

Configuration de la topologie à deux FAI avec deux concentrateurs et quatre rayons dans la même région

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Plates-formes logicielles et matérielles prises en charge](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Étape 1 : création d'une topologie SD-WAN avec WAN-1 comme interface VPN](#)

[Étape 2 : configuration de l'interface DVTI \(Dynamic Virtual Tunnel Interface\) sur le concentrateur principal](#)

[Étape 3 : configuration de l'interface DVTI \(Dynamic Virtual Tunnel Interface\) sur le concentrateur secondaire](#)

[Étape 4. Configuration des rayons](#)

[Étape 5. Configuration des paramètres d'authentification](#)

[Étape 6. Configuration des paramètres SD-WAN](#)

[Étape 7. Création d'une topologie SD-WAN avec WAN-2 comme interface VPN](#)

[Étape 8 : configuration des zones ECMP](#)

[Étape 9. Modification de la préférence locale BGP sur le concentrateur](#)

[Vérifier](#)

[Vérification des états du tunnel](#)

[Vérification des interfaces de tunnel virtuel](#)

[Vérification de l'équilibrage de charge du trafic VPN](#)

[Vérification de la redondance ISP double](#)

[Vérification de la redondance au niveau du concentrateur](#)

Introduction

Ce document décrit comment configurer une topologie à deux FAI avec deux concentrateurs et quatre rayons dans la même région à l'aide de l'assistant SD-WAN.

Conditions préalables

Plates-formes logicielles et matérielles prises en charge

Responsable	FTD	Plates-formes prises en charge
-------------	-----	--------------------------------

• FMC >= 7.6.0 et API REST FMC • cdFMC >= 7.6.0 • FDM - Non pris en charge	• FTD du concentrateur >= 7.6.0 • DTC satellite >= 7,3,0	Toutes les plates-formes que FMC >= 7.6.0 peut gérer
--	---	--

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center
- WAN défini par logiciel (SD-WAN)

Composants utilisés

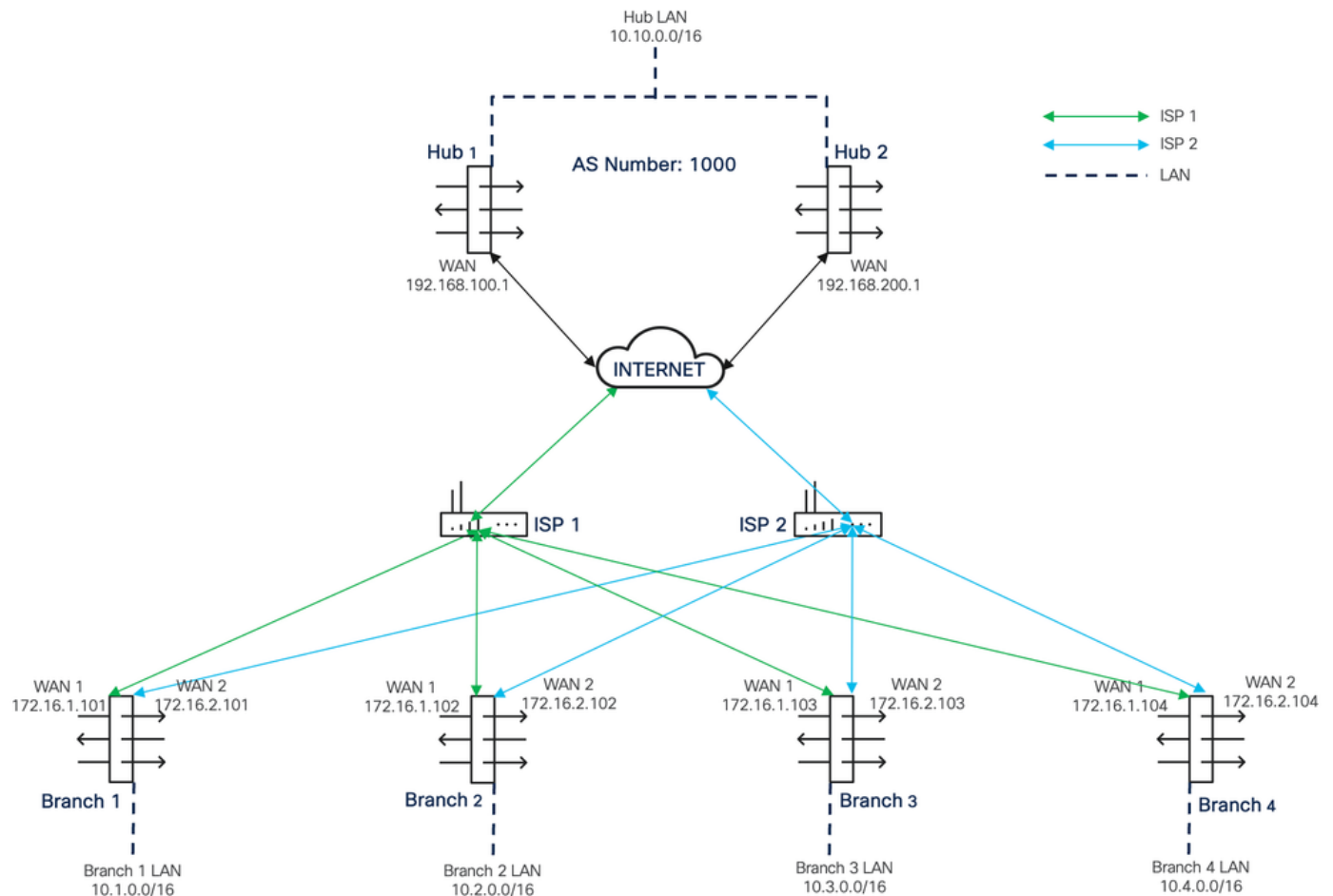
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- FTD version 7.6.0
- FMC version 7.6.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Diagramme du réseau



Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

Deploy admin SECURE

View By: Group

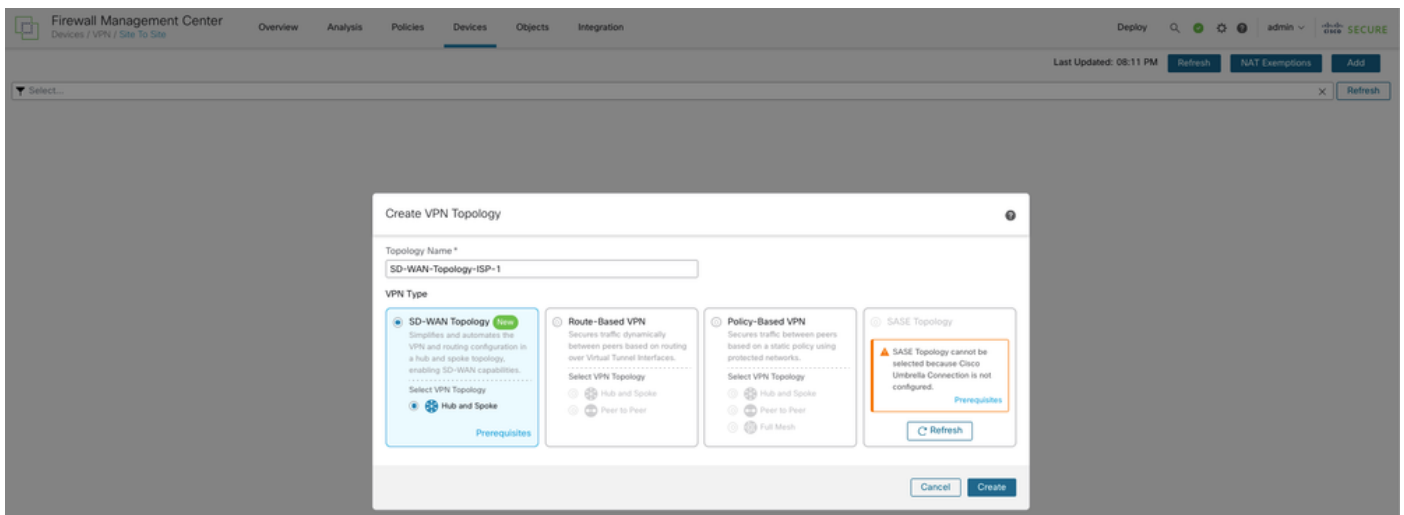
All (8)
Error (0)
Warning (0)
Offline (0)
Normal (8)
Deployment Pending (0)
Upgrade (0)
Snort 3 (8)

[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		

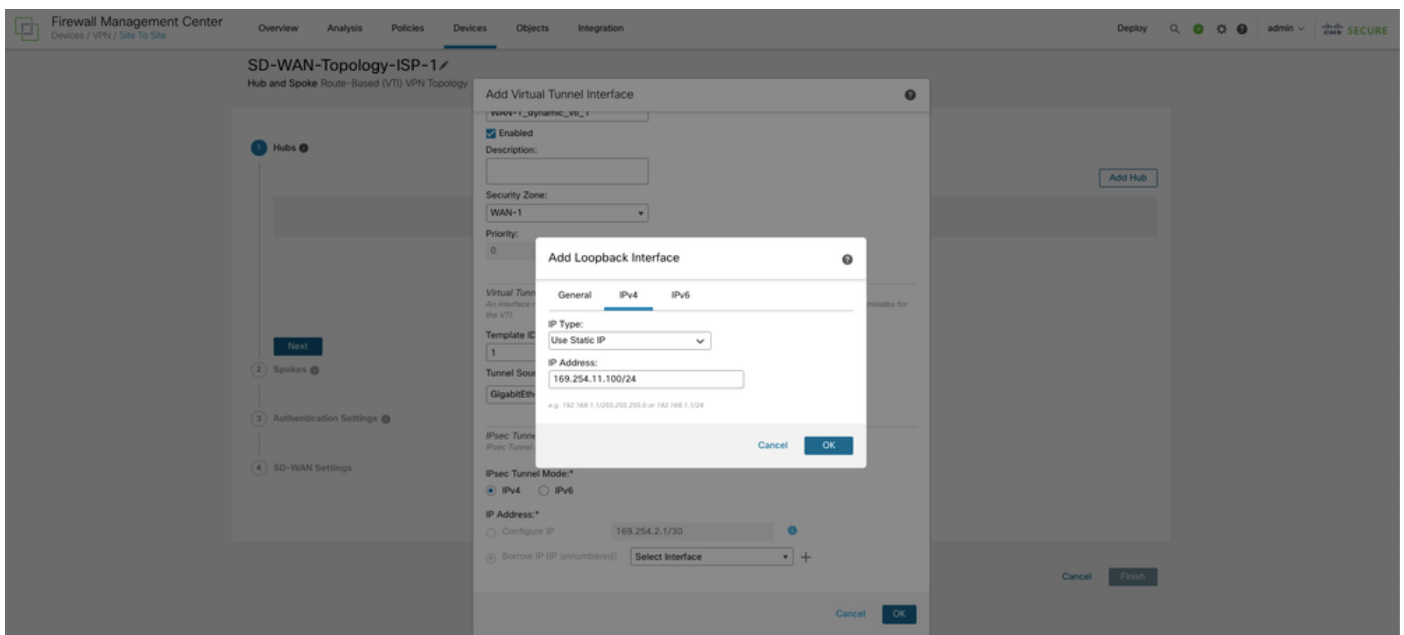
Étape 1 : création d'une topologie SD-WAN avec WAN-1 comme interface VPN

Accédez à Devices > VPN > Site To Site. Sélectionnez Add, et entrez un nom approprié dans le champ Topology Name pour la première topologie avec WAN-1 comme interface VPN. Choisissez SD-WAN Topology et sélectionnez Create.

