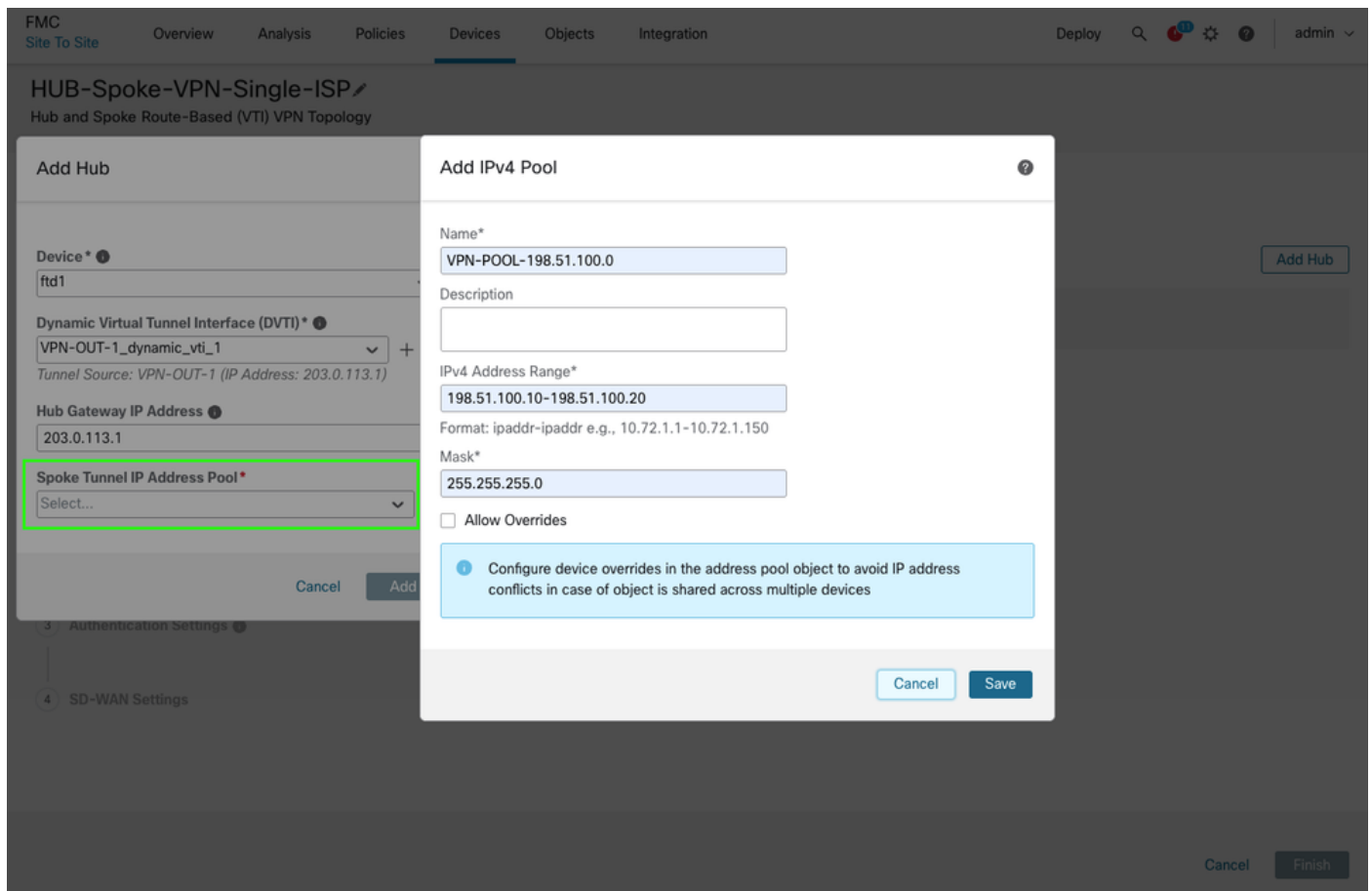
IPsec Tunnel Mode: *
☒ IPv4 ☐ IPv6

IP Address: *
☐ Configure IP
☒ Borrow IP (IP unnumbered) Loopback1 (VPN-Loopback-IB... +

VPN Topology Usage

Cancel OK

- 创建分支隧道IP地址池，然后单击保存，然后单击添加。ip地址池用于将VTI隧道IP地址分配给分支。



- 单击下一步继续并添加辐条。如果您有通用接口/区域名称，则可以利用批量添加选项，也可以单独添加辐条。

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 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

