

Configurazione di SD-WAN per la VPN da sito a sito su firewall protetto

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Informazioni sulle funzionalità](#)

[Topologie trattate](#)

[HUB e spoke \(ISP singolo\)](#)

[Due hub e spoke \(ISP singolo per hub ridondante tramite EBGp tra hub secondario e spoke\)](#)

[Hub e spoke doppi \(ISP doppio per hub e ISP ridondanti tramite EBGp tra hub e spoke secondari\)](#)

[Conclusioni](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive gli scenari di distribuzione di VPN basate su route con routing di overlay BGP utilizzando la funzione SD-WAN su Secure Firewall.

Prerequisiti

Tutti gli hub e gli spoke eseguono software FTD 7.6 o versioni successive e sono gestiti tramite lo stesso FMC, che esegue anche software 7.6 o versioni successive.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- IKEv2
- VPN basata sul percorso
- VTI (Virtual Tunnel Interfaces)
- IPSec
- BGP

Componenti usati

Le informazioni fornite in questo documento si basano su:

- Cisco Secure Firewall Threat Defense 7.7.10

- Cisco Secure Firewall Management Center 7.7.10

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Informazioni sulle funzionalità

Il Management Center semplifica la configurazione dei tunnel VPN e il routing tra le sedi centrali (hub) e le sedi remote (spoke) utilizzando la nuova procedura guidata SD-WAN.

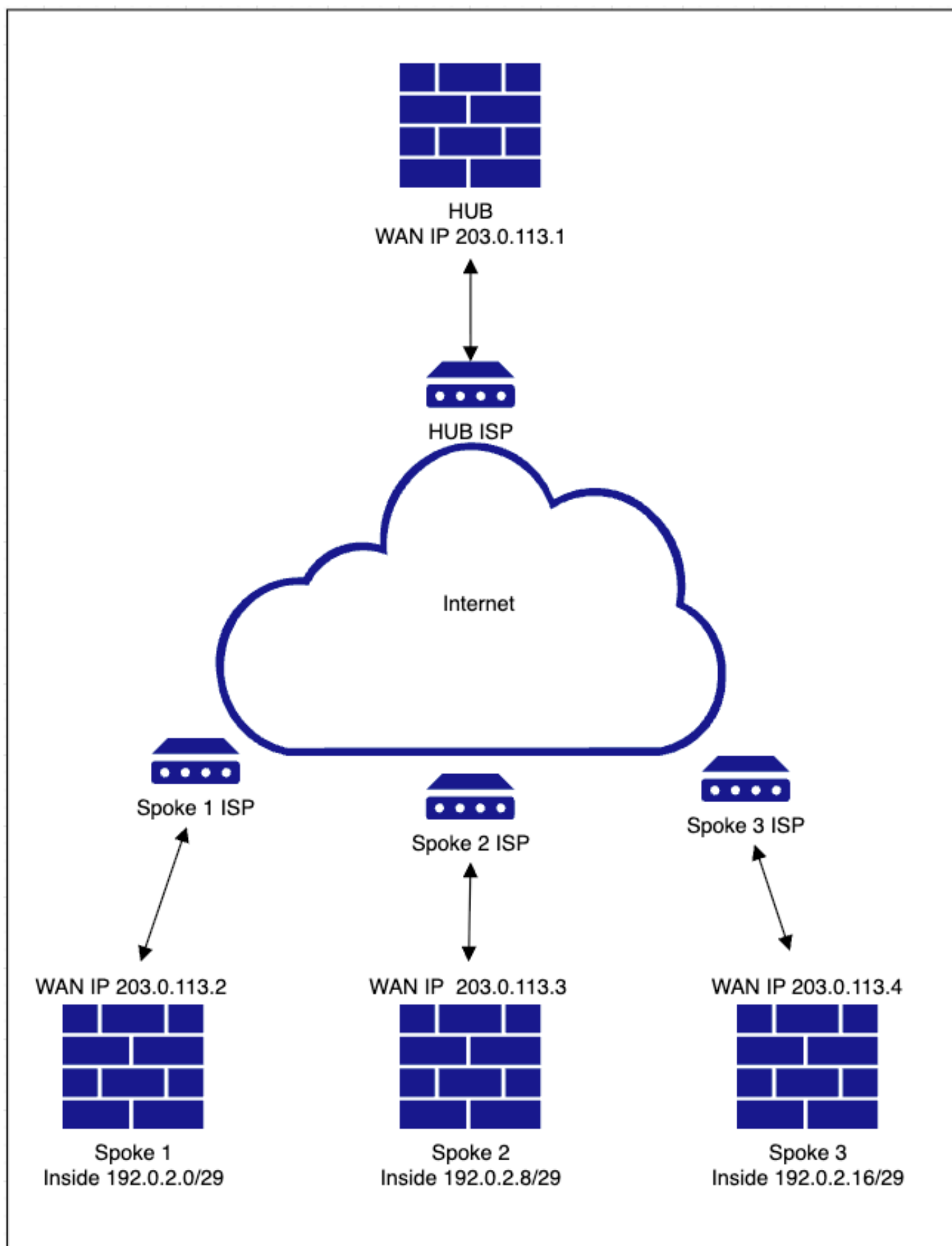
- Automazione della configurazione VPN sfruttando la tecnologia DVTI (Dynamic Virtual Tunnel Interface) sugli hub e la tecnologia SVTI (Static Virtual Tunnel Interface) sugli spoke, con overlay routing abilitato tramite BGP.
- Assegna automaticamente gli indirizzi IP SVTI per gli spoke e attiva la configurazione VTI completa, inclusi i parametri crittografici.
- Fornisce una semplice configurazione del routing in un unico passaggio all'interno della stessa procedura guidata per abilitare BGP per il routing sovrapposto.
- Abilita il routing scalabile e ottimale sfruttando l'attributo route-reflector per BGP.
- Consente l'aggiunta simultanea di più raggi con il minimo intervento da parte dell'utente.

Topologie trattate

In questo articolo vengono illustrate più topologie per garantire che gli utenti siano a conoscenza dei diversi scenari di distribuzione.

HUB e spoke (ISP singolo)

Esempio di rete



Configurazioni

- Selezionare Dispositivi > VPN > Sito in sito > Aggiungi > Topologia SD-WAN > > Crea.

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](#)

- Aggiungere un hub e creare un DVTI all'estremità dell'hub. Come parte della configurazione DVTI, assicurarsi di selezionare l'interfaccia di origine del tunnel corretta in base alla topologia.

