

セキュアファイアウォールを介したサイト間VPNのためのSD-WANの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[機能情報](#)

[対象トポロジ](#)

[ハブ&スポーク \(単一のISP\)](#)

[デュアルハブアンドスポーク \(セカンダリハブとスポーク間のEBGPを介した冗長ハブ用のシングルISP\)](#)

[デュアルハブ&スポーク \(冗長ハブ用のデュアルISP、およびセカンダリハブとスポーク間のEBGPを介したISP\)](#)

[結論](#)

[関連情報](#)

はじめに

このドキュメントでは、Secure FirewallのSD-WAN機能を使用したBGPオーバーレイルーティングによるルートベースのVPN導入シナリオについて説明します。

前提条件

すべてのハブとスポークでFTD 7.6以降のソフトウェアが稼働しており、これらのハブとスポークは、7.6以降のソフトウェアが稼働している同じFMC経由で管理されます。

要件

次の項目に関する知識があることが推奨されます。

- IKEv2
- ルートベースのVPN
- 仮想トンネルインターフェイス(VTI)
- IPSec
- BGP

使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Cisco Secure Firewall脅威対策7.7.10
- Cisco Secure Firewall Management Center 7.7.10

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

機能情報

Management Centerは、新しいSD-WANウィザードを使用して、一元化された本社（ハブ）とリモートブランチサイト（スポーク）間のVPNトンネルおよびルーティングの設定を簡素化します。

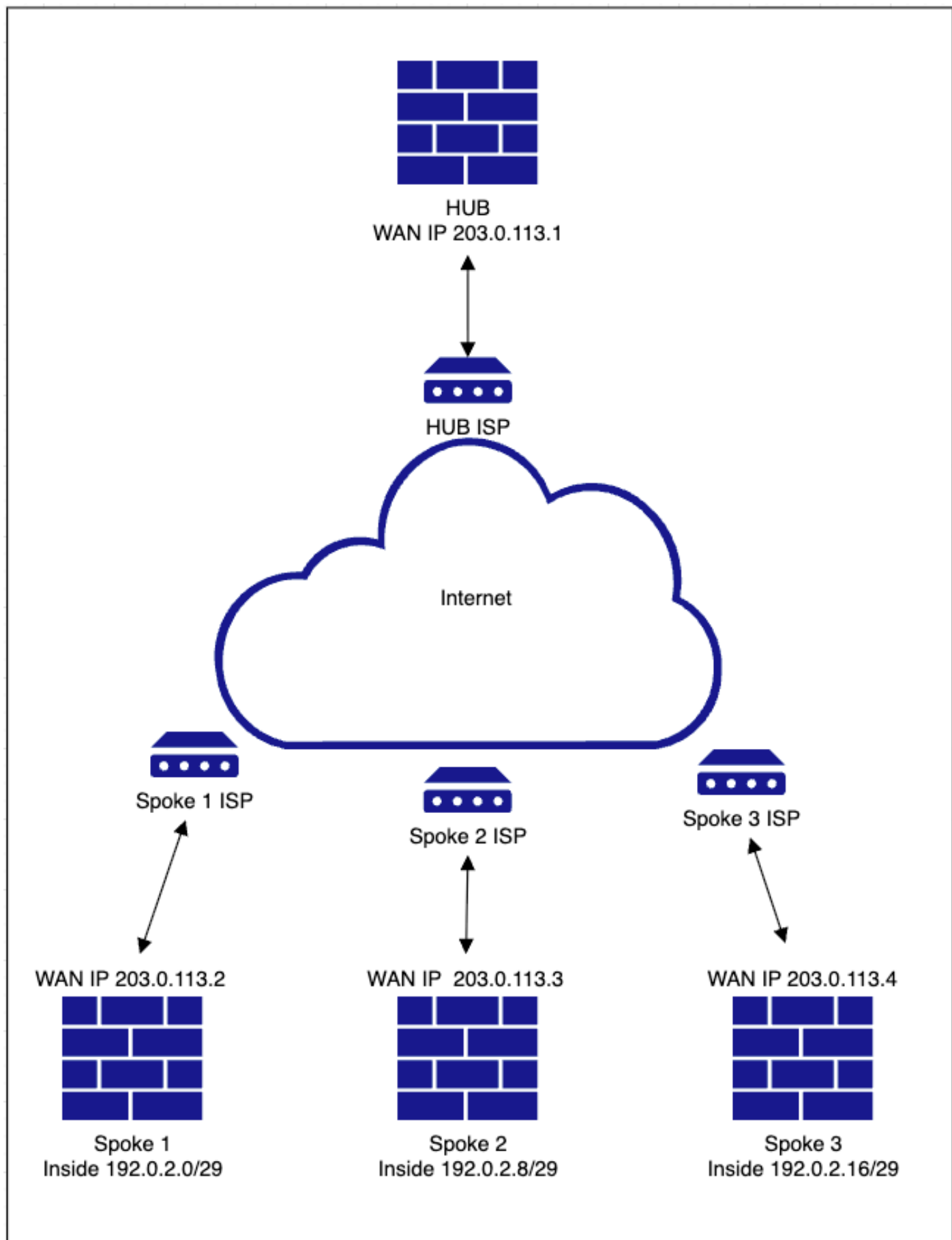
- ハブ上でDVTI(Dynamic Virtual Tunnel Interface)を活用し、スポーク上でSVTI(Static Virtual Tunnel Interface)を活用することでVPN設定を自動化します。オーバーレイルーティングはBGPを介して有効にします。
- スポークにSVTI IPアドレスを自動的に割り当て、暗号化パラメータを含む完全なVTI設定をプッシュします。
- 同じウィザード内で簡単な1ステップのルーティング設定を行い、BGPでオーバーレイルーティングを有効にします。
- BGPのルートリフレクタアトリビュートを活用することにより、スケーラブルで最適なルーティングを可能にします。
- 最小限のユーザ操作で複数のスポークを同時に追加できます。

