

Configurazione della topologia a doppio ISP con due hub e quattro spoke nella stessa area

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Piattaforme software e hardware supportate](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Passaggio 1. Creare una topologia SD-WAN con WAN-1 come interfaccia VPN](#)

[Passaggio 2. Configurare la funzionalità DVTI \(Dynamic Virtual Tunnel Interface\) sull'hub primario](#)

[Passaggio 3. Configurare la funzionalità DVTI \(Dynamic Virtual Tunnel Interface\) sull'hub secondario](#)

[Passaggio 4. Configurazione dei raggi](#)

[Passaggio 5. Configurazione delle impostazioni di autenticazione](#)

[Passaggio 6. Configurare le impostazioni SD-WAN](#)

[Passaggio 7. Creare una topologia SD-WAN con WAN-2 come interfaccia VPN](#)

[Passaggio 8. Configurazione delle zone ECMP](#)

[Passaggio 9. Modificare la preferenza locale BGP sull'hub](#)

[Verifica](#)

[Verifica degli stati del tunnel](#)

[Verifica interfacce tunnel virtuale](#)

[Verifica del bilanciamento del carico del traffico VPN](#)

[Verifica della ridondanza di due ISP](#)

[Verifica ridondanza a livello di hub](#)

Introduzione

Questo documento descrive come configurare una topologia con due ISP con due hub e quattro spoke nella stessa area usando la procedura guidata SD-WAN.

Prerequisiti

Piattaforme software e hardware supportate

Responsabile	FTD	Piattaforme supportate
FMC >= 7.6.0 e API REST	FTD hub >= 7.6.0	Tutte le piattaforme che FMC >= 7.6.0 può gestire

FMC • cdFMC >= 7.6.0 • FDM - Non supportato	• FTD raggio >= 7.3.0	
---	--	--

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center
- Software-Defined WAN (SD-WAN)

Componenti usati

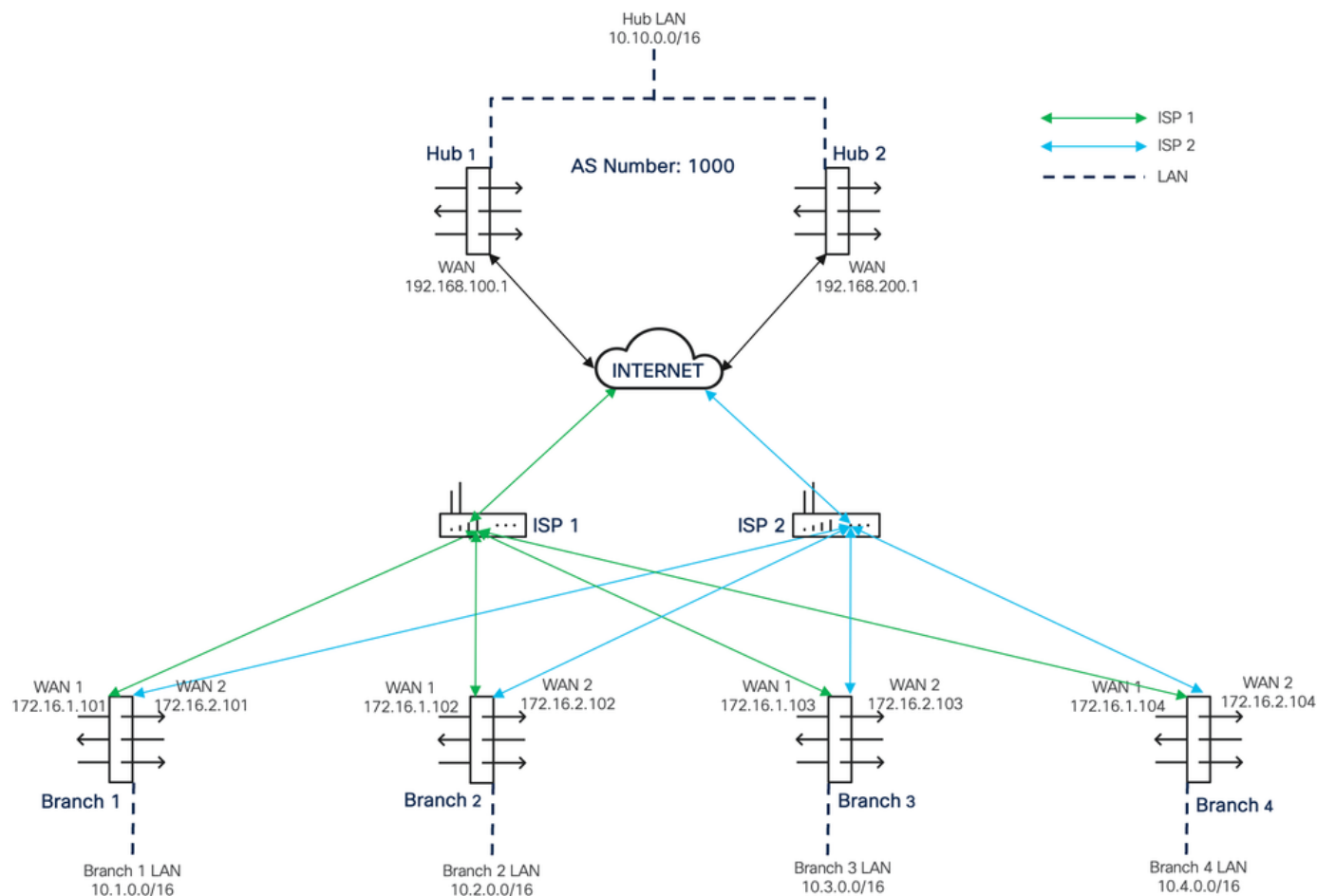
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- FTD versione 7.6.0
- FMC versione 7.6.0

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.

Configurazione

Esempio di rete



Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

Deploy admin SECURE

View By: Group

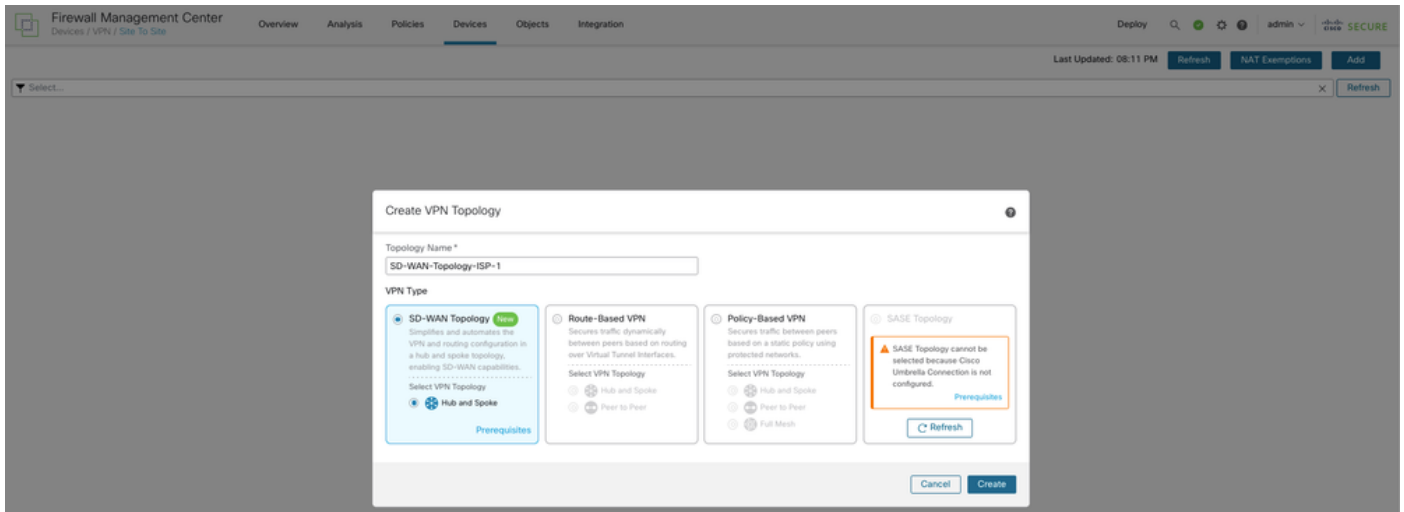
All (8)
Error (0)
Warning (0)
Offline (0)
Normal (8)
Deployment Pending (0)
Upgrade (0)
Snort 3 (8)