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

- Creare un pool di indirizzi IP del tunnel spoke, fare clic su Salva, quindi su Aggiungi. Il pool di indirizzi IP viene utilizzato per assegnare gli indirizzi IP del tunnel VTI agli spoke.

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	

Next

2 Spokes 📘 Edit

3 Authentication Settings 📘 Edit

4 SD-WAN Settings Edit

Cancel Finish

- Fare clic su Next (Avanti) per continuare e aggiungere i raggi. È possibile utilizzare entrambe le opzioni di aggiunta di massa se si dispone di nomi di interfaccia/zona comuni o se si

aggiungono i singoli raggi.

The screenshot shows the FMC Site To Site configuration interface. The top navigation bar includes 'FMC Site To Site', 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The right side has 'Deploy', search, and user 'admin' options. The main title is 'HUB-Spoke-VPN-Single-ISP' with a subtitle 'Hub and Spoke Route-Based (VTI) VPN Topology'. A progress bar on the left shows four steps: 1. Hubs (selected), 2. Spokes, 3. Authentication Settings, and 4. SD-WAN Settings. In the 'Hubs' step, a table lists configuration details: Device (ftd1), DVTI (VPN-OUT-1_dynamic_vti_1), Gateway IP Address (203.0.113.1), and Spoke Tunnel IP Address Pool (VPN-POOL-198.51.100.0). In the 'Spokes' step, there are three buttons: 'View Generated Tunnel Interfaces', 'Add Spokes (Bulk Addition)' (highlighted with a green box), and 'Add Spoke'. Below these buttons is a message: 'No spokes are configured. Add a spoke.' At the bottom left, there is a 'Next' button. At the bottom right, there are 'Cancel' and 'Finish' buttons.

- Selezionare i dispositivi e specificare un modello di denominazione per l'interfaccia WAN/esterna. Se i dispositivi condividono lo stesso nome di interfaccia, è sufficiente utilizzare le iniziali. Fare clic su Avanti e, se la convalida ha esito positivo, fare clic su Aggiungi. Per le aggiunte di massa, potete utilizzare anche il nome della zona nello stesso modo.

FMC
Site To Site

OverviewAnalysisPolicies**Devices**ObjectsIntegration

Deploy 🔍 11 ⚙️ ? admin ▾

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

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

2 Spokes

Next

3 Authentication Settings

4 SD-WAN Settings

Spokes (Bulk Addition)

Add Spoke

Edit

Edit

Cancel

Finish

1 Add Devices

2 Validate Devices

Available Devices *

Add

Remove

Selected Devices *

ftd2

ftd3

ftd4

Select VPN Interface Using *

☒ Interface Name Pattern

☐ Security Zone

Select...

+

Cancel

Next

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

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs Edit

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

2 Spokes Edit

1 Add Devices

2 Validate Devices

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

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

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

Spokes (Bulk Addition) Add Spoke

Next

3 Authentication Settings Edit

4 SD-WAN Settings Edit

Cancel Back Add

Cancel Finish

- Verificare i dettagli dell'interfaccia spoke e overlay per assicurarsi che siano selezionate le interfacce corrette, quindi fare clic su Next (Avanti).

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

- È possibile mantenere i parametri predefiniti per la configurazione IPsec o specificare cifrature personalizzate in base alle esigenze. Fare clic su Next (Avanti) per continuare. In questo documento vengono utilizzati i parametri predefiniti.

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

- Infine, è possibile configurare il routing di overlay all'interno della stessa procedura guidata per questa topologia specificando i parametri BGP appropriati, ad esempio il numero AS, l'annuncio dell'interfaccia interna e i tag della community per il filtro dei prefissi. L'area di sicurezza può essere utile per il filtro del traffico tramite i criteri di controllo di accesso, mentre è possibile creare un oggetto per le interfacce e utilizzarlo nella redistribuzione delle interfacce connesse se il nome è diverso da quello interno o non è simmetrico tra i dispositivi nella topologia.

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

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

- Per completare il processo, fare clic su Avanti, quindi su Fine e infine su Distribuisci.

Verifica

- Per verificare lo stato del tunnel, selezionare Dispositivi > VPN > Sito in sito.

Firewall Management Center

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ? admin ▾

Last Updated: 12:06 PM Refresh NAT Exemptions Add

Select...

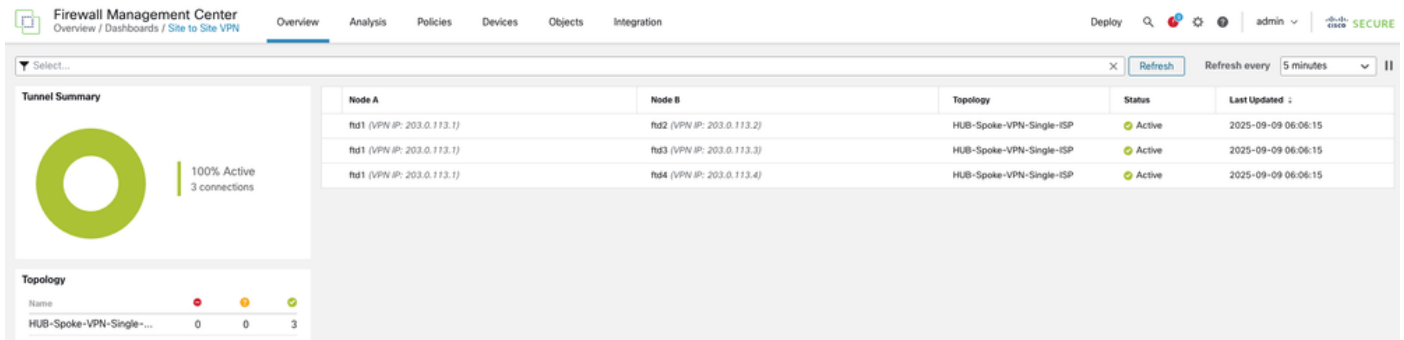
Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
HUB-Spoke-VPN-Single-ISP	Route Based (VTI)	SD-WAN Topology	Tunnels	✓	