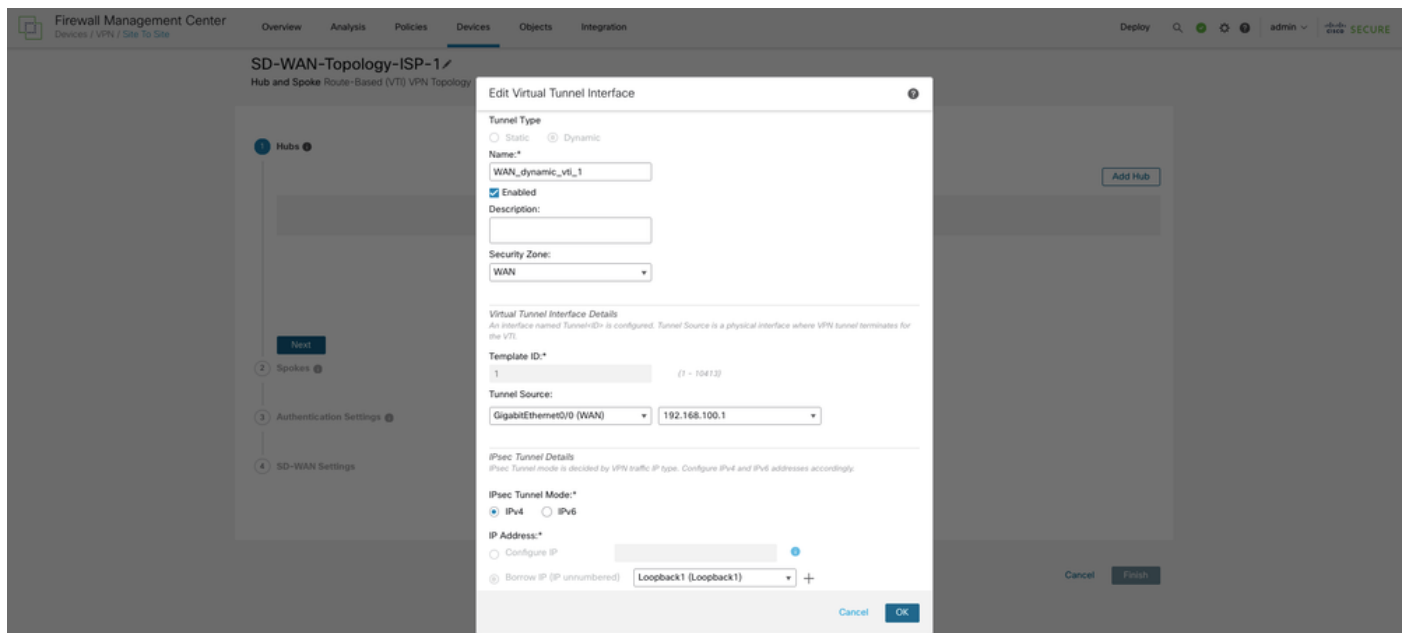


Étape 2 : configuration de l'interface DVTI (Dynamic Virtual Tunnel Interface) sur le concentrateur principal

Sélectionnez Add Hub et choisissez le concentrateur principal dans la liste déroulante Device. Sélectionnez l'icône + en regard de Dynamic Virtual Tunnel Interface (DVTI). Configurez un nom, une zone de sécurité et un ID de modèle et attribuez WAN-1 comme interface source de tunnel pour le DVTI.



Choisissez une interface physique ou de bouclage dans la liste déroulante Emprunter IP. Dans la topologie actuelle, le DVTI hérite d'une adresse IP d'interface de bouclage. Sélectionnez OK.



Choisissez un pool d'adresses ou cliquez sur l'icône + en regard de Spoke Tunnel IP Address Pool pour créer un nouveau pool d'adresses. Lorsque vous ajoutez des rayons, l'Assistant génère automatiquement des interfaces de tunnel en rayon et attribue des adresses IP à ces interfaces en rayon à partir de ce pool d'adresses 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

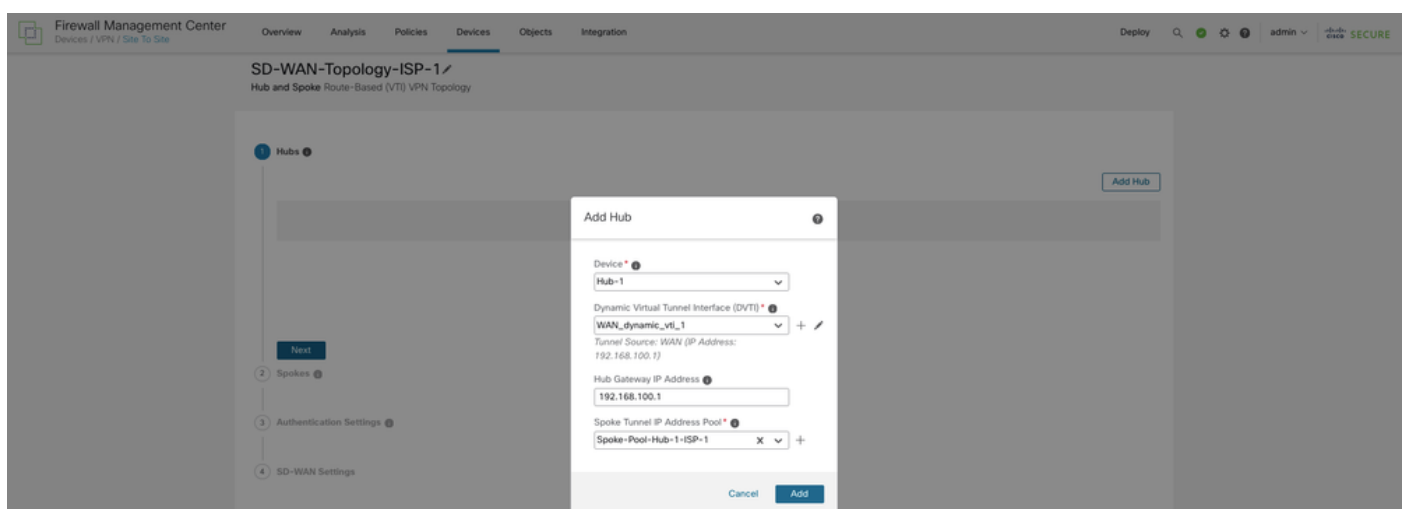


Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

Cancel

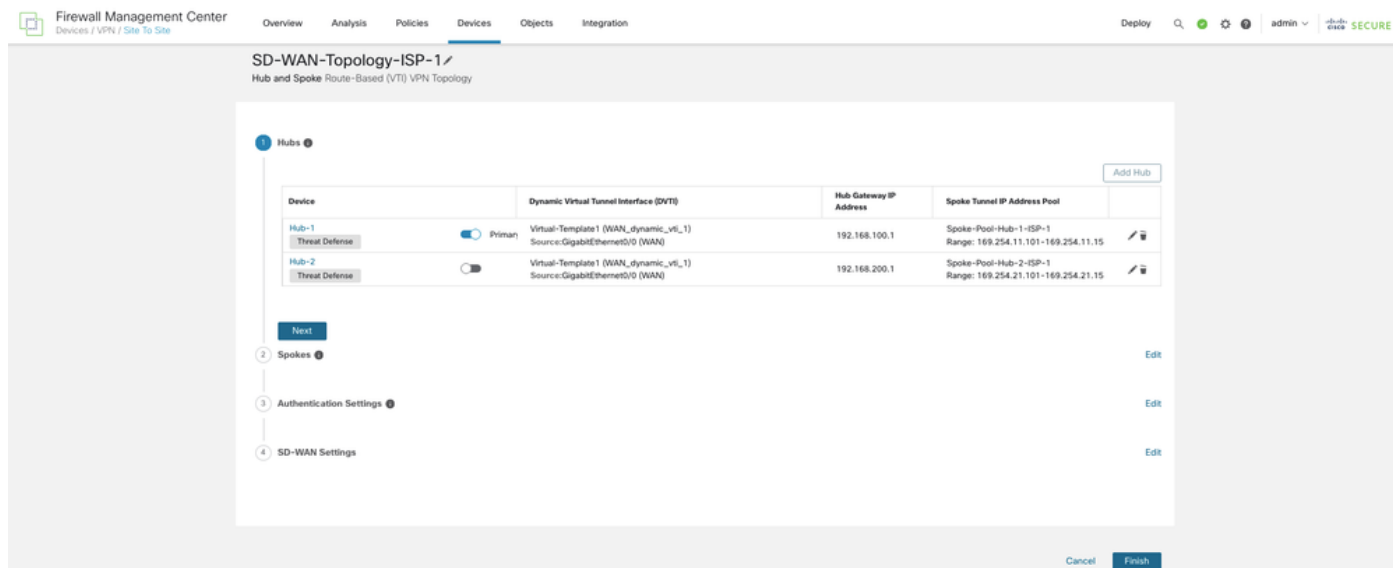
Save

Une fois la configuration du concentrateur principal terminée, sélectionnez Add pour enregistrer le concentrateur principal dans la topologie.