[Collapse All](#) [Download Device List Report](#)

☐	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
☐	▼ Branch (4)							
☐	Branch-1 Snort 3 10.10.1.206 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (5 more...)	FTD-ACP		
☐	Branch-2 Snort 3 10.10.1.207 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (5 more...)	FTD-ACP		
☐	Branch-3 Snort 3 10.10.1.208 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (5 more...)	FTD-ACP		
☐	Branch-4 Snort 3 10.10.1.209 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (5 more...)	FTD-ACP		
☐	▼ HQ (2)							
☐	Hub-1 Snort 3 10.10.1.199 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (5 more...)	FTD-ACP		
☐	Hub-2 Snort 3 10.10.1.205 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (5 more...)	FTD-ACP		

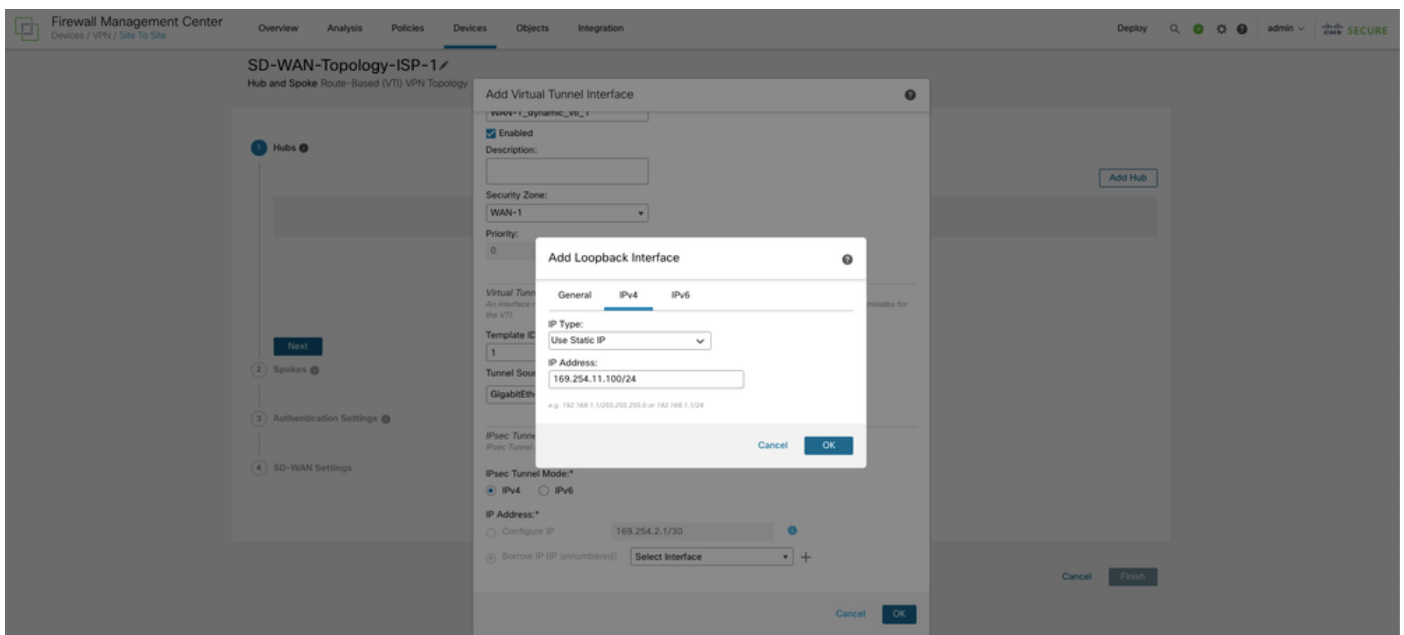
Passaggio 1. Creare una topologia SD-WAN con WAN-1 come interfaccia VPN

Selezionare Dispositivi > VPN > Sito - Sito. Selezionare Add, quindi immettere un nome appropriato nel campo Topology Name (Nome topologia) per la prima topologia con WAN-1 come interfaccia VPN. Selezionare SD-WAN Topology (Topologia SD-WAN) e selezionare Create (Crea).

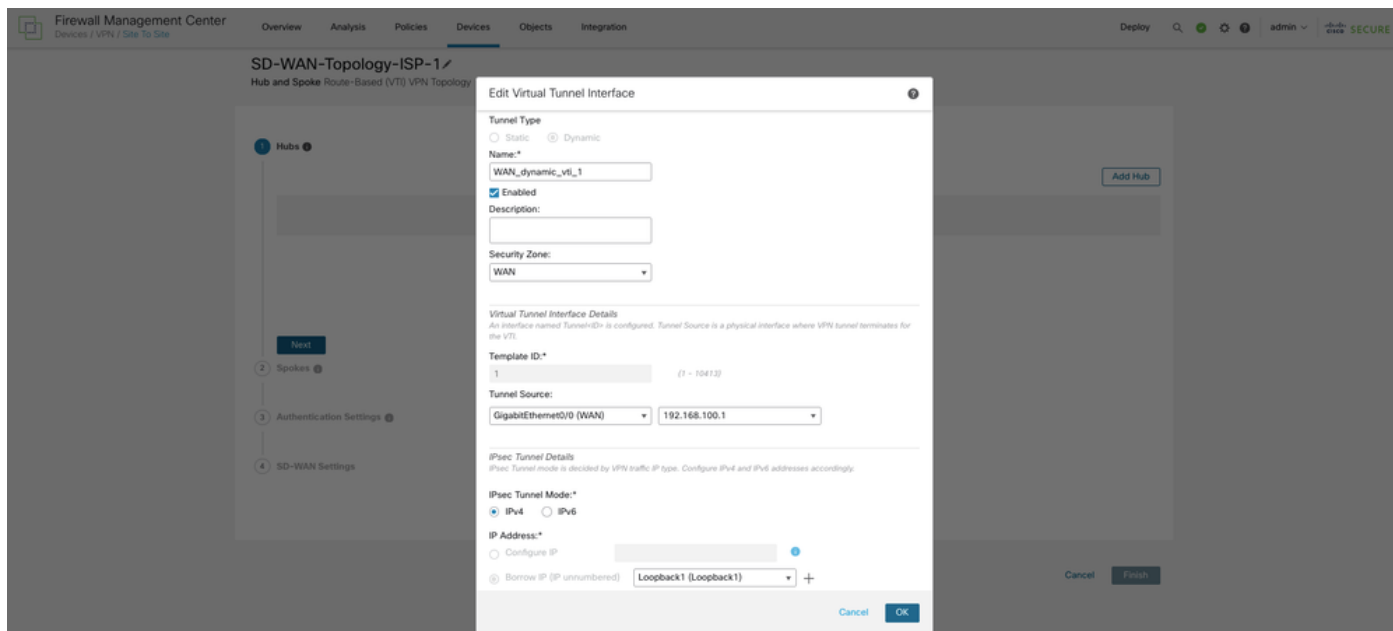


Passaggio 2. Configurare l'interfaccia DVTI (Dynamic Virtual Tunnel Interface) sull'hub primario

Selezionare Add Hub e scegliere l'hub principale dall'elenco a discesa Device (Dispositivo). Selezionare l'icona + accanto a Dynamic Virtual Tunnel Interface (DVTI). Configurare un nome, un'area di sicurezza e un ID modello e assegnare WAN-1 come interfaccia origine tunnel per DVTI.