Hub			Spoke		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynamic_vti_1 (10.18.89.254)	ftd2	VPN-OUT-1 (203.0.113.2)	VPN-OUT-1_static_vti_1 (198.51.100.10)
ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynamic_vti_1 (10.18.89.254)	ftd3	VPN-OUT-1 (203.0.113.3)	VPN-OUT-1_static_vti_1 (198.51.100.11)
ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynamic_vti_1 (10.18.89.254)	ftd4	VPN-OUT-4 (203.0.113.4)	VPN-OUT-4_static_vti_1 (198.51.100.12)

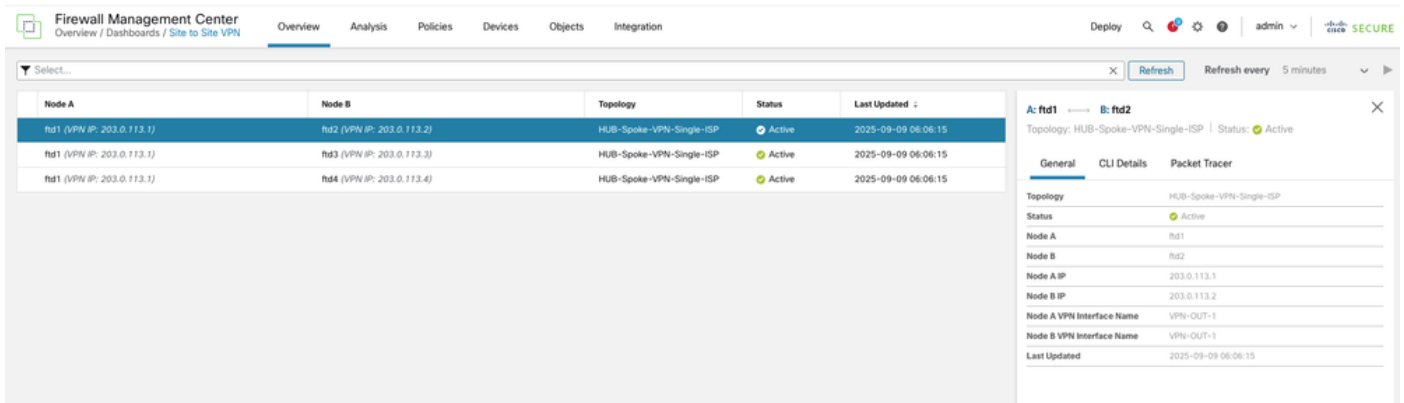
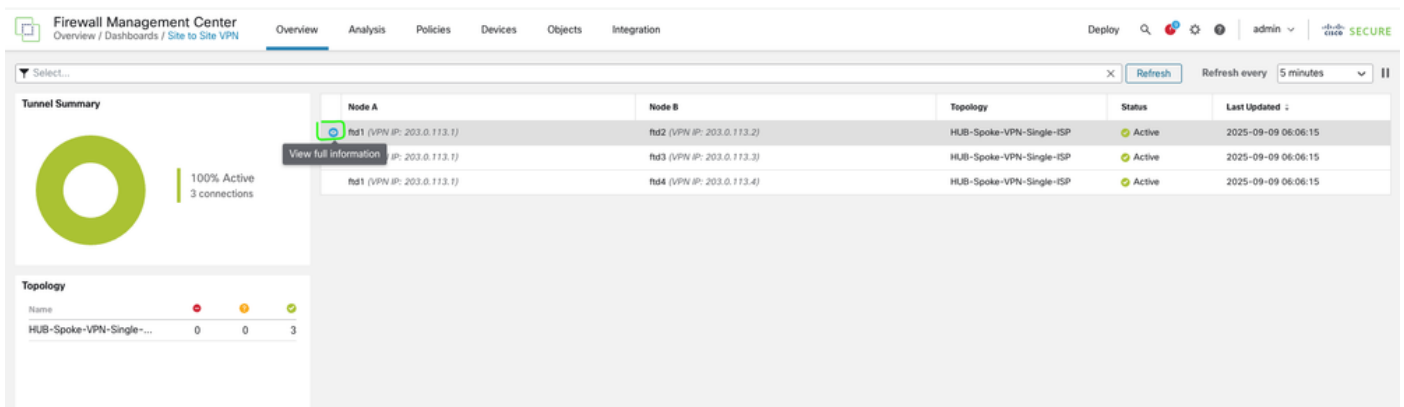
Viewing 1-3 of 3

- È possibile verificare ulteriori dettagli selezionando Panoramica > Dashboard > VPN da sito

a sito.



- Per ulteriori informazioni, selezionare il tunnel e fare clic su Visualizza informazioni complete.



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): (0.0.0.0/0.0.0.0/0/0)
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

- L'output viene visualizzato direttamente dalla CLI FTD e può essere aggiornato per visualizzare contatori aggiornati e informazioni importanti, quali i dettagli SPI (Security Parameter Index).

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

- La CLI di FTD può essere utilizzata anche per controllare le informazioni di routing e lo stato del peering BGP.

Sul lato dell'hub

<#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

Su lato raggio

La stessa verifica può essere eseguita anche sui dispositivi spoke. Ecco un esempio da uno dei raggi.