Étape 3 : configuration de l'interface DVTI (Dynamic Virtual Tunnel Interface) sur le concentrateur secondaire

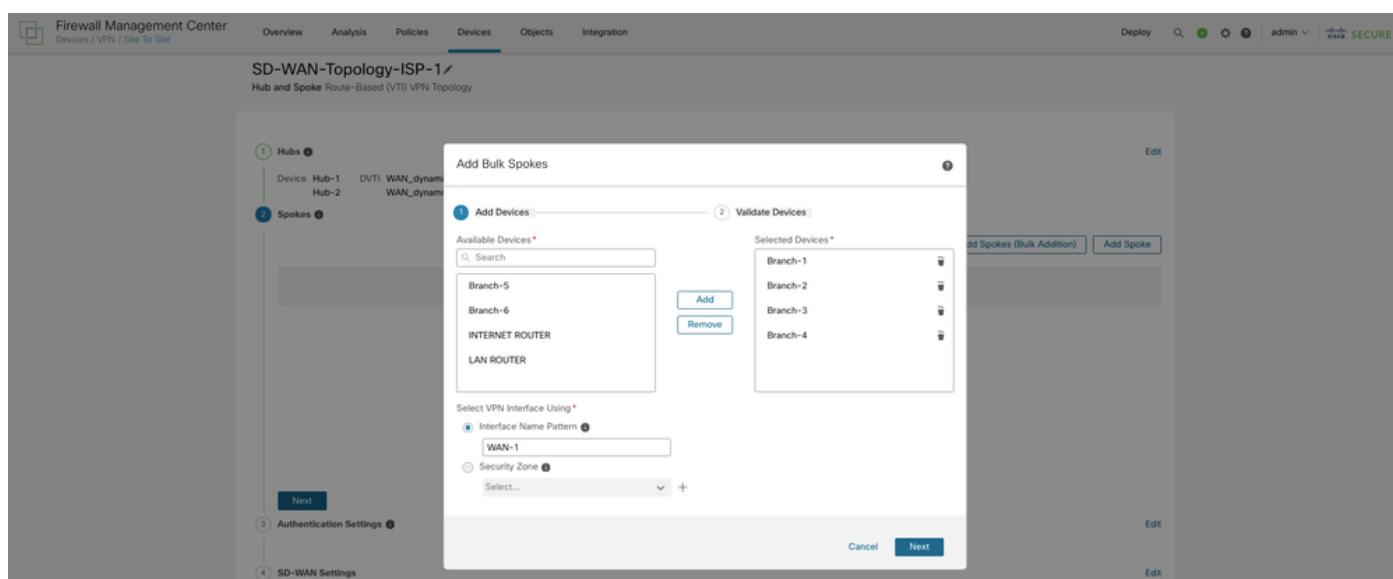
Sélectionnez à nouveau Add Hub pour configurer le concentrateur secondaire dans la topologie avec WAN-1 comme interface VPN en répétant les étapes 1 et 2. Sélectionnez Next.



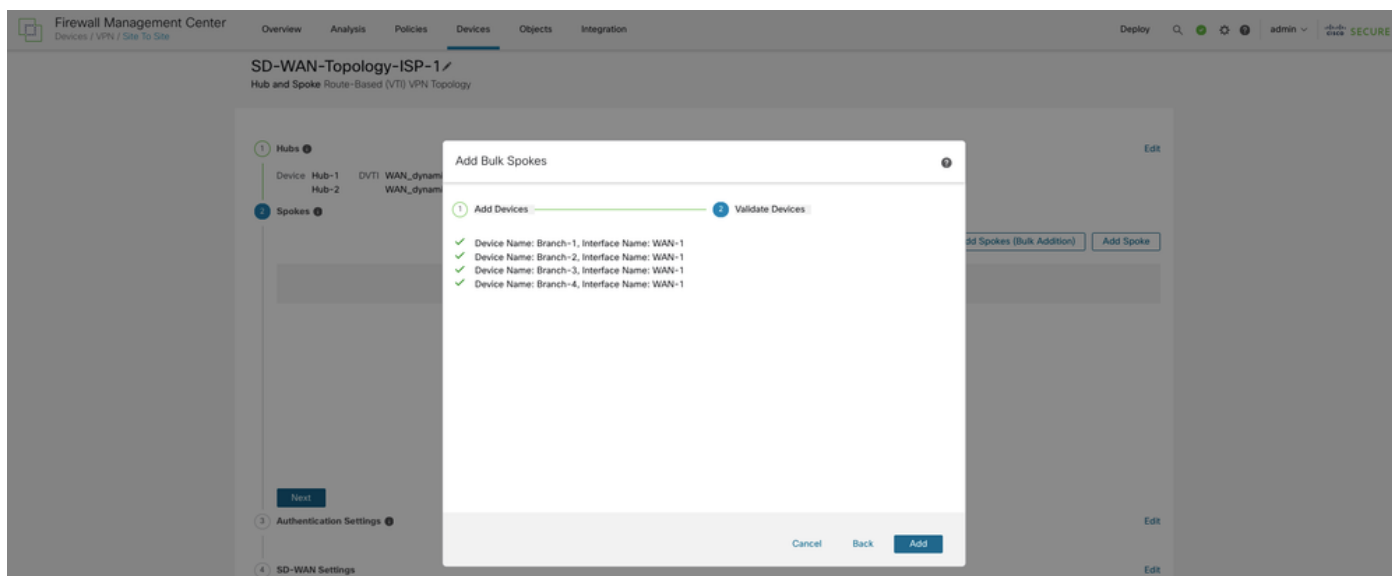
Étape 4. Configuration des rayons

Sélectionnez Add Spoke pour ajouter un périphérique à rayon unique ou cliquez sur Add Spokes (Bulk Addition) pour ajouter plusieurs rayons à votre topologie. La topologie actuelle utilise cette dernière option pour ajouter plusieurs FTD de branche à la topologie. Dans la boîte de dialogue Ajouter des rayons en masse, sélectionnez les FTD requis à ajouter en tant que rayons.