- 选择设备并指定WAN/外部接口的命名模式。如果设备共享相同的接口名称，使用首字母就足够了。单击Next，如果验证成功，则单击Add。对于批量添加，您也可以以相同的方式使用区域名称。

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 🔍 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 ⓘ

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 ⓘ
4 SD-WAN Settings

Spokes (Bulk Addition) Add Spoke Edit
Cancel Finish

- 验证分支和重叠接口详细信息以确保选择了正确的接口，然后单击Next。

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

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

4 SD-WAN Settings

Cancel Finish

- 您可以保留IPsec配置的默认参数，也可以根据需要指定自定义密码。单击 Next (下一步) 继续。在本文档中，您使用的是默认参数。

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

ftd2	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
ftd4 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- SHA-LATEST x Show Details

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

Next

4 SD-WAN Settings

Cancel Finish

- 最后，可以通过指定适当的BGP参数（例如，用于前缀过滤的AS编号、内部接口通告和社区标记），在此拓扑的同一向导内配置重叠路由。安全区域可以通过访问控制策略协助流量过滤，同时您也可以为接口创建一个对象，并在连接的接口重分配中使用它们（如果名称与拓扑中的内部名称不同或不跨拓扑中的设备对称）。

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

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

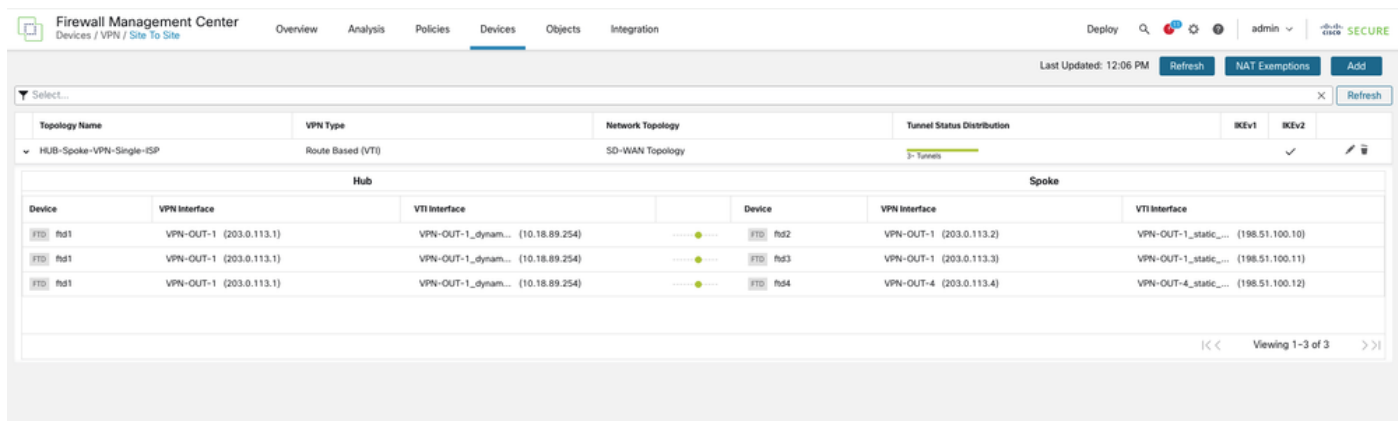
Next You have unsaved changes

Cancel **Finish**

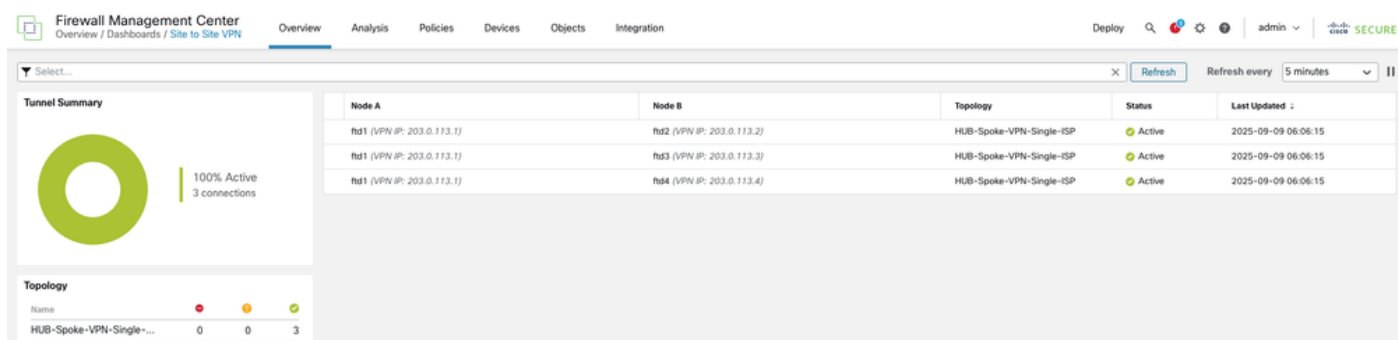
- 单击Next，然后单击Finish，最后单击Deploy完成此过程。

确认

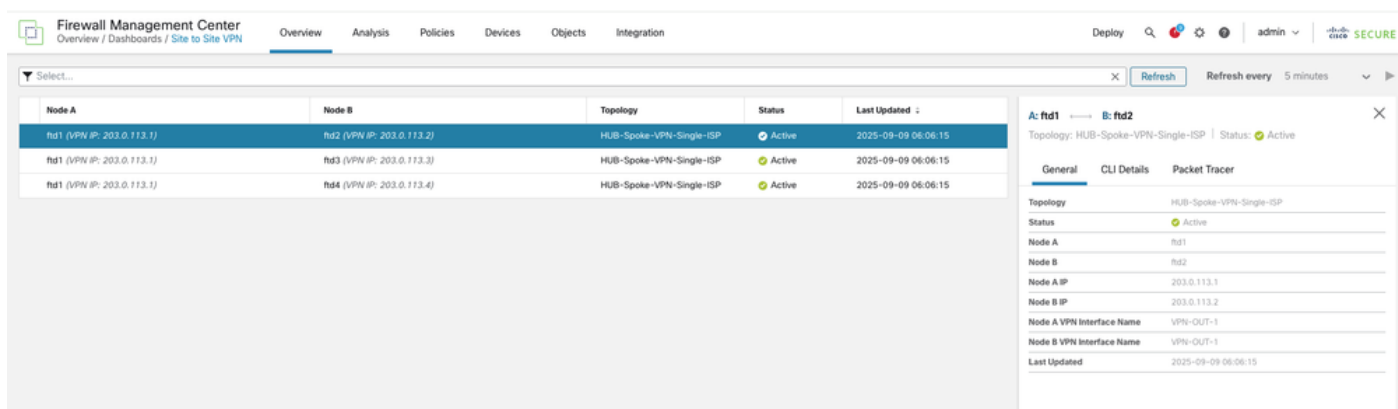
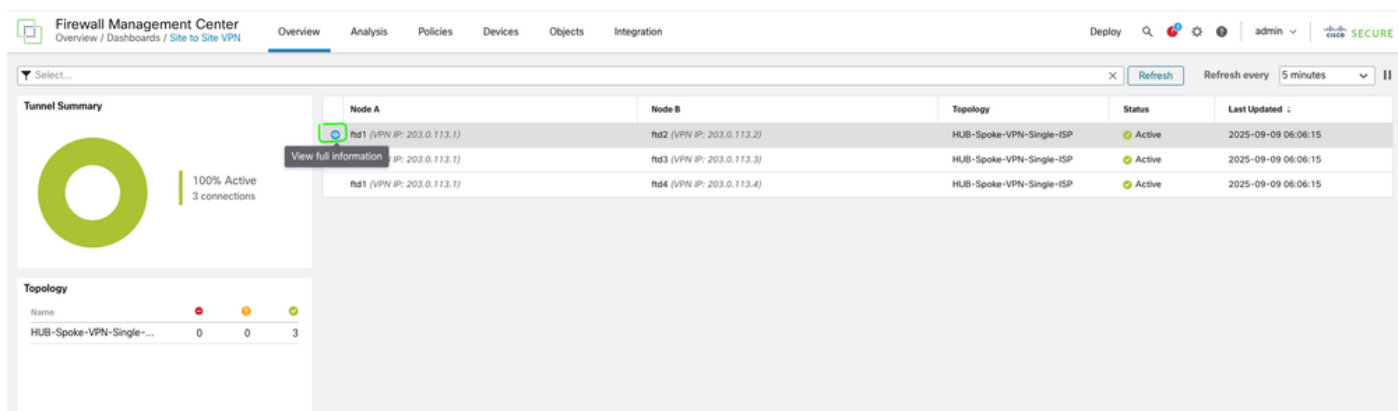
- 您可以通过导航到Devices > VPN > Site to Site来验证隧道状态。



- 通过导航到概述>控制面板>站点到站点VPN，可以验证其他详细信息。



- 要获得进一步的见解，请选择隧道，然后单击查看完整信息。



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 (lrvrf): 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 (lrvrf): 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