<#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

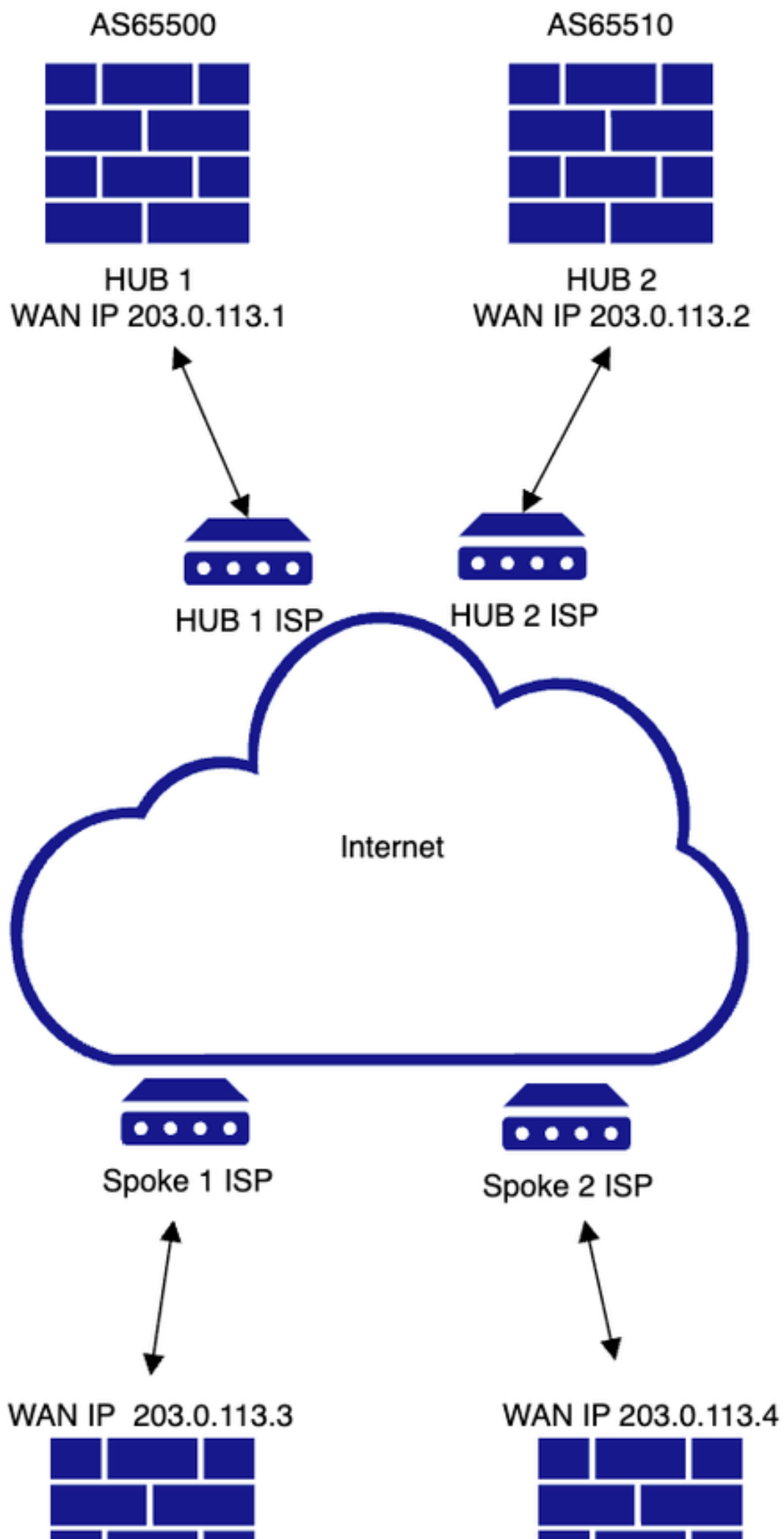
<<<<< spoke 2 inside network

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

<<<<< spoke 3 inside network

Due hub e spoke (ISP singolo per hub ridondante tramite EBGP tra hub secondario e spoke)

Esempio di rete



Dopo aver aggiunto il primo HUB, procedere con l'aggiunta del secondo HUB seguendo la stessa procedura utilizzata in precedenza per HUB1.

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

Dual-HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Add Hub

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

Next

- Continuare con la creazione della DVTI (Dynamic Virtual Tunnel Interface).

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

Dual-HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

Add Hub

Add Virtual Tunnel Interface

Add Loopback Interface

- È necessario un nuovo pool di indirizzi IP per i tunnel VTI HUB 2 sul lato spoke. Creare e configurare il nuovo pool, quindi salvare le modifiche.

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 24

4 SD-WAN Settings

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

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

- Per configurare il peering eBGP tra il secondo HUB e gli spoke, modificare le impostazioni SD-WAN nel passaggio finale. Abilitare l'opzione L'hub secondario si trova in un sistema autonomo diverso e specificare il numero del sistema autonomo (AS) per l'hub secondario. È inoltre possibile utilizzare IBGP se non vi sono limitazioni all'uso di un numero AS diverso nell'ambiente, lasciando deselezionata l'opzione Hub secondario in un sistema autonomo diverso. In questo modo, viene inviato lo stesso tag community e lo stesso numero AS anche per l'hub secondario. L'articolo è incentrato su eBGP per la configurazione corrente.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin | **SECURE**