Scegliere un'interfaccia fisica o di loopback dall'elenco a discesa Indirizzo IP prestato. Nella topologia corrente, la tecnologia DVTI eredita un indirizzo IP dell'interfaccia di loopback. Selezionare OK.



Scegliere un pool di indirizzi o selezionare l'icona + accanto a Pool di indirizzi IP tunnel spoke per creare un nuovo pool di indirizzi. Quando si aggiungono spoke, la procedura guidata genera automaticamente interfacce tunnel spoke e assegna indirizzi IP a tali interfacce spoke da questo pool di indirizzi IP.

Add IPv4 Pool



Name*

Spoke-Pool-Hub-1-ISP-1

Description

IPv4 Address Range*

169.254.11.101-169.254.11.150

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*

255.255.255.0

☐ Allow Overrides

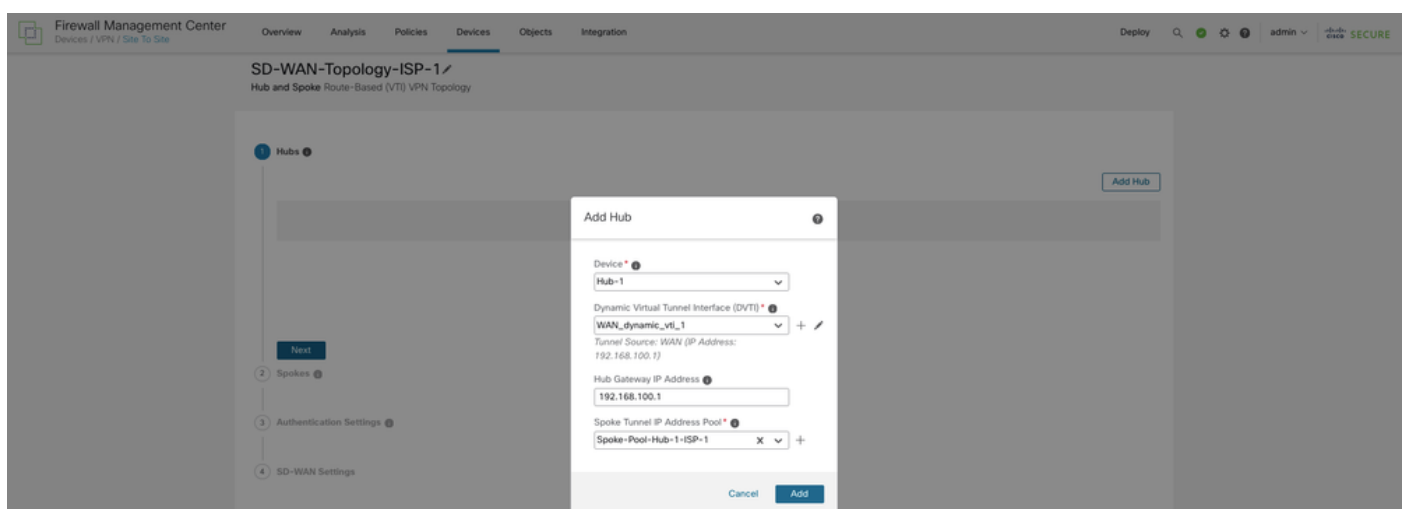


Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

Cancel

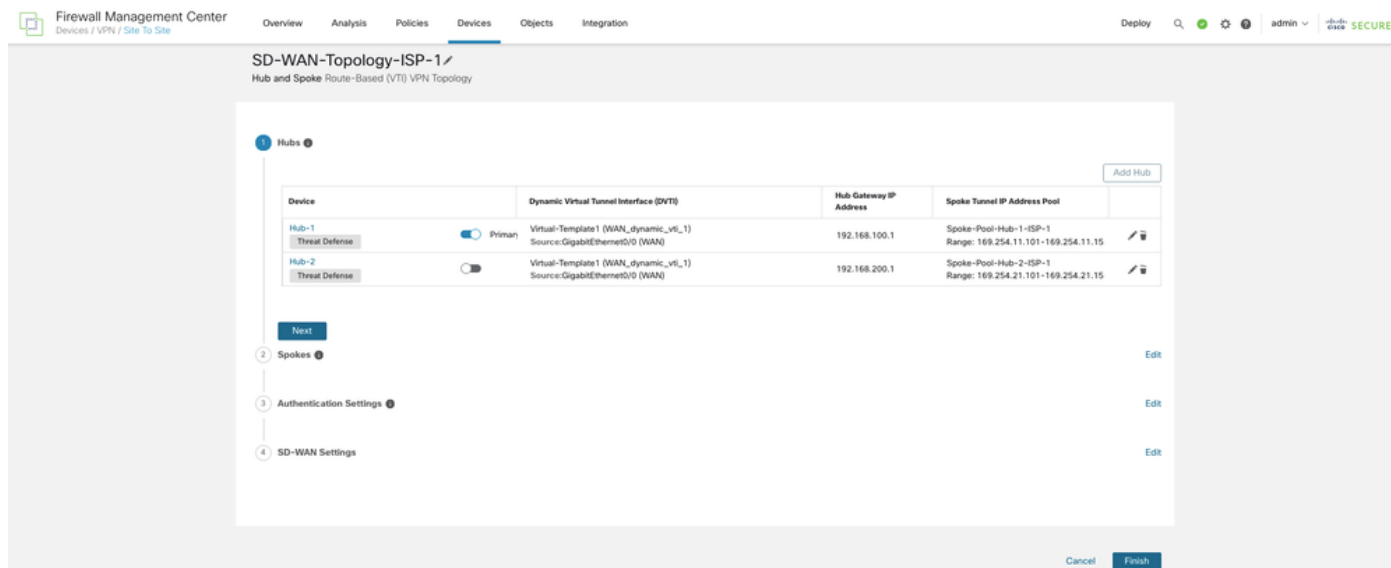
Save

Una volta completata la configurazione dell'hub primario, selezionare Aggiungi per salvare l'hub primario nella topologia.