対象トポロジ

この記事では、ユーザがさまざまな導入シナリオを認識できるように、複数のトポロジについて説明します。

ハブ&スポーク（単一のISP）

ネットワーク図



コンフィギュレーション

- Devices > VPN > Site to Site > Add > SD-WAN Topology > > Createの順に移動します。

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](#)

- ・ ハブを追加し、ハブの終端にDVTIを作成します。DVTI設定の一部として、トポロジに従って正しいトンネル送信元インターフェイスを必ず選択してください。

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

- Spoke Tunnel IP address poolを作成し、SaveをクリックしてからAddをクリックします。IPアドレスプールは、スポークにVTIトンネルIPアドレスを割り当てるために使用されます。

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

Cancel Finish

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

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs 📘

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

Next

2 Spokes 📘 Edit

3 Authentication Settings 📘 Edit

4 SD-WAN Settings Edit

Cancel Finish

- Nextをクリックして続行し、スポークを追加します。共通のインターフェイス/ゾーン名がある場合、またはスポークを個別に追加する場合は、一括追加オプションを利用できます。

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

- デバイスを選択し、WAN/Outsideインターフェイスの命名パターンを指定します。デバイスが同じインターフェイス名を共有する場合は、イニシャルを使用するだけで十分です。Nextをクリックし、検証が正常に終了したらAddをクリックします。一括追加の場合も、同じ方法でゾーン名を使用できます。

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 ① Edit

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

2 Spokes ①

Spokes (Bulk Addition)

Add Spoke

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 ① Edit

4 SD-WAN Settings Edit

Cancel Finish

- スポークとオーバーレイインターフェイスの詳細を確認して正しいインターフェイスが選択されていることを確認し、Nextをクリックします。

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

- IPSec設定のデフォルトパラメータをそのまま使用することも、必要に応じてカスタム暗号を指定することもできます。Next をクリックして続けます。このドキュメントでは、デフォルトのパラメータを使用しています。

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

[Edit](#)

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

2 Spokes

[Edit](#)

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

Transform Sets (IPsec Proposals)*

AES-GCM x

[Show Details](#)

IKEv2 Policies*

AES-GCM-NUL-SSH-LATEST x

[Show Details](#)

Pre-shared Key Length*

24 The range is 1 to 127.

Next

4 SD-WAN Settings

[Edit](#)