Dual-HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

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

Edit

2 Spokes

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

Edit

3 Authentication Settings

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

Edit

4 SD-WAN Settings

Spoke Tunnel Interface Auto Generation

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

Spoke Tunnel Interface Security Zone

VPN-OUT-1 x v +

Overlay Routing Configuration

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

☒ Enable BGP on the VPN Overlay Topology

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

☒ Redistribute Connected Interfaces

Default inside* v +

☒ Secondary Hub is in different Autonomous System

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

☒ Enable Multiple Paths for BGP

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

Next

You have unsaved changes

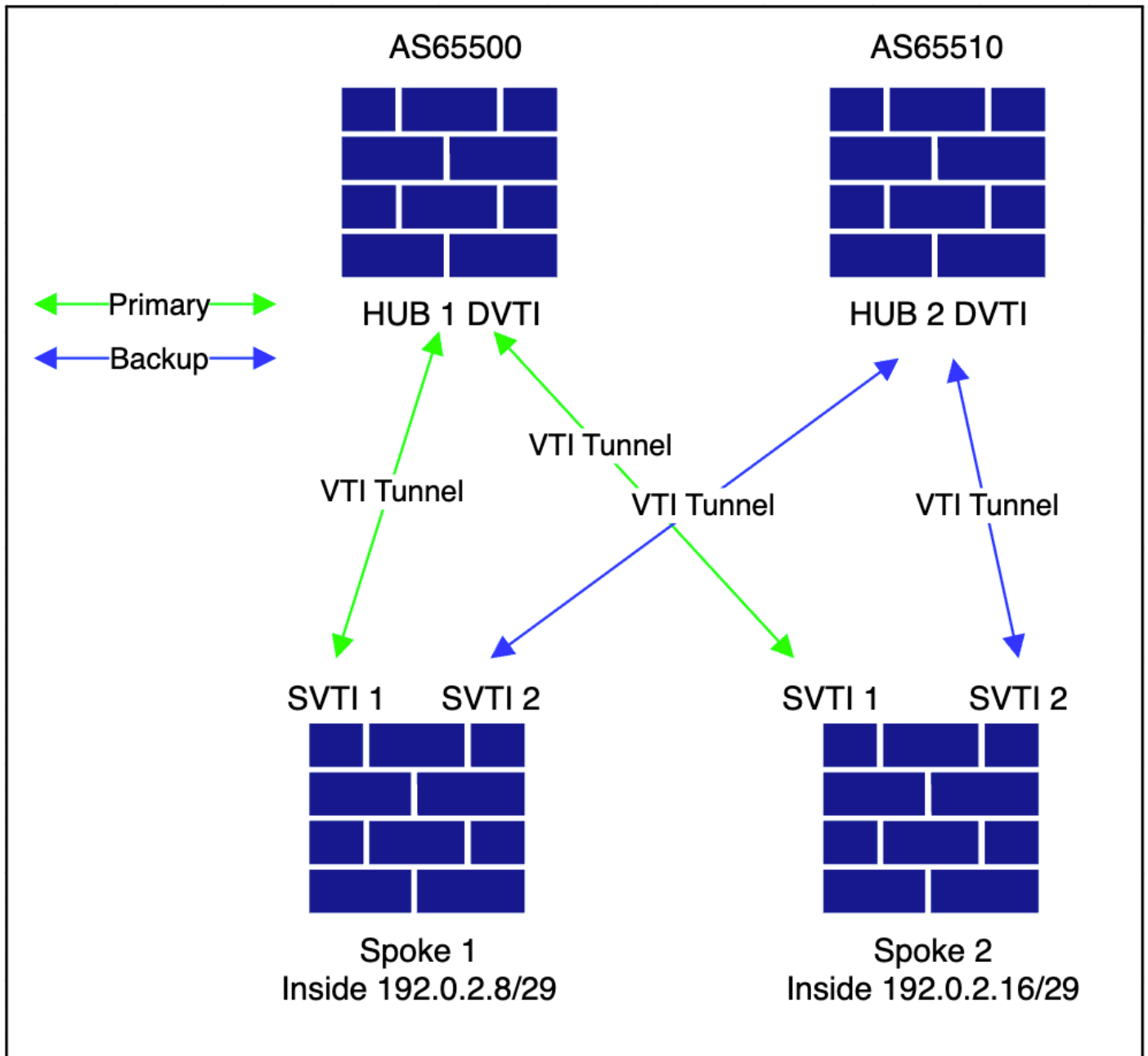
Cancel

Finish

Verificare che il numero Autonomous System (AS) e il tag community siano univoci in questa configurazione.

Verifica

Il diagramma mostra la topologia di sovrapposizione.



- Nel FMC, selezionare Devices > VPN > Site to Site (Dispositivi > VPN > Da sito a sito).

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾ SECURE

Last Updated: 02:20 PM [Refresh](#) [NAT Exemptions](#) [Add](#)

Select... X [Refresh](#)

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

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

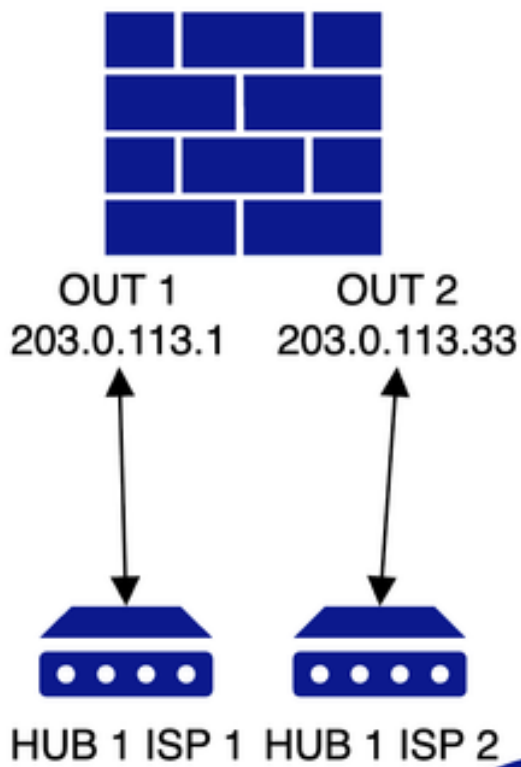
<< Viewing 1-4 of 4 >>

- Tutti gli altri passaggi rimangono invariati.

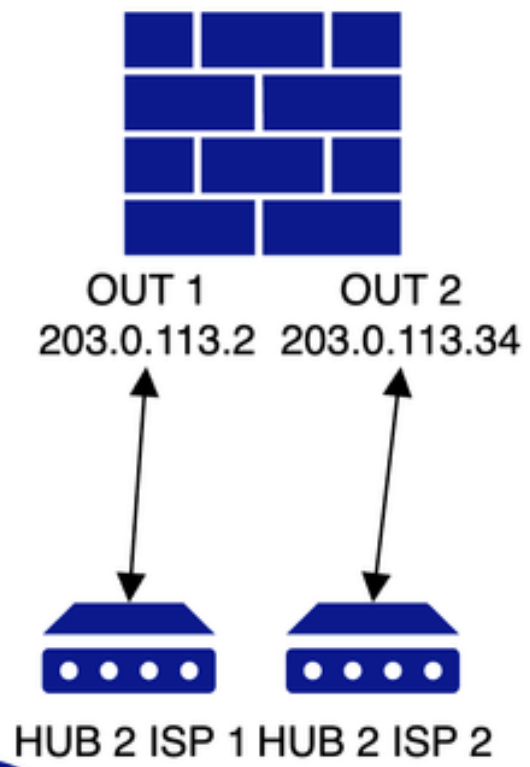
Hub e spoke doppi (ISP doppio per hub e ISP ridondanti tramite EBGp tra hub e spoke secondari)