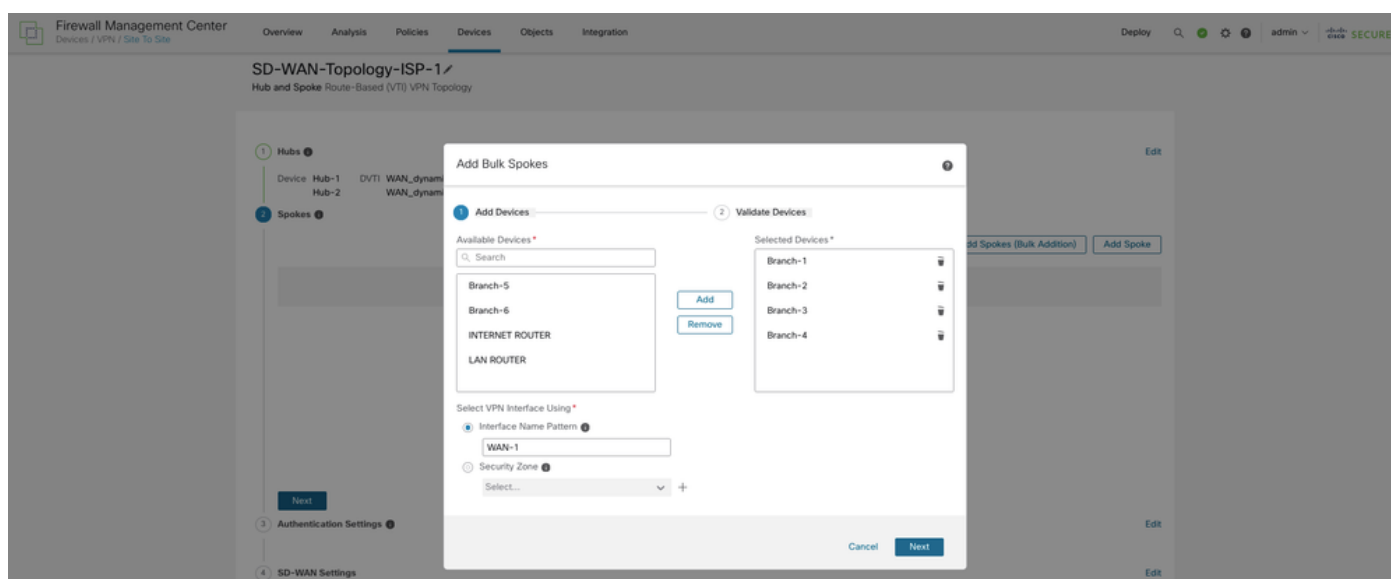
Passaggio 3. Configurare l'interfaccia DVTI (Dynamic Virtual Tunnel Interface) sull'hub secondario

Selezionare Add Hub di nuovo per configurare l'hub secondario nella topologia con WAN-1 come interfaccia VPN ripetendo i passaggi 1 e 2. Selezionare Next.

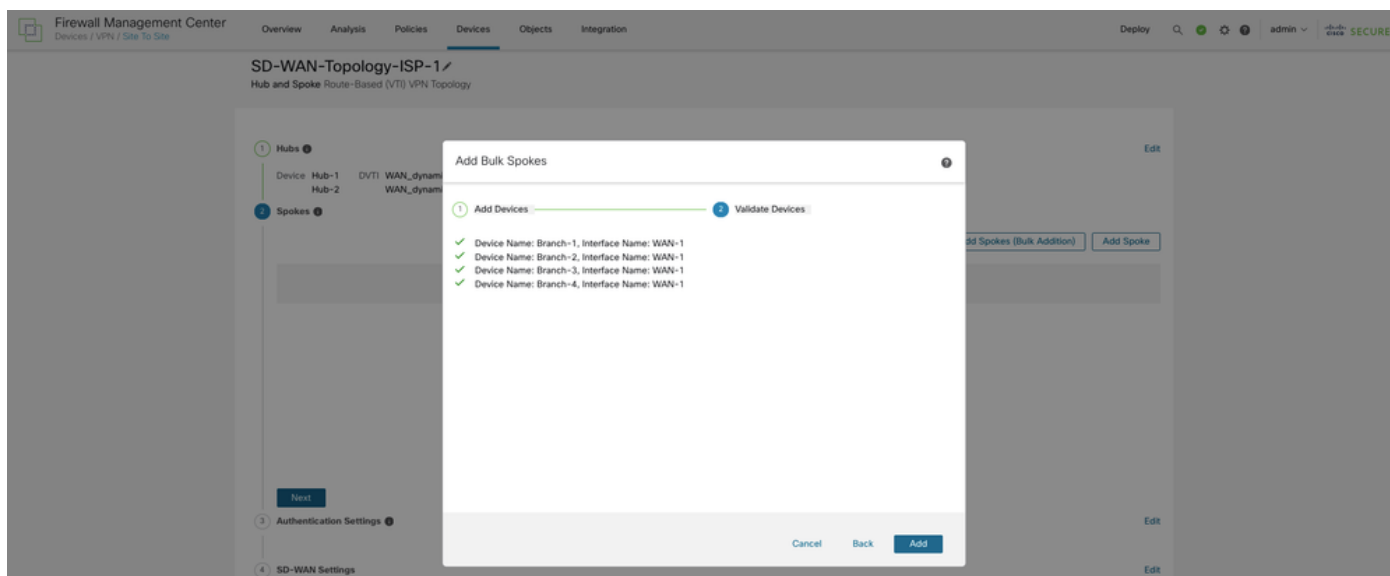


Passaggio 4. Configurazione dei raggi

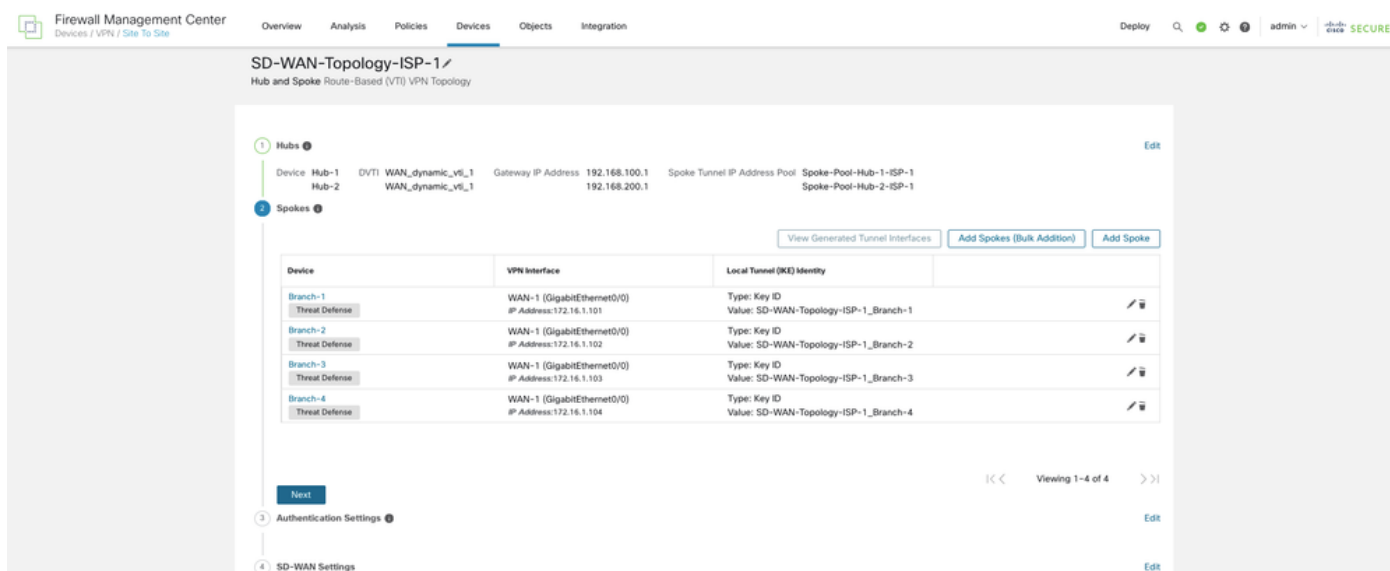
Selezionare Aggiungi spoke per aggiungere un dispositivo a spoke singolo oppure fare clic su Aggiungi spoke (aggiunta di massa) per aggiungere più spoke alla topologia. La topologia corrente utilizza quest'ultima opzione per aggiungere più FTD di diramazione alla topologia. Nella finestra di dialogo Aggiungi raggi ausiliari, selezionate gli FTD da aggiungere come raggi. Selezionare un modello di nome interfaccia comune che corrisponda al nome logico della WAN-1 su tutti i spoke o all'area di sicurezza associata alla WAN-1.



Selezionare Avanti in modo che la procedura guidata verifichi se gli spoke dispongono di interfacce con il pattern o l'area di sicurezza specificati.

