

عقروم ىلإ عقروم نم VPN ل SD-WAN نيوكت نم آةيامح رادج ربع

تايوتحملا

[عمدقملا](#)

[ةيساسالاب تابلطتملا](#)

[تابلطتملا](#)

[عمدختسملا تانوكملا](#)

[ةزيملا تامولعم](#)

[ةاطغملا ايجولوبوطلا](#)

[\(دحاو \(ISP\) تنرتنالا عمدخ دوزم\) ملكتملا وعزوملا](#)

[لوكوتورب ربع ةيطايتحل لصو ةحول ىلإ ISP لوكوتورب لخدأ\) ةجودزم ةثداحمولصو ةحول
\(ةيعرفلا ماسقألاو ةيوناثلا لصولا ةحول نيي eBGP](#)

[ربع ISP لصومو ريكتملا عزوملل ةجودزم \(ISP\) تنرتنالا عمدخ دوزم\) ةجودزم ةثداحمولصو ةحول
\(ةيعرفلا ماسقألاو ةيوناثلا عزوملا نيي eBGP لوكوتورب](#)

[يارقلا](#)

[ةلص تاذ تامولعم](#)

عمدقملا

هيجوت عم راسملا ىلإ ةدنتسملا VPN تاكبش رشن تاهوي راني س دنتسملا اذه فصى
نم آلآةيامح رادج ىلإ SD-WAN ةزيم مادختساب BGP ةيشغت

ةيساسالاب تابلطتملا

سفن لالخ نم اهترادإ متتو، هذعب ام وأ FTD 7.6 جم انرب ليغشتب دي داخألاو رواحملا لك موقت
رخأتم ةيجمر رب وأ 7.6 ليغشتب اضيأ موقت يتلاو، ةيلاملا ةرادإلا يف مكحتلا ةدحو

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كي دل نوكت ناب Cisco ي صوت

- IKEv2
- راسملا ىلإ دنتست VPN ةكبش
- (VTI) ةيرهاظلا قافنألا تاهجاو
- IPsec
- BGP

عمدختسملا تانوكملا

ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست

- Cisco Secure Firewall Threat Defense 7.7.10
- Cisco Secure Firewall Management Center 7.7.10

ةصاخ ةي