Esempio di rete

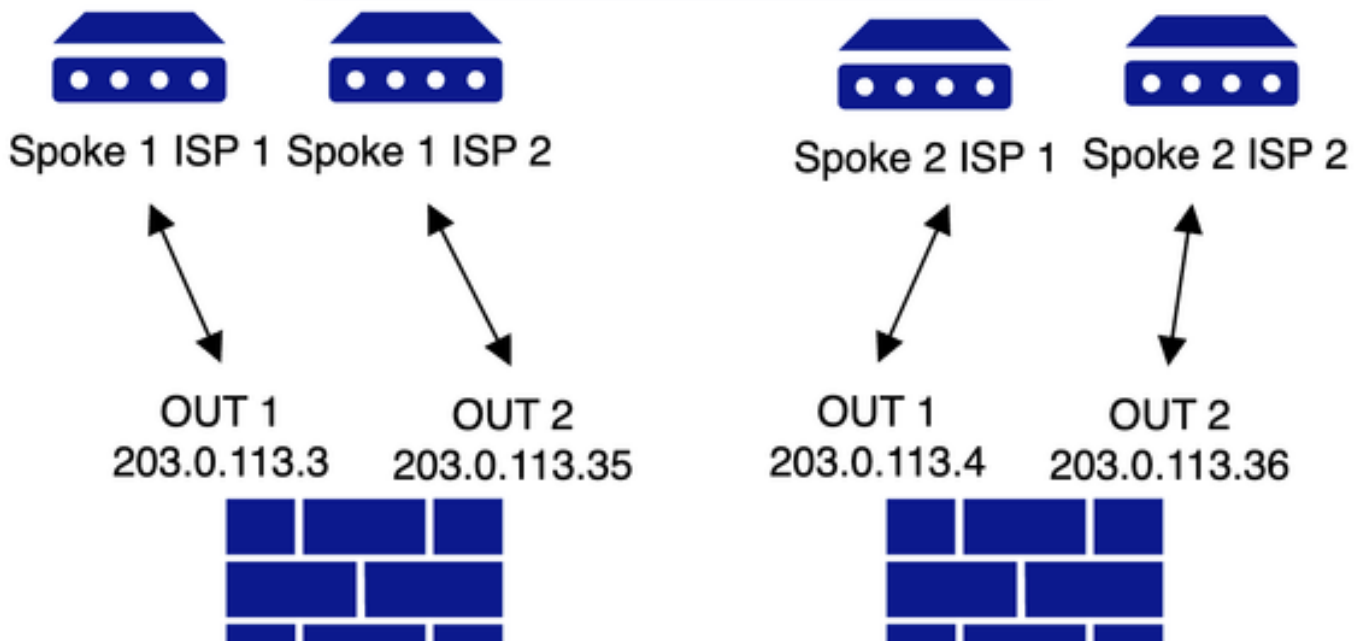
AS65500



AS65510



Internet



La distribuzione per questa topologia viene ignorata utilizzando il primo ISP, poiché tale argomento è trattato nella topologia precedente.

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

- Quindi, procedere all'aggiunta della seconda topologia creando due interfacce DVTI aggiuntive per HUB, ciascuna utilizzando l'interfaccia sottostante per ISP 2 (VPN-OUT-2).

The screenshot shows the Firewall Management Center interface with the 'Dual-HUB-Spoke-VPN-Dual-ISP-2' topology selected. The 'Add Virtual Tunnel Interface' dialog is open, showing the 'General' tab. The 'Tunnel Type' is set to 'Dynamic'. The 'Name' is 'VPN-OUT-1_dynamic_vti_2'. The 'Enabled' checkbox is checked. The 'Security Zone' is set to 'GigabitEthernet0/1 (VPN-OUT-2)'. The 'Priority' is 0. The 'Virtual Tunnel Interface Details' section shows 'Template ID' as 2. The 'Tunnel Source' is 'GigabitEthernet0/1 (VPN-OUT-2)' with IP address '203.0.113.33'. The 'IPsec Tunnel Details' section shows 'IPsec Tunnel Mode' as 'IPv4'. The 'IP Address' is '169.254.2.1/30'. The 'Borrow IP (IP unnumbered)' option is selected, and the 'Loopback2 (VPN-2-LOOPBACK...)' is chosen.

- È stato effettuato il provisioning di un pool di indirizzi IP VPN aggiuntivo specifico per gli indirizzi VTI (Virtual Tunnel Interface) spoke.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾

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

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs ⓘ

2 Spokes ⓘ

3 Authentication Settings ⓘ

4 SD-WAN Settings

Next

Add Hub

Device *

Dynamic Virtual Tunnel Interface (DVTI) * + ✎
Tunnel Source: VPN-OUT-2 (IP Address: 203.0.113.33)

Hub Gateway IP Address

Spoke Tunnel IP Address Pool * x ▾ +

Cancel Add

Cancel Finish

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾

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

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs ⓘ

2 Spokes ⓘ

3 Authentication Settings ⓘ

4 SD-WAN Settings

Next

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

Spokes ⓘ

Authentication Settings ⓘ

SD-WAN Settings

Edit Edit Edit

Cancel Finish

- Per aggiungere un hub secondario, ripetere il processo creando DVTI 2 utilizzando l'interfaccia ISP secondaria (VPN-OUT-2) e configurare un pool IP aggiuntivo per gli indirizzi VTI spoke-end.

Firewall Management Center
Devices / VPN / Site To Site

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

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

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

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

2 Spokes

3 Authentication Settings

4 SD-WAN Settings

Add Hub

Device *
ftd2

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

Hub Gateway IP Address

Cancel Add

Add Virtual Tunnel Interface

General Path Monitoring

Tunnel Type
☐ Static ☒ Dynamic

Name:*
VPN-OUT-1_dynamic_vti_2

☒ Enabled

Description:

Security Zone:
VPN-OUT-2

Priority:
0 (0 - 65535)

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

Template ID:*
2 (1 - 10413)

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

IPsec Tunnel Details
IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*
☒ IPv4 ☐ IPv6

IP Address:*
☐ Configure IP 169.254.2.1/30
☒ Borrow IP (IP unnumbered) Loopback2 (VPN-2-LOOPBACK) +