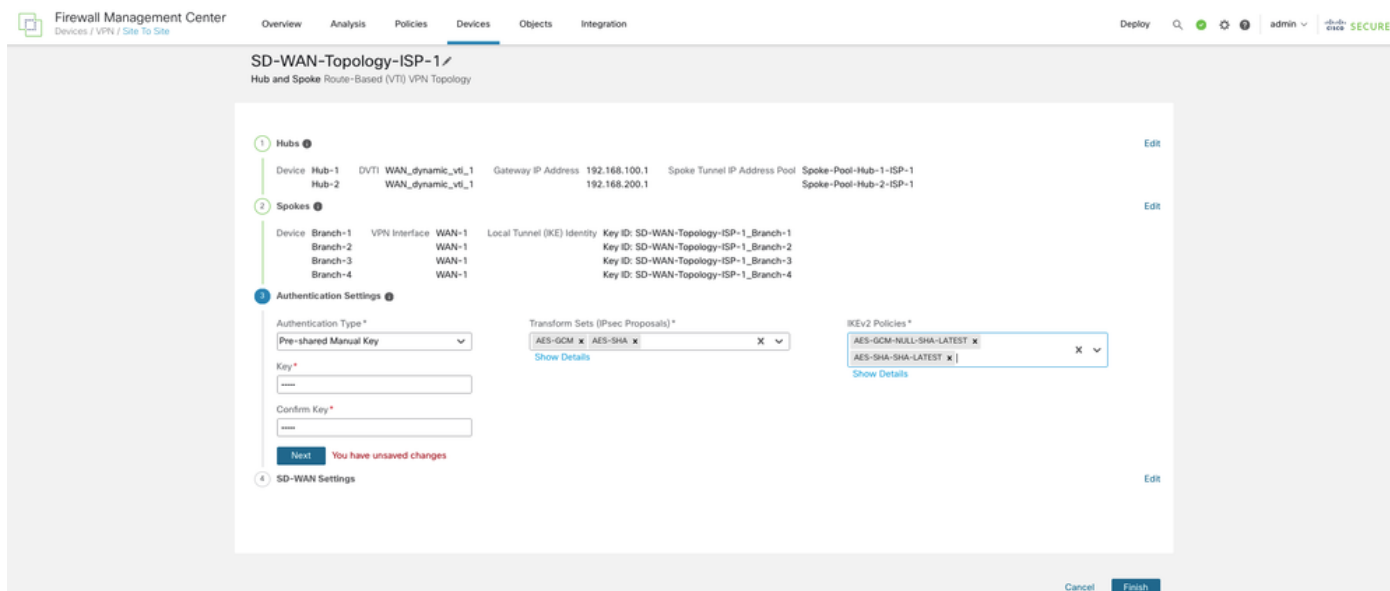


Selezionare Add (Aggiungi). La procedura guidata seleziona automaticamente il DVTI dell'hub come indirizzo IP di origine del tunnel per ogni spoke.



Passaggio 5. Configurare le impostazioni di autenticazione

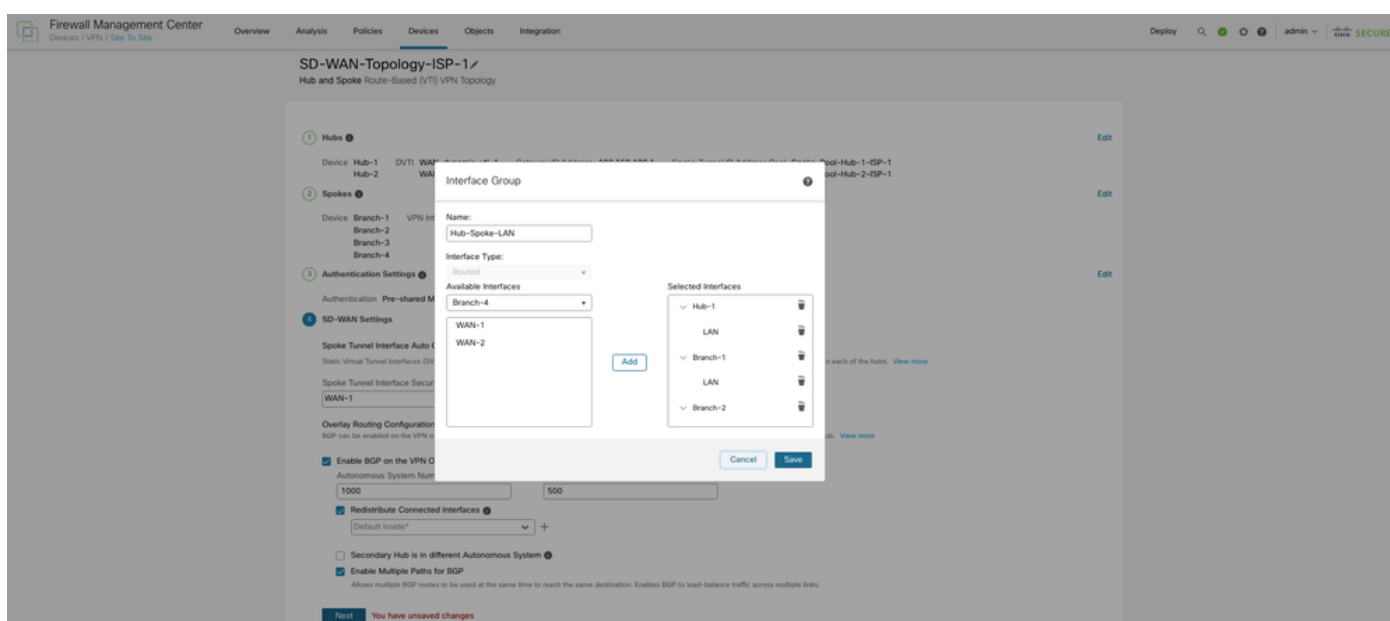
Selezionare Avanti per configurare le impostazioni di autenticazione. Per l'autenticazione dei dispositivi, è possibile selezionare una chiave precondivisa manuale, una chiave precondivisa generata automaticamente o un certificato nell'elenco a discesa Tipo di autenticazione. Selezionare uno o più algoritmi dagli elenchi a discesa Set di trasformazioni e Criteri IKEv2.



Passaggio 6. Configurare le impostazioni SD-WAN

Selezionare Next (Avanti) per configurare le impostazioni SD-WAN. Questo passaggio include la generazione automatica di interfacce tunnel spoke e la configurazione BGP della rete overlay. Dall'elenco a discesa Area di sicurezza interfaccia tunnel spoke, scegliere un'area di sicurezza o selezionare + per creare un'area di sicurezza alla quale la procedura guidata aggiunga automaticamente le SVTI (Static Virtual Tunnel Interfaces) generate automaticamente dallo spoke.

Selezionare la casella di controllo Abilita BGP sulla topologia di overlay VPN per automatizzare le configurazioni BGP tra l'interfaccia del tunnel di overlay. Nel campo Numero sistema autonomo, immettere un numero AS (Autonomous System). Selezionare la casella di controllo Ridistribuisce interfacce connesse e scegliere un gruppo di interfacce dall'elenco a discesa oppure selezionare + per creare un gruppo di interfacce con interfacce LAN connesse degli hub e degli spoke per la redistribuzione della route BGP nella topologia di overlay.



Nel campo Tag community per route locali, immettere l'attributo della community BGP per

contrassegnare le route locali connesse e ridistribuite. Questo attributo consente di applicare facilmente filtri di route. Selezionare la casella di controllo Hub secondario in sistema autonomo diverso se si dispone di un hub secondario in un SA diverso. Infine, selezionare la casella di controllo Enable Multiple Paths for BGP per abilitare BGP per il bilanciamento del carico del traffico su più collegamenti.