Cancel

Finish

- 最後に、AS番号、内部インターフェイスアドバタイズメント、プレフィクスフィルタリングのコミュニティタグなどの適切なBGPパラメータを指定することで、このトポロジに対して同じウィザード内でオーバーレイルーティングを設定できます。セキュリティゾーンは、アクセスコントロールポリシーによるトラフィックフィルタリングに役立ちます。また、インターフェイスのオブジェクトを作成し、名前がトポロジ内のデバイス間で内部と異なる場合、または名前がトポロジ内のデバイス間で対称でない場合は、接続されたインターフェイスの再配布でそれらを使用することもできます。

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

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

Edit

2 Spokes

ftd2 VPN-OUT-1

ftd3 VPN-OUT-1

ftd4 VPN-OUT-4

VPN Interface

VPN Interface

VPN Interface

Local Tunnel (IKE) Identity

Local Tunnel (IKE) Identity

Local Tunnel (IKE) Identity

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

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

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

Edit

3 Authentication Settings

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

Edit

4 SD-WAN Settings

Spoke Tunnel Interface Auto Generation

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

Spoke Tunnel Interface Security Zone

VPN-OUT-1

+

Overlay Routing Configuration

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

☒ Enable BGP on the VPN Overlay Topology

Autonomous System Number *

65500

Community Tag for Local Routes *

101010

☒ Redistribute Connected Interfaces

Default inside*

+

☒ Enable Multiple Paths for BGP

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

Next

You have unsaved changes

Cancel Finish

- Next、Finish、最後にDeployの順にクリックして、プロセスを完了します。

検証

- Devices > VPN > Site to Siteの順に選択して、トンネルのステータスを確認できます。

Firewall Management Center

Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ? admin ▾

Last Updated: 12:06 PM Refresh NAT Exemptions Add

Select...

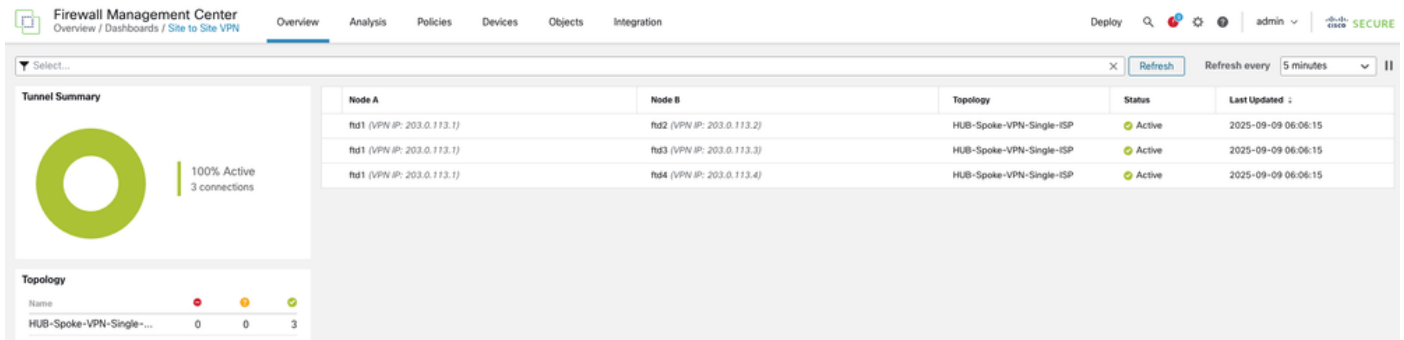
Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
HUB-Spoke-VPN-Single-ISP	Route Based (VTI)	SD-WAN Topology	Tunnels	✓	