Cancel OK

Firewall Management Center
Devices / VPN / Site To Site

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

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

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

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

2 Spokes

3 Authentication Settings

4 SD-WAN Settings

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

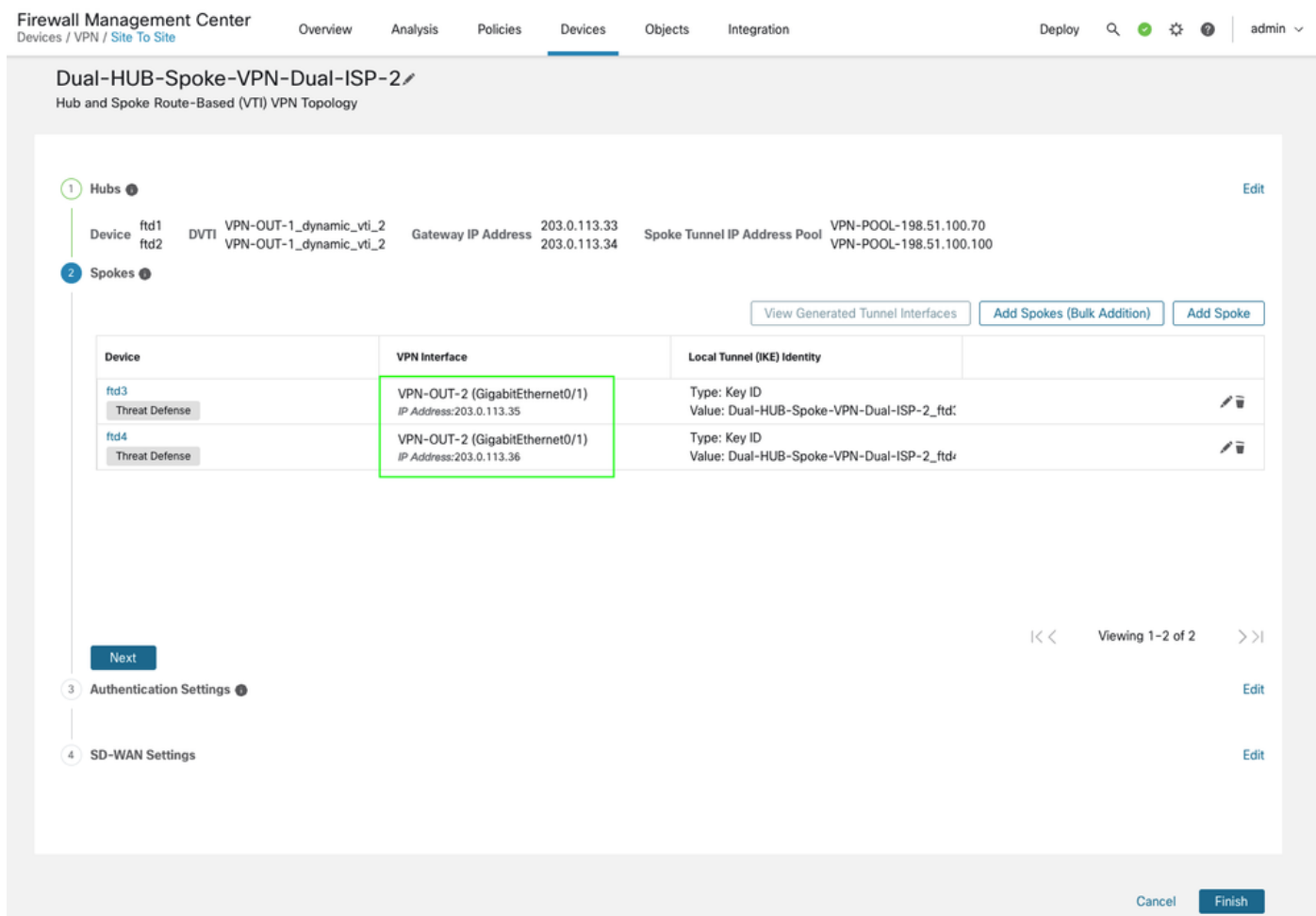
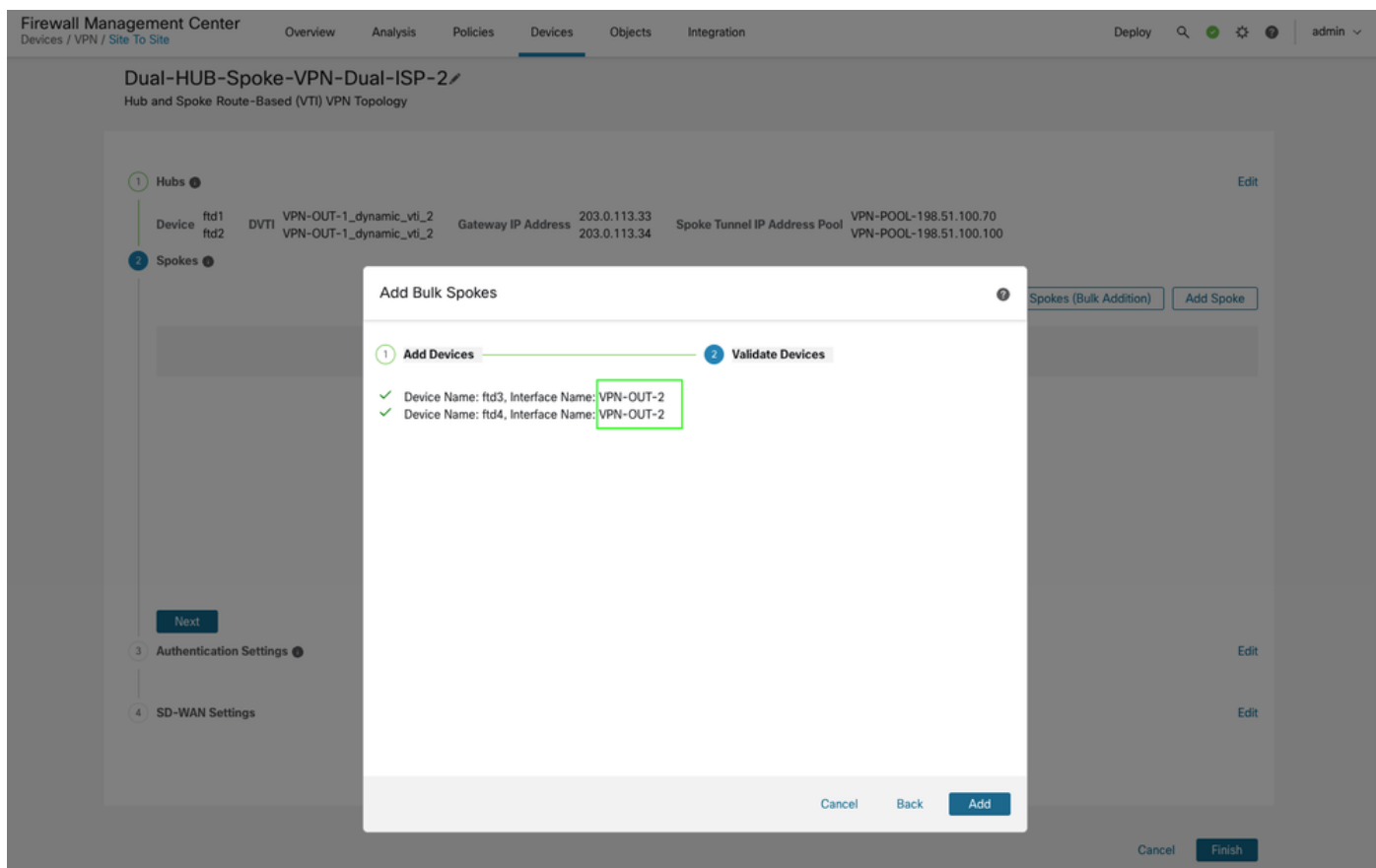
Spoke Tunnel IP Address Pool*
VPN-POOL-198.51.100.100 x +

Cancel Add

Next

Finish

- Quando si aggiunge uno spoke, accertarsi che sia specificata l'interfaccia WAN/underlay corretta per i tunnel VTI. Questa topologia utilizza l'interfaccia ISP secondaria VPN-OUT-2.