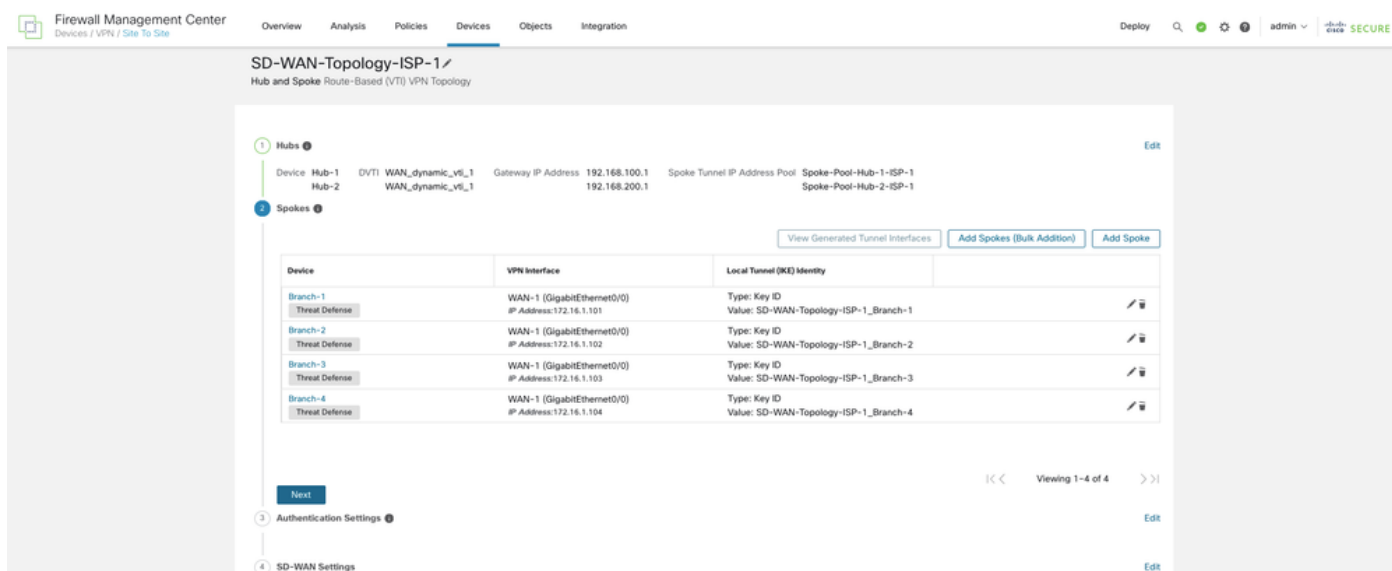
Sélectionnez un modèle de nom d'interface commun qui correspond au nom logique de WAN-1 sur tous les rayons ou la zone de sécurité qui est associée à WAN-1.



Sélectionnez Next afin que l'assistant vérifie si les rayons ont des interfaces avec le modèle ou la zone de sécurité spécifié.

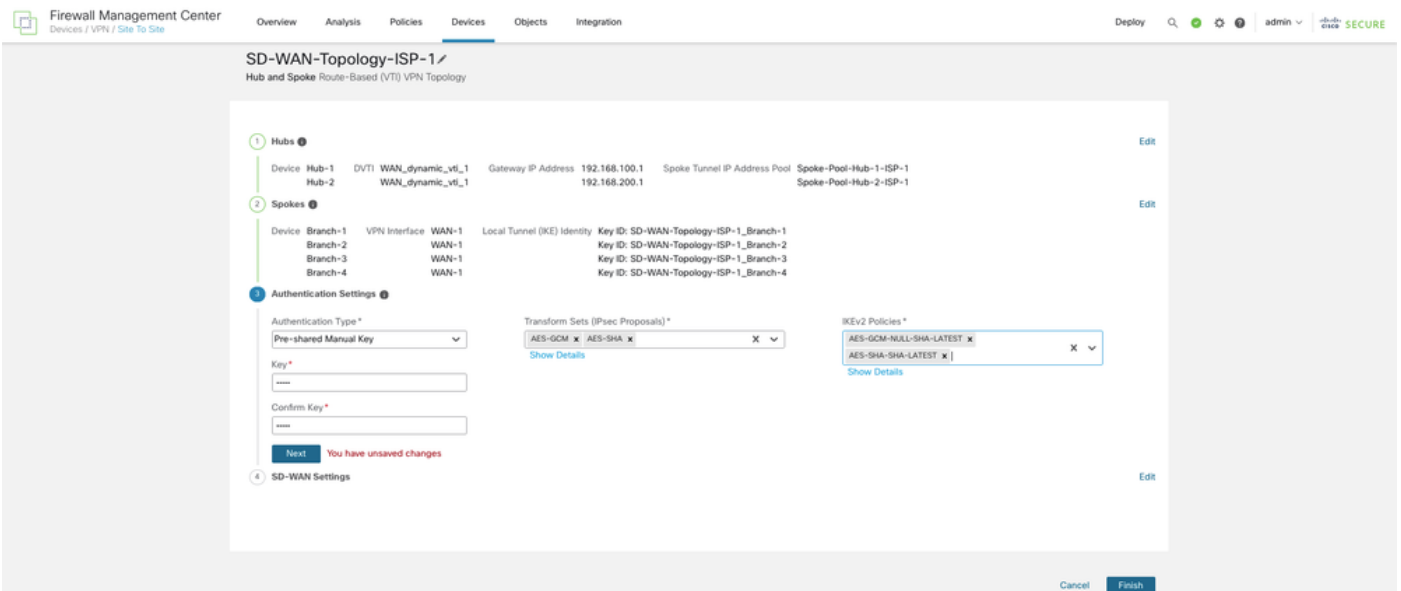


Sélectionnez Add et l'assistant sélectionne automatiquement le concentrateur DVTI comme adresse IP source du tunnel pour chaque rayon.