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

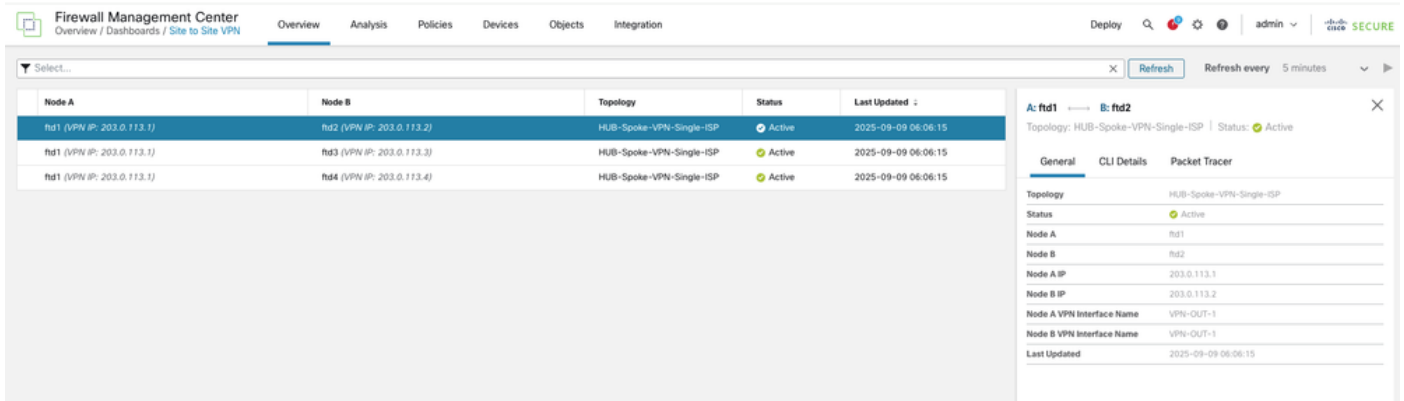
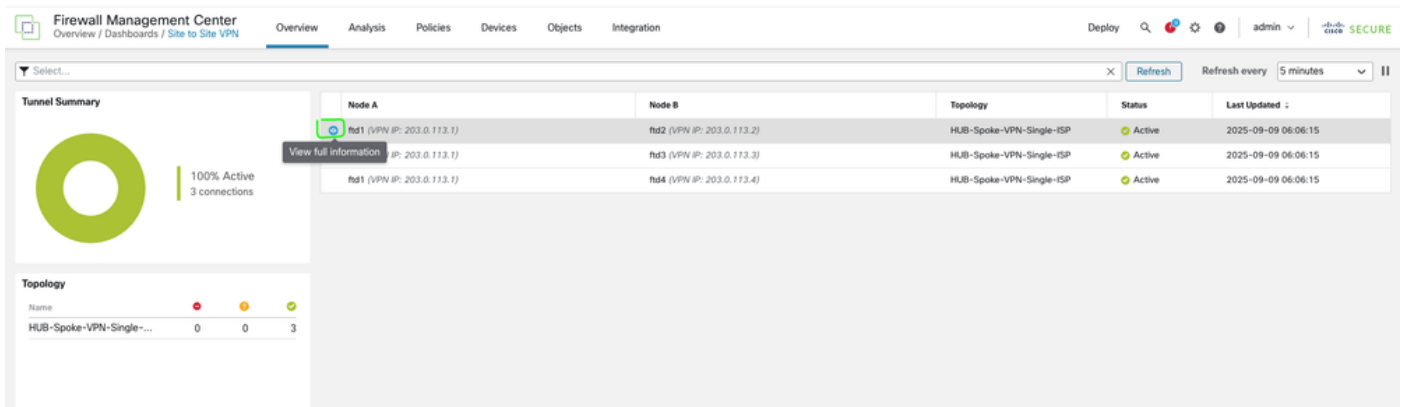
Viewing 1-3 of 3

- その他の詳細については、Overview > Dashboards > Site to Site VPNの順に移動して確認で

きます。



- さらに詳しい情報については、トンネルを選択して、View Full Informationをクリックしてください。



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

```

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)
remote ident (addr/mask/prot/port): (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)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0)
current_peer: 203.0.113.1