SD-WAN-Topology-ISP-1
Hub and Spoke Route-Based (VTI) VPN Topology

Hubs

Device	DVTI	WAN_dynamic_vti_1	Gateway IP Address	Spoke Tunnel IP Address Pool
Hub-1	WAN_dynamic_vti_1	WAN_dynamic_vti_1	192.168.100.1	Spoke-Pool-Hub-1-ISP-1
Hub-2	WAN_dynamic_vti_1	WAN_dynamic_vti_1	192.168.200.1	Spoke-Pool-Hub-2-ISP-1

Spokes

Device	VPN Interface	Local Tunnel (IKE) Identity	Key ID
Branch-1	WAN-1	WAN-1	SD-WAN-Topology-ISP-1_Branch-1
Branch-2	WAN-1	WAN-1	SD-WAN-Topology-ISP-1_Branch-2
Branch-3	WAN-1	WAN-1	SD-WAN-Topology-ISP-1_Branch-3
Branch-4	WAN-1	WAN-1	SD-WAN-Topology-ISP-1_Branch-4

Authentication Settings

Authentication: Pre-shared Manual Key

SD-WAN Settings

Spoke Tunnel Interface Auto Generation

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

Spoke Tunnel Interface Security Zone: WAN-1

Overlay Routing Configuration

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

☒ Enable BGP on the VPN Overlay Topology

Autonomous System Number: 1000

Community Tag for Local Routes: 500

☒ Redistribute Connected Interfaces

Hub-Spoke-LAN

☐ Secondary Hub is in different Autonomous System

☒ 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](#)

Fare clic su Finish (Fine) per salvare e convalidare la topologia SD-WAN.

SD-WAN-Topology-ISP-1
Hub and Spoke Route-Based (VTI) VPN Topology

Hubs

Device	DVTI	WAN_dynamic_vti_1	Gateway IP Address	Spoke Tunnel IP Address Pool
Hub-1	WAN_dynamic_vti_1	WAN_dynamic_vti_1	192.168.100.1	Spoke-Pool-Hub-1-ISP-1
Hub-2	WAN_dynamic_vti_1	WAN_dynamic_vti_1	192.168.200.1	Spoke-Pool-Hub-2-ISP-1

Spokes

Device	VPN Interface	Local Tunnel (IKE) Identity	Key ID
Branch-1	WAN-1	WAN-1	SD-WAN-Topology-ISP-1_Branch-1
Branch-2	WAN-1	WAN-1	SD-WAN-Topology-ISP-1_Branch-2
Branch-3	WAN-1	WAN-1	SD-WAN-Topology-ISP-1_Branch-3
Branch-4	WAN-1	WAN-1	SD-WAN-Topology-ISP-1_Branch-4

Authentication Settings

Authentication: Pre-shared Manual Key

SD-WAN Settings

BGP enabled: true

Autonomous System Number: 1000

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

È possibile visualizzare la topologia in Dispositivi > VPN da sito a sito. Il numero totale di tunnel nella prima topologia SD-WAN è 8.

SD-WAN-Topology-ISP-1
Route Based (VTI)

Network Topology: SD-WAN Topology

Tunnel Status Distribution: Deployment Pending

Spoke

Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-1	WAN-1 (172.16.1.101)	WAN-1_static_vti_1 (169.254.11.101)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-2	WAN-1 (172.16.1.102)	WAN-1_static_vti_1 (169.254.11.102)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-3	WAN-1 (172.16.1.103)	WAN-1_static_vti_1 (169.254.11.103)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-4	WAN-1 (172.16.1.104)	WAN-1_static_vti_1 (169.254.11.104)

Viewing 1-8 of 8

Passaggio 7. Creare una topologia SD-WAN con WAN-2 come interfaccia VPN

Ripetere i passaggi da 1 a 6 per configurare una topologia SD-WAN con WAN-2 come interfaccia VPN. Il numero totale di tunnel nella seconda topologia SD-WAN è 8. Le topologie finali devono essere simili all'immagine mostrata di seguito.

SD-WAN-Topology-ISP-1			
Hub		Spoke	
Device	VPN Interface	Device	VPN Interface
Hub-1	WAN (192.168.100.1)	Branch-1	WAN-1 (172.16.1.101)
Hub-1	WAN (192.168.100.1)	Branch-2	WAN-1 (172.16.1.102)
Hub-1	WAN (192.168.100.1)	Branch-3	WAN-1 (172.16.1.103)
Hub-1	WAN (192.168.100.1)	Branch-4	WAN-1 (172.16.1.104)

SD-WAN-Topology-ISP-2			
Hub		Spoke	
Device	VPN Interface	Device	VPN Interface
Hub-1	WAN (192.168.100.1)	Branch-1	WAN-2 (172.16.2.101)
Hub-1	WAN (192.168.100.1)	Branch-2	WAN-2 (172.16.2.102)
Hub-1	WAN (192.168.100.1)	Branch-3	WAN-2 (172.16.2.103)
Hub-1	WAN (192.168.100.1)	Branch-4	WAN-2 (172.16.2.104)

Passaggio 8. Configurazione delle zone ECMP

Su ciascuna filiale, selezionare Routing > ECMP e configurare le zone ECMP (Equal-Cost Multi-Path) per le interfacce WAN e gli SVTI che si connettono all'hub principale e a quello secondario, come mostrato di seguito. In questo modo è possibile fornire ridondanza dei collegamenti e abilitare il bilanciamento del carico del traffico VPN.

Name	Interfaces
SVTH-HUB-2-ECMP-ZONE	WAN-1_static_vti_2, WAN-2_static_vti_4
WAN-ECMP-ZONE	WAN-1, WAN-2
SVTH-HUB-1-ECMP-ZONE	WAN-1_static_vti_1, WAN-2_static_vti_3

Passaggio 9. Modificare la preferenza locale BGP sull'hub

Selezionare Routing > General Settings > BGP sull'hub secondario. Selezionare Abilita BGP, configurare il numero AS e impostare il valore della preferenza locale predefinita in Selezione del miglior percorso su un valore inferiore a quello configurato sull'hub primario. Selezionare Salva. In questo modo le route verso l'hub principale vengono preferite rispetto alle route verso l'hub secondario. Quando l'hub primario diventa inattivo, subentrano i percorsi verso l'hub secondario.

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⚙️ admin ▾ **SECURE**

Hub-2
Cisco Secure Firewall Threat Defense for VMware

Device Interfaces Inline Sets **Routing** DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP
BFD
OSPF
OSPFv3
EBGP
BGP

Policy Based Routing

BGP

IPv4
IPv6

Static Route

Multicast Routing

IGMP
PIM
Multicast Routes
Multicast Boundary Filter

General Settings

BGP

Enable BGP: ☒
AS Number*: 1000
(1-4294967295 or 1.0-45535.65535)
☐ Override BGP general settings router-id address:
Router Id: Automatic
IP Address*:
General
Scanning Interval: 60
Number of AS numbers in AS_PATH attribute of received routes: None
Log Neighbor Changes: Yes
Use TCP path MTU discovery: Yes
Reset session upon fallover: Yes
Enforce the first AS is peer's AS for EBGP routes: Yes
Use dot notation for AS number: No
Aggregate Timer: 30
Neighbor Timers
Keepalive Interval: 60
Hold time: 180
Min hold time: 0
Next Hop
Address tracking: Yes
Delay interval: 5
Graceful Restart (use in fallover or spinned cluster mode)
Graceful Restart: No
Restart time: 120
Stalepath time: 360
Best Path Selection
Default local preference: 90
Allow comparing MED from different neighbors: No
Compare Router ID for identical EBGP paths: No
Pick the best-MED path among paths advertised by neighbor AS: No
Treat missing MED as the best preferred path: No

Distribuire le configurazioni su tutti i dispositivi.

Verifica

Verifica degli stati del tunnel

Per verificare se i tunnel VPN delle topologie SD-WAN sono attivi, selezionare Dispositivo > VPN > Da sito a sito.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⚙️ admin ▾ **SECURE**

Last Updated: 09:21 PM Refresh NAT Exemptions Add

Select...

Topology Name VPN Type Network Topology Tunnel Status Distribution IKEv1 IKEv2

SD-WAN-Topology-ISP-1 Route Based (VTI) SD-WAN Topology 0 Tunnels

Hub Spoke

Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-1	WAN-1 (172.16.1.101)	WAN-1_static_vti_1 (169.254.11.101)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-2	WAN-1 (172.16.1.102)	WAN-1_static_vti_1 (169.254.11.102)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-3	WAN-1 (172.16.1.103)	WAN-1_static_vti_1 (169.254.11.103)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	Branch-4	WAN-1 (172.16.1.104)	WAN-1_static_vti_1 (169.254.11.104)

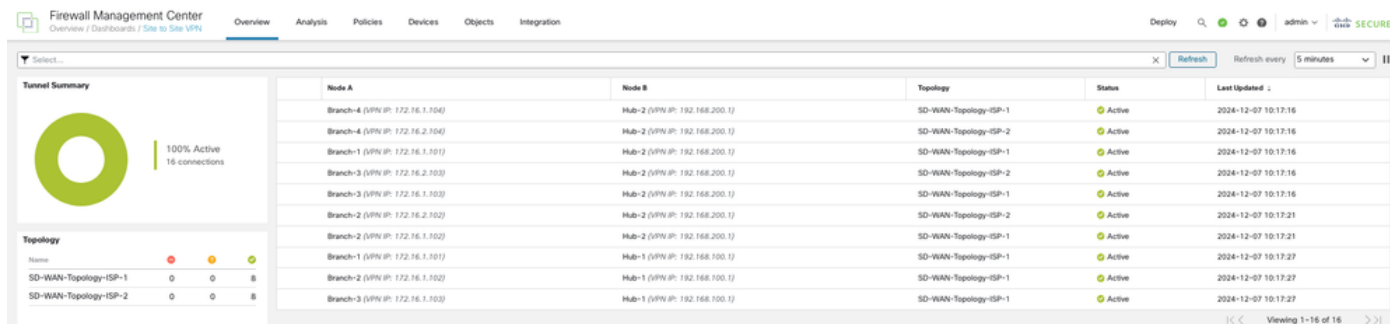
SD-WAN-Topology-ISP-2 Route Based (VTI) SD-WAN Topology 0 Tunnels

Hub Spoke

Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	Branch-1	WAN-2 (172.16.2.101)	WAN-2_static_vti_3 (169.254.12.101)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	Branch-2	WAN-2 (172.16.2.102)	WAN-2_static_vti_3 (169.254.12.102)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	Branch-3	WAN-2 (172.16.2.103)	WAN-2_static_vti_3 (169.254.12.103)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	Branch-4	WAN-2 (172.16.2.104)	WAN-2_static_vti_3 (169.254.12.104)

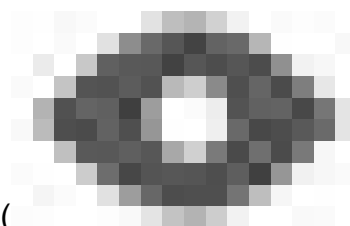
Viewing 1-8 of 8

Per visualizzare i dettagli dei tunnel VPN da sito a sito, scegliere Panoramica > Dashboard > VPN da sito a sito.



Per visualizzare ulteriori dettagli su ciascun tunnel VPN:

1. Passare il mouse su un tunnel.



2. Selezionare il pulsante di opzione Visualizza informazioni complete (). Verrà visualizzato un riquadro con i dettagli del tunnel e altre azioni.

3. Selezionare la scheda Dettagli CLI nel riquadro laterale per visualizzare i comandi show e i dettagli delle associazioni di sicurezza IPsec.

A: Branch-1 ↔ B: Hub-1



Topology: SD-WAN-Topology-ISP-2 | Status: Active

General CLI Details Packet Tracer

Refresh Maximize view

Summary

Node A (172.16.2.101/500) ⓘ Node B (192.168.100.1/500) ⓘ

Transmitted: 8.46 KB (8664 B) Transmitted: 5.98 KB (6123 B)

Received: 27.73 KB (28400 B) Received: 7.68 KB (7868 B)

IPsec Security Associations (2)

0.0.0.0/0.0.0.0/0/0		0.0.0.0/0.0.0.0/0/0	
Settings:	L2L,Tunnel,IKEv2,...	Settings:	L2L,Tunnel,IKEv2,VTI
Encaps/Encrypt:	140 / 140 pkts	Encaps/Encrypt:	92 / 92 pkts
Dcaps/Decrypt:	232 / 232 pkts	Dcaps/Decrypt:	96 / 96 pkts
Remaining Lifetime for SPI ID: 0x5B2983A9			
Outbound:	3.69 GB (3962871000 B) 12:47:26 (26246 sec)	Inbound:	3.65 GB (3916794000 B) 12:50:26 (26426 sec)
Remaining Lifetime for SPI ID: 0x0F4EA9C0			
Inbound:	3.99 GB (4285416000 B) 12:47:26 (26246 sec)	Outbound:	3.69 GB (3962874000 B) 12:50:26 (26426 sec)
0.0.0.0/0.0.0.0/0/0			
Settings:	L2L,Tunnel,IKEv2,...	Info is not available for Extranet device	
Encaps/Encrypt:	96 / 96 pkts		
Dcaps/Decrypt:	92 / 92 pkts		
Remaining Lifetime for SPI ID: 0x1DEFCEB21			
Outbound:	4.03 GB (4331514000 B) 12:50:25 (26425 sec)	Inbound:	No data
Remaining Lifetime for SPI ID: 0x53B1AE47			
Inbound:	3.65 GB (3916794000 B) 12:50:25 (26425 sec)	Outbound:	No data

Branch-1 (VPN Interface IP: 172.16.2.101)

show crypto ipsec sa peer 192.168.100.1 ⓘ

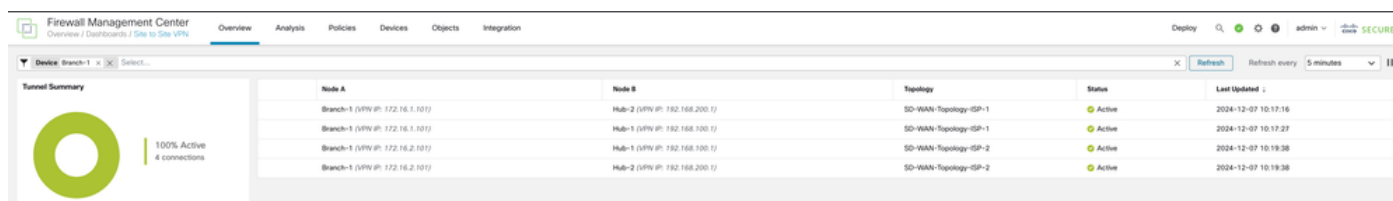
WAN-2_static_vti_3 - Da SVTI a Hub 1 tramite ISP 2

WAN-1_static_vti_2 - Da SVTI a Hub 2 tramite ISP 1

WAN-2_static_vti_4 - Da SVTI a Hub 2 tramite ISP 2

Verifica del bilanciamento del carico del traffico VPN

Lo stato del tunnel può essere visualizzato nel dashboard della VPN da sito a sito. Idealmente, tutti i tunnel devono essere attivi:



Le route all'hub principale sono preferibili. Il comando show route sulla filiale 1 indica che il traffico VPN è con carico bilanciato tra i due SVTI sull'ISP 1 e sull'ISP 2 e diretti all'hub principale:

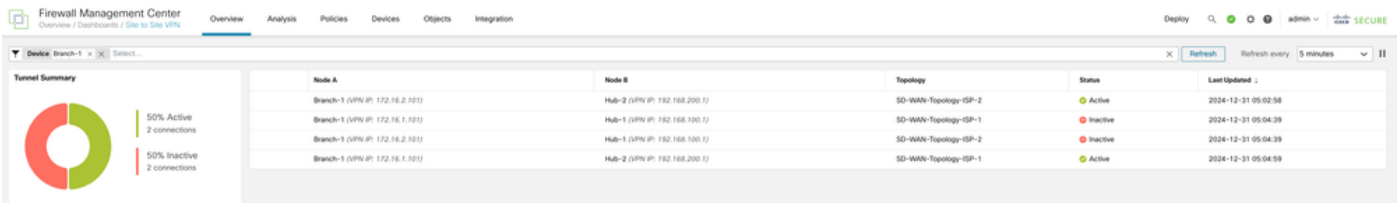
```
CLI Troubleshoot
> Command: show route
Execute Refresh Copy
Device: Branch-1

> show route
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

C    10.1.0.0 255.255.0.0 is directly connected, LAN
L    10.1.0.1 255.255.255.255 is directly connected, LAN
B    10.10.0.0 255.255.0.0 [200/1] via 169.254.12.100, 01:41:02
    [200/1] via 169.254.11.100, 01:41:02
C    169.254.11.0 255.255.255.0 is directly connected, WAN-1_static_vti_1
V    169.254.11.100 255.255.255.255
    connected by VPN (advertised), WAN-1_static_vti_1
L    169.254.11.101 255.255.255.255
    is directly connected, WAN-1_static_vti_1
C    169.254.12.0 255.255.255.0 is directly connected, WAN-2_static_vti_3
V    169.254.12.100 255.255.255.255
    connected by VPN (advertised), WAN-2_static_vti_3
L    169.254.12.101 255.255.255.255
    is directly connected, WAN-2_static_vti_3
C    169.254.21.0 255.255.255.0 is directly connected, WAN-1_static_vti_2
V    169.254.21.100 255.255.255.255
    connected by VPN (advertised), WAN-1_static_vti_2
L    169.254.21.101 255.255.255.255
    is directly connected, WAN-1_static_vti_2
C    169.254.22.0 255.255.255.0 is directly connected, WAN-2_static_vti_4
V    169.254.22.100 255.255.255.255
    connected by VPN (advertised), WAN-2_static_vti_4
L    169.254.22.101 255.255.255.255
    is directly connected, WAN-2_static_vti_4
C    172.16.1.0 255.255.255.0 is directly connected, WAN-1
L    172.16.1.101 255.255.255.255 is directly connected, WAN-1
C    172.16.2.0 255.255.255.0 is directly connected, WAN-2
L    172.16.2.101 255.255.255.255 is directly connected, WAN-2
D    192.168.1.0 255.255.255.0 [90/768] via 172.16.1.1, 02:03:26, WAN-1
D    192.168.2.0 255.255.255.0 [90/768] via 172.16.2.1, 02:03:26, WAN-2
D    192.168.100.0 255.255.255.0 [90/1024] via 172.16.2.1, 02:03:26, WAN-2
    [90/1024] via 172.16.1.1, 02:03:26, WAN-1
D    192.168.200.0 255.255.255.0 [90/1024] via 172.16.2.1, 02:03:26, WAN-2
    [90/1024] via 172.16.1.1, 02:03:26, WAN-1
```

L'interfaccia in uscita utilizzata per il traffico VPN effettivo può essere rilevata in Eventi unificati:

Quando l'hub primario è inattivo, lo stato del tunnel indica che i tunnel verso l'hub secondario sono attivi:



Poiché l'hub primario non è attivo, vengono preferiti i percorsi all'hub secondario. Il comando show route sulla filiale 1 indica che il traffico VPN è con carico bilanciato tra i due SVTI sull'ISP 1 e sull'ISP 2 e diretti all'hub secondario:

```
CLI Troubleshoot

>_ Command: show route [Execute] [Refresh] [Copy] Device: Branch-1

> show route

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

C 10.1.0.0 255.255.0.0 is directly connected, LAN
L 10.1.0.1 255.255.255.255 is directly connected, LAN
B 10.10.0.0 255.255.0.0 [200/1] via 169.254.22.100, 00:09:02
[200/1] via 169.254.21.100, 00:09:02
C 169.254.21.0 255.255.255.0 is directly connected, WAN-1 static vti 2
V 169.254.21.100 255.255.255.255
connected by VPN (advertised), WAN-1 static vti 2
L 169.254.21.101 255.255.255.255
is directly connected, WAN-1 static vti 2
C 169.254.22.0 255.255.255.0 is directly connected, WAN-2 static vti 4
V 169.254.22.100 255.255.255.255
connected by VPN (advertised), WAN-2 static vti 4
L 169.254.22.101 255.255.255.255
is directly connected, WAN-2 static vti 4
C 172.16.1.0 255.255.255.0 is directly connected, WAN-1
L 172.16.1.101 255.255.255.255 is directly connected, WAN-1
C 172.16.2.0 255.255.255.0 is directly connected, WAN-2
L 172.16.2.101 255.255.255.255 is directly connected, WAN-2
D 192.168.1.0 255.255.255.0 [90/768] via 172.16.1.1, 00:11:13, WAN-1
D 192.168.2.0 255.255.255.0 [90/768] via 172.16.2.1, 00:11:13, WAN-2
D 192.168.100.0 255.255.255.0 [90/1024] via 172.16.2.1, 00:11:13, WAN-2
[90/1024] via 172.16.1.1, 00:11:13, WAN-1
D 192.168.200.0 255.255.255.0 [90/1024] via 172.16.2.1, 00:11:13, WAN-2
[90/1024] via 172.16.1.1, 00:11:13, WAN-1
```

L'interfaccia in uscita utilizzata per il traffico VPN effettivo può essere rilevata in Eventi unificati:

The screenshot shows the 'Unified Events' section of the Firewall Management Center. It displays a table of events with columns for Time, Event Type, Source IP, Destination IP, Source Port / ICMP Type, Destination Port / ICMP Code, Web Application, Access Control Rule, Access Control Policy, Device, Decrypt Peer, Egress Interface, Encrypt Peer, and VPN Action. The 'Egress Interface' column shows 'WAN-1_static_vti_2' and 'WAN-2_static_vti_4' for the respective devices.

Time	Event Type	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule	Access Control Policy	Device	Decrypt Peer	Egress Interface	Encrypt Peer	VPN Action
2024-12-31 05:27:10	% Connection	10.1.0.100	10.10.0.100	37096 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Branch-1		WAN-1_static_vti_2	192.168.200.1	Encrypt
2024-12-31 05:27:10	% Connection	10.1.0.100	10.10.0.100	37096 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Hub-2	172.16.1.101	LAN		Decrypt
2024-12-31 05:27:07	% Connection	10.1.0.100	10.10.0.100	53570 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Branch-1		WAN-2_static_vti_4	192.168.200.1	Encrypt
2024-12-31 05:27:07	% Connection	10.1.0.100	10.10.0.100	53570 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Hub-2	172.16.2.101	LAN		Decrypt

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).