Étape 5. Configuration des paramètres d'authentification

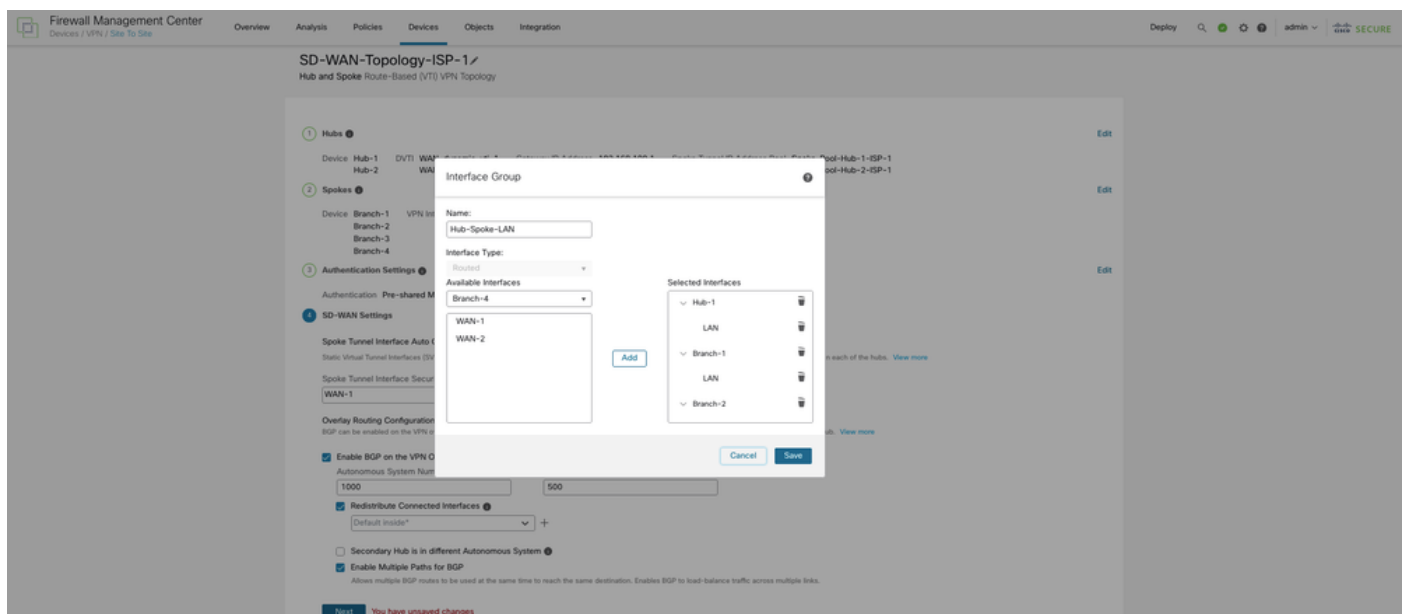
Sélectionnez Next pour configurer les paramètres d'authentification. Pour l'authentification de périphérique, vous pouvez sélectionner une clé pré-partagée manuelle, une clé pré-partagée générée automatiquement ou un certificat dans la liste déroulante Authentication Type. Choisissez un ou plusieurs algorithmes dans les listes déroulantes Transform Sets et IKEv2 Policies.



Étape 6. Configuration des paramètres SD-WAN

Sélectionnez Next pour configurer les paramètres SD-WAN. Cette étape implique la génération automatique des interfaces de tunnel en étoile et la configuration BGP du réseau de superposition. Dans la liste déroulante Spoke Tunnel Interface Security Zone, choisissez une zone de sécurité ou sélectionnez + pour créer une zone de sécurité à laquelle l'assistant ajoute automatiquement les interfaces SVTI (Static Virtual Tunnel Interfaces) générées automatiquement par les rayons.

Cochez la case Enable BGP on the VPN Overlay Topology pour automatiser les configurations BGP entre l'interface de tunnel de superposition. Dans le champ Autonomous System Number, entrez un numéro de système autonome (AS). Cochez la case Redistribute Connected Interfaces et choisissez un groupe d'interfaces dans la liste déroulante ou sélectionnez + pour créer un groupe d'interfaces avec des interfaces LAN connectées des concentrateurs et des rayons pour la redistribution de route BGP dans la topologie de superposition.



Dans le champ Balise de communauté pour les routes locales, entrez l'attribut de communauté BGP pour baliser les routes locales connectées et redistribuées. Cet attribut permet un filtrage facile des routes. Cochez la case Secondary Hub is in the Different Autonomous System si vous avez un concentrateur secondaire dans un autre système autonome. Enfin, cochez la case Enable Multiple Paths for BGP pour permettre à BGP d'équilibrer la charge du trafic sur plusieurs liaisons.

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	192.168.100.1	Spoke-Pool-Hub-1-ISP-1	
Hub-2	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	SD-WAN-Topology-ISP-1_Branch-1	SD-WAN-Topology-ISP-1_Branch-1
Branch-2	WAN-1	SD-WAN-Topology-ISP-1_Branch-2	SD-WAN-Topology-ISP-1_Branch-2
Branch-3	WAN-1	SD-WAN-Topology-ISP-1_Branch-3	SD-WAN-Topology-ISP-1_Branch-3
Branch-4	WAN-1	SD-WAN-Topology-ISP-1_Branch-4	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 hubs. [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](#)

Cliquez sur Finish pour enregistrer et valider la topologie 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	192.168.100.1	Spoke-Pool-Hub-1-ISP-1	
Hub-2	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	SD-WAN-Topology-ISP-1_Branch-1	SD-WAN-Topology-ISP-1_Branch-1
Branch-2	WAN-1	SD-WAN-Topology-ISP-1_Branch-2	SD-WAN-Topology-ISP-1_Branch-2
Branch-3	WAN-1	SD-WAN-Topology-ISP-1_Branch-3	SD-WAN-Topology-ISP-1_Branch-3
Branch-4	WAN-1	SD-WAN-Topology-ISP-1_Branch-4	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](#)

Vous pouvez afficher la topologie sous Périphériques > VPN de site à site. Le nombre total de tunnels dans la première topologie SD-WAN est de 8.

SD-WAN-Topology-ISP-1

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEx1	IKEx2
SD-WAN-Topology-ISP-1	Route Based (VTI)	SD-WAN Topology	Deployment Pending	✓	✓

Hub

Device	VPN Interface	VTI Interface
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)

Spoke

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

Viewing 1-8 of 8

Étape 7. Création d'une topologie SD-WAN avec WAN-2 comme interface VPN

Répétez les étapes 1 à 6 pour configurer une topologie SD-WAN avec WAN-2 comme interface VPN. Le nombre total de tunnels dans la seconde topologie SD-WAN est de 8. Les topologies finales doivent ressembler à l'image ci-dessous.