```

Viewing 1-3 of 3

- 出力はFTD CLIから直接表示され、更新されたカウンタやセキュリティパラメータインデックス(SPI)の詳細などの重要な情報を表示するために更新できます。

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

- FTD CLIを使用して、ルーティング情報とBGPピアリングステータスを確認することもできます。

ハブ側

<#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

スポーク側

同じ検証をスポークデバイスでも実行できます。スポークの1つの例を次に示します。

<#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

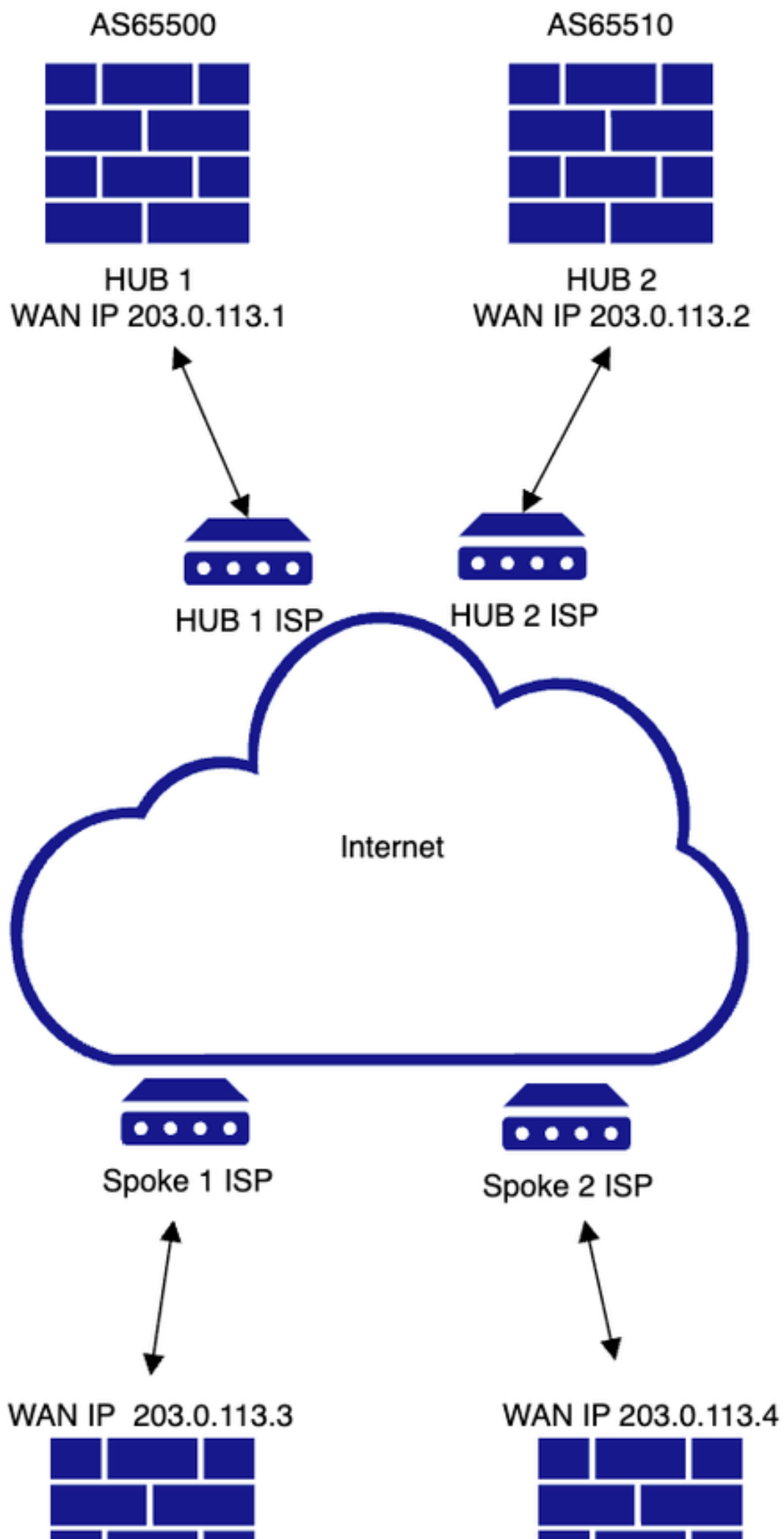
<<<<<<< spoke 2 inside network

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

<<<<<<< spoke 3 inside network

デュアルハブアンドスポーク (セカンダリハブとスポーク間のEBGPを介した冗長
 ハブ用のシングルISP)

ネットワーク図



翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。