- Quando si configura il routing, verificare che i tag della community e i numeri AS per

entrambi gli HUB in questa topologia siano coerenti con quelli utilizzati nella topologia ISP1 precedente. La topologia utilizza aree di sicurezza diverse, ma le configurazioni rimanenti, come i numeri AS per gli HUB primario e secondario, insieme ai tag della community sono le stesse. Questa operazione è obbligatoria per il completamento della convalida della topologia da parte dell'interfaccia utente.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 🟢 ⚙️ ⓘ admin ▾

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

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs

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

Edit

2 Spokes

Device ftd3
ftd4 VPN Interface VPN-OUT-2
VPN-OUT-2 Local Tunnel (IKE) Identity Key ID: Dual-HUB-Spoke-VPN-Dual-ISP-2_ftd3
Key ID: Dual-HUB-Spoke-VPN-Dual-ISP-2_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-2 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* +

☒ 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

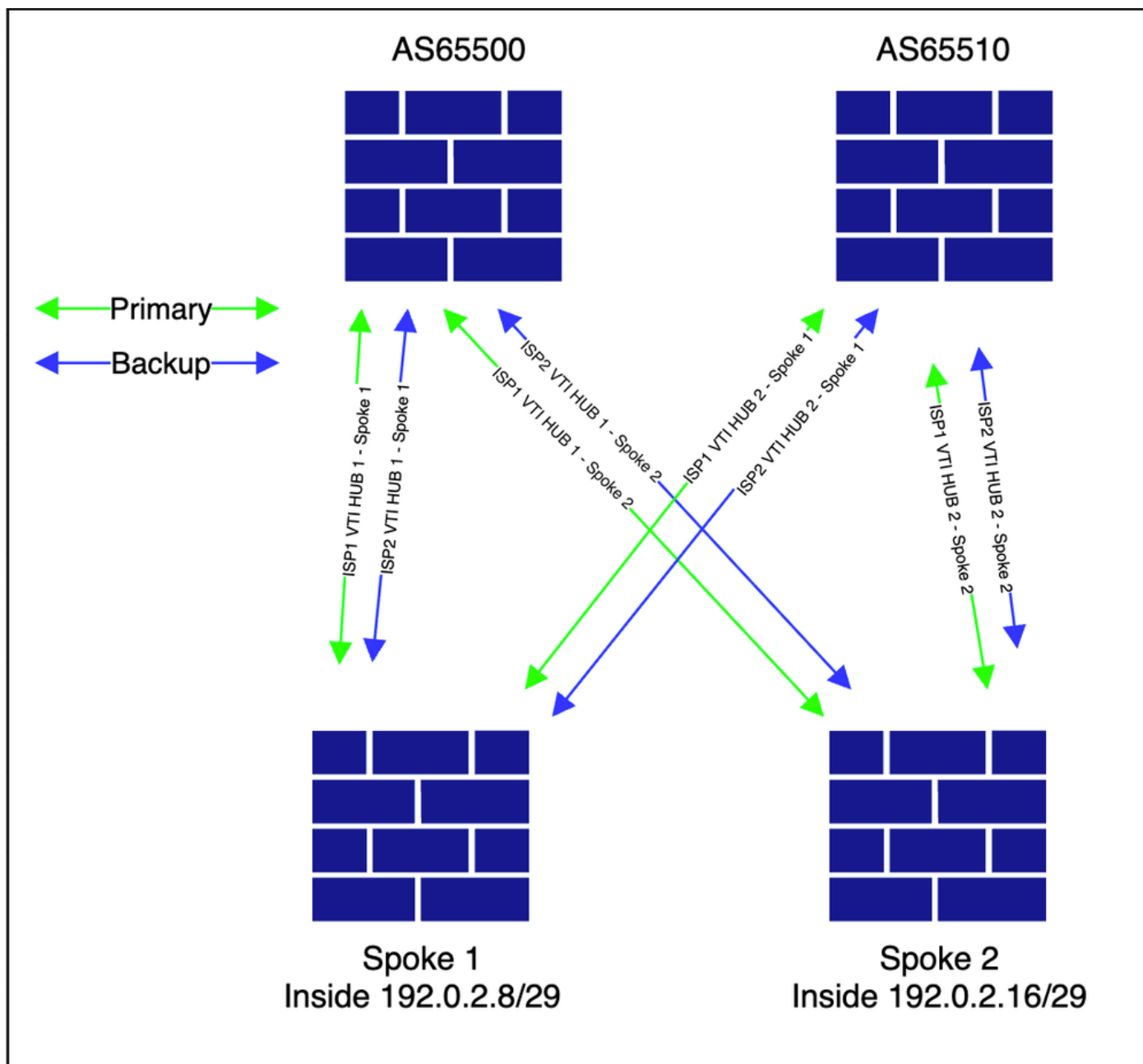
Cancel

Finish

- Tutte le altre impostazioni rimangono invariate. Completare la procedura guidata e procedere con la distribuzione.

Verifica

- La topologia viene visualizzata come illustrato.



- Passare a Dispositivi > VPN > Da sito a sito per visualizzare la topologia.

<<<<<<<<< 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 via

BGP table version is 4, local router ID is 203.0.113.35

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

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

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

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

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

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

Total number of prefixes 2

La tabella di routing viene visualizzata come mostrato per confermare che il traffico è con carico bilanciato tra entrambi i collegamenti sul lato spoke.

<#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

Conclusioni

Lo scopo di questo articolo è quello di spiegare vari scenari di distribuzione che possono essere facilmente implementati utilizzando una singola procedura guidata di installazione.

Informazioni correlate

- Per ulteriore assistenza, contattare TAC. È necessario un contratto di supporto valido: [Contatti del supporto Cisco internazionali](#).
- [Qui](#) è possibile anche visitare la Cisco VPN Community.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).