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution
SD-WAN-Topology-ISP-1	Route Based (VTI)	SD-WAN Topology	Deployment Pending
Hub			
Device	VPN Interface	VTI Interface	
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.11.100)	
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.11.100)	
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_3 (169.254.11.100)	
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_4 (169.254.11.100)	
Spoke			
Device	VPN Interface	VTI Interface	
Branch-1	WAN-1 (172.16.1.101)	WAN-1_static_vti_1 (169.254.11.101)	
Branch-2	WAN-1 (172.16.1.102)	WAN-1_static_vti_2 (169.254.11.102)	
Branch-3	WAN-1 (172.16.1.103)	WAN-1_static_vti_3 (169.254.11.103)	
Branch-4	WAN-1 (172.16.1.104)	WAN-1_static_vti_4 (169.254.11.104)	

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution
SD-WAN-Topology-ISP-2	Route Based (VTI)	SD-WAN Topology	Deployment Pending
Hub			
Device	VPN Interface	VTI Interface	
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_1 (169.254.12.100)	
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_2 (169.254.12.100)	
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_3 (169.254.12.100)	
Hub-1	WAN (192.168.100.1)	WAN_dynamic_vti_4 (169.254.12.100)	
Spoke			
Device	VPN Interface	VTI Interface	
Branch-1	WAN-2 (172.16.2.101)	WAN-2_static_vti_1 (169.254.12.101)	
Branch-2	WAN-2 (172.16.2.102)	WAN-2_static_vti_2 (169.254.12.102)	
Branch-3	WAN-2 (172.16.2.103)	WAN-2_static_vti_3 (169.254.12.103)	
Branch-4	WAN-2 (172.16.2.104)	WAN-2_static_vti_4 (169.254.12.104)	

Étape 8 : configuration des zones ECMP

Sur chaque branche, accédez à Routing > ECMP et configurez les zones ECMP (Equal-Cost Multi-Path) pour les interfaces WAN et les SVTI se connectant au concentrateur principal et secondaire, comme indiqué ci-dessous. Cela peut fournir une redondance de liaison et activer l'équilibrage de charge du trafic VPN.

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

Étape 9. Modification de la préférence locale BGP sur le concentrateur

Accédez à Routing > General Settings > BGP sur le concentrateur secondaire. Sélectionnez Enable BGP, configurez le numéro AS, et définissez la valeur de préférence locale par défaut sous Best Path Selection à une valeur inférieure à celle configurée sur le concentrateur principal. Sélectionnez Enregistrer. Cela garantit que les routes vers le concentrateur principal sont préférées aux routes vers le concentrateur secondaire. Lorsque le concentrateur principal tombe en panne, les routes vers le concentrateur secondaire prennent le relais.

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

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

EGRP

RIP

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

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

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

Déployez les configurations sur tous les périphériques.

Vérifier

Vérification des états du tunnel

Pour vérifier si les tunnels VPN des topologies SD-WAN sont actifs, sélectionnez Device > VPN > Site-to-Site.

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy Search Add admin

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)

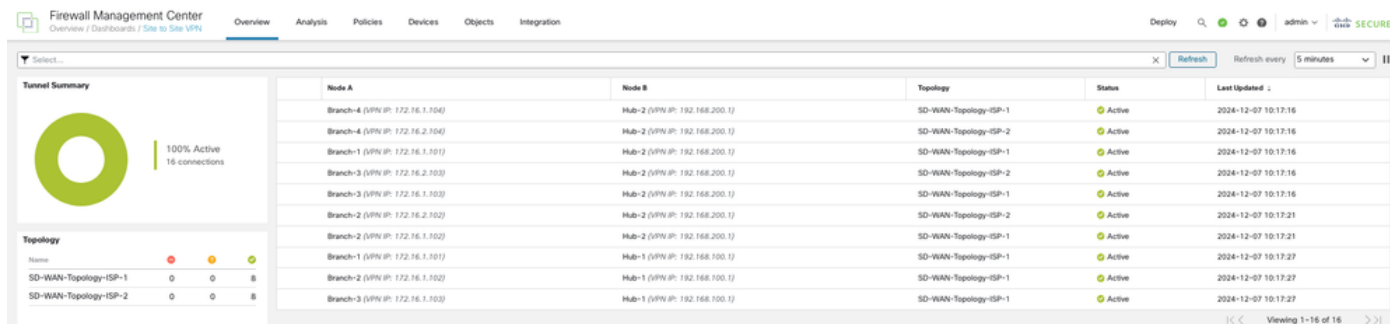
SD-WAN-Topology-ISP-2 Route Based (VTI) SD-WAN Topology 0 Tunnels

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)

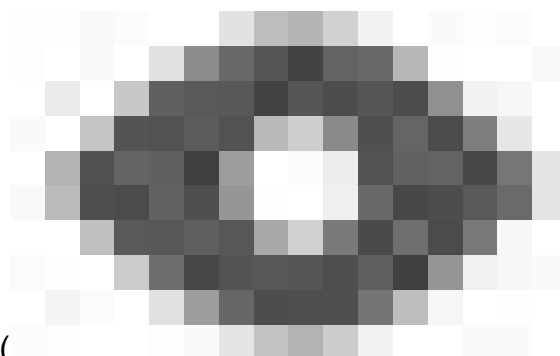
Viewing 1-8 of 8

Pour afficher les détails des tunnels VPN SD-WAN, choisissez Overview > Dashboards > Site-to-site VPN.



Pour afficher plus de détails sur chaque tunnel VPN :

1. Survolez un tunnel.



2. Sélectionnez l'option Afficher toutes les informations (). Un volet contenant les détails du tunnel et d'autres actions s'affiche.

3. Sélectionnez l'onglet CLI Details dans le volet latéral pour afficher les commandes show et les détails des associations de sécurité 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

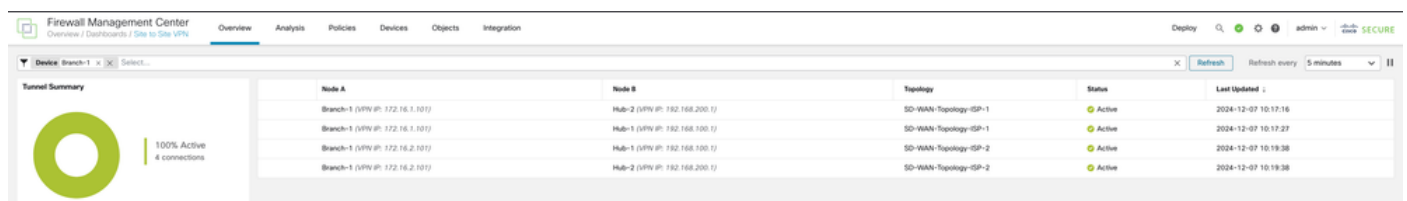
Branch-1 (VPN Interface IP: 172.16.2.101)

show crypto ipsec sa peer 192.168.100.1 ⓘ

WAN-2_static_vti_3 - SVTI vers concentrateur 1 via FAI 2
 WAN-1_static_vti_2 - SVTI vers concentrateur 2 via FAI 1
 WAN-2_static_vti_4 - SVTI vers le concentrateur 2 via le FAI 2

Vérification de l'équilibrage de charge du trafic VPN

L'état du tunnel est visible dans le tableau de bord VPN site à site. Idéalement, tous les tunnels doivent être actifs :