- 输出直接从FTD CLI显示，可以刷新以显示更新的计数器和重要信息，如安全参数索引(SPI)详细信息。

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_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 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

- FTD CLI还可用于检查路由信息和BGP对等状态。

在集线器端

```
<#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 receieved 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 receieved 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

在辐射端

也可以在分支设备上执行相同的验证。以下是一个辐条示例。

<#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

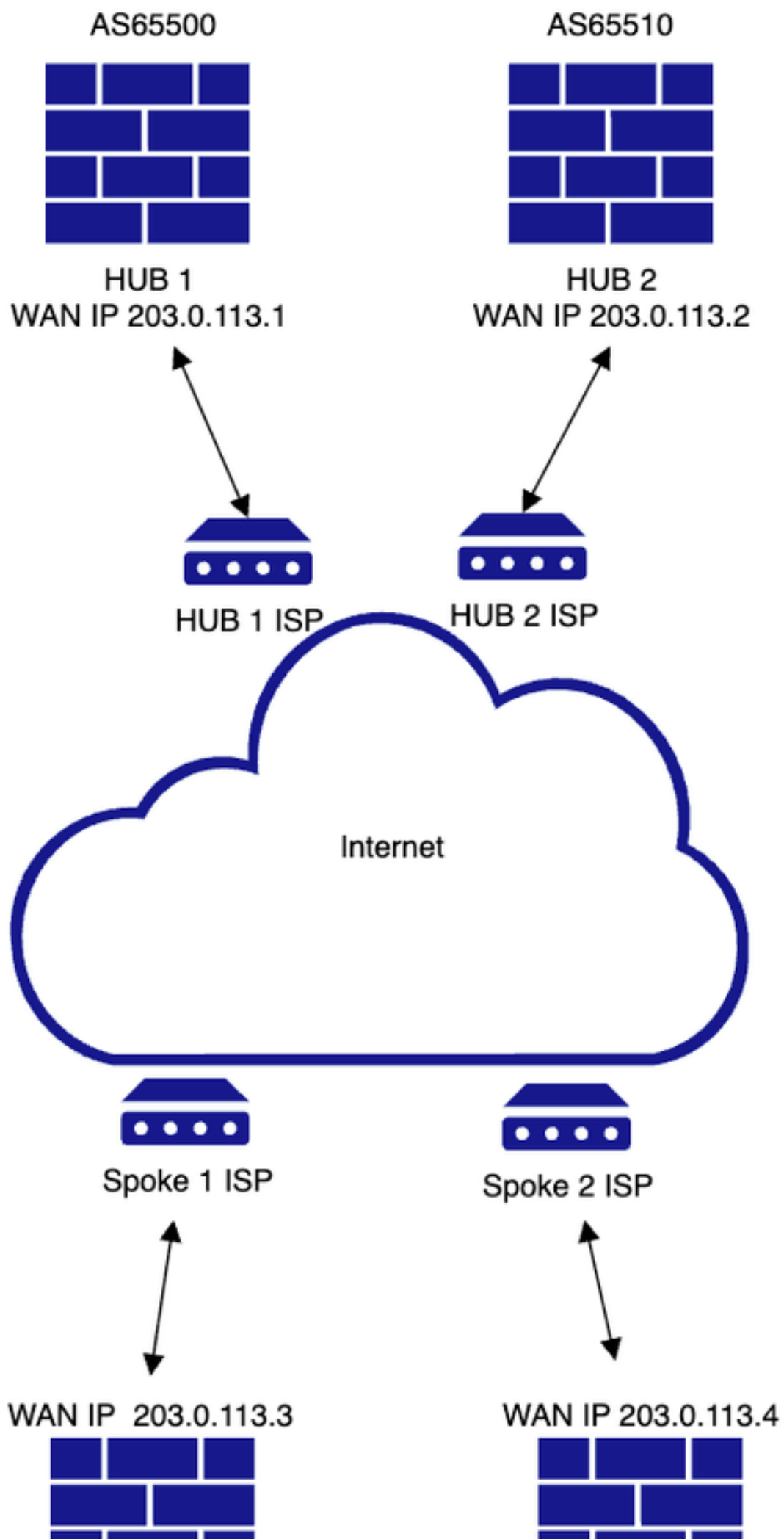
<<<<<<< spoke 2 inside network

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

<<<<<<< spoke 3 inside network

双中心辐射型 (通过辅助中心辐射和辐射之间的EBGP为冗余中心提供单一ISP)

网络图



关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。