Node A	Node B	Topology	Status	Last Updated
Branch-1 (VPN IP: 172.16.1.101)	Hub-2 (VPN IP: 192.168.200.1)	SD-WAN-Topology-ISP-1	Active	2024-12-07 10:17:16
Branch-1 (VPN IP: 172.16.1.101)	Hub-1 (VPN IP: 192.168.100.1)	SD-WAN-Topology-ISP-1	Active	2024-12-07 10:17:27
Branch-1 (VPN IP: 172.16.2.101)	Hub-1 (VPN IP: 192.168.100.1)	SD-WAN-Topology-ISP-2	Active	2024-12-07 10:19:38
Branch-1 (VPN IP: 172.16.2.101)	Hub-2 (VPN IP: 192.168.200.1)	SD-WAN-Topology-ISP-2	Active	2024-12-07 10:19:38

Les routes vers le concentrateur principal sont privilégiées. La commande show route sur Branch1 indique que le trafic VPN est équilibré en charge entre les deux SVTI sur ISP1 et ISP2 vers le concentrateur principal :

CLI Troubleshoot

>_ Command:
Execute Refresh Copy

Device:

```

> 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

```

Close

L'interface de sortie prise pour le trafic VPN réel peut être vue dans Unified Events :

Firewall Management Center												
Analysis / Unified Events												
Events Troubleshooting												
Source IP: 10.10.0.100 x Destination IP: 10.10.0.100 x												
12 100 0 0 0 0 12 events												
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
2024-12-08 08:11:13	% Connection	10.10.0.100	10.10.0.100	53910 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Branch-1	172.16.1.101	WAN-2_static_v6_3	192.168.100.1
2024-12-08 08:11:13	% Connection	10.10.0.100	10.10.0.100	53910 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Branch-1	172.16.1.101	LAN	192.168.100.1
2024-12-08 08:11:12	% Connection	10.10.0.100	10.10.0.100	53896 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Branch-1	172.16.1.101	WAN-1_static_v6_1	192.168.100.1
2024-12-08 08:11:11	% Connection	10.10.0.100	10.10.0.100	53896 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Hub-1	172.16.1.101	LAN	192.168.100.1

Vérification de la redondance ISP double

Lorsque ISP-2 est désactivé, l'état du tunnel indique que les tunnels via ISP-1 sont actifs :

Firewall Management Center

Overview / Dashboards / Site to Site VPN

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

admin

SECURE

Device: branch-1 x Select...

Refresh

Refresh every 5 minutes

Tunnel Summary

50% Active
2 connections

50% Inactive
2 connections

Node A	Node B	Topology	Status	Last Updated
Branch-1 (VPN IP: 172.16.1.101)	Hub-2 (VPN IP: 192.168.200.1)	SD-WAN-Topology-ISP-1	Active	2024-12-07 10:17:16
Branch-1 (VPN IP: 172.16.1.101)	Hub-1 (VPN IP: 192.168.100.1)	SD-WAN-Topology-ISP-1	Active	2024-12-07 10:17:27
Branch-1 (VPN IP: 172.16.2.101)	Hub-1 (VPN IP: 192.168.100.1)	SD-WAN-Topology-ISP-2	Inactive	2024-12-08 08:29:41
Branch-1 (VPN IP: 172.16.2.101)	Hub-2 (VPN IP: 192.168.200.1)	SD-WAN-Topology-ISP-2	Inactive	2024-12-08 08:29:41

Les routes vers le concentrateur principal sont privilégiées. La commande show route sur Branch1 indique que le trafic VPN est routé via les SVTI sur ISP-1 vers le concentrateur principal :

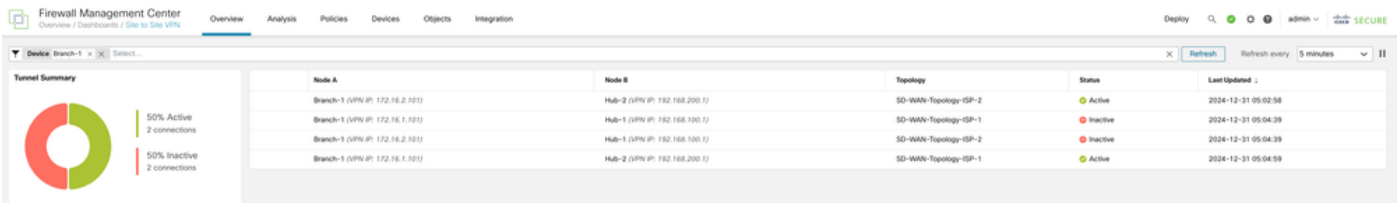
CLI Troubleshoot												
Device: Branch-1												
> Command: show route Execute Refresh Copy												
> show route Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF 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 169.254.11.100, 00:04:02 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 169.254.21.0 255.255.255.0 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 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 D 172.16.2.0 255.255.255.0 [90/1280] via 172.16.1.1, 00:04:03, WAN-1 D 192.168.1.0 255.255.255.0 [90/768] via 172.16.1.1, 22:12:57, WAN-1 D 192.168.2.0 255.255.255.0 [90/1024] via 172.16.1.1, 00:04:03, WAN-1 D 192.168.100.0 255.255.255.0 [90/1024] via 172.16.1.1, 00:04:03, WAN-1 D 192.168.200.0 255.255.255.0 [90/1024] via 172.16.1.1, 00:04:03, WAN-1												

L'interface de sortie prise pour le trafic VPN réel peut être vue dans Unified Events :

Firewall Management Center												
Analysis / Unified Events												
Events Troubleshooting												
Source IP: 10.10.0.100 x Destination IP: 10.10.0.100 x												
16 100 0 0 0 0 16 events												
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
2024-12-08 08:30:33	% Connection	10.10.0.100	10.10.0.100	32800 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Branch-1	172.16.1.101	WAN-1_static_v6_1	192.168.100.1
2024-12-08 08:30:32	% Connection	10.10.0.100	10.10.0.100	32800 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Hub-1	172.16.1.101	LAN	192.168.100.1
2024-12-08 08:30:28	% Connection	10.10.0.100	10.10.0.100	32794 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Branch-1	172.16.1.101	WAN-1_static_v6_1	192.168.100.1
2024-12-08 08:30:27	% Connection	10.10.0.100	10.10.0.100	32794 / tcp	22 (ssh) / tcp		New-Rule-#1-ALLOW	FTD-ACP	Hub-1	172.16.1.101	LAN	192.168.100.1

Vérification de la redondance au niveau du concentrateur

Lorsque le concentrateur principal est en panne, l'état du tunnel indique que les tunnels vers le concentrateur secondaire sont actifs :



Comme le concentrateur principal est en panne, les routes vers le concentrateur secondaire sont privilégiées. La commande show route sur Branch1 indique que le trafic VPN est équilibré en charge entre les deux SVTI sur ISP1 et ISP2 vers le concentrateur secondaire :

```
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'interface de sortie prise pour le trafic VPN réel peut être vue dans Unified Events :

The screenshot shows the Firewall Management Center interface with the 'Unified Events' tab selected. The table displays the following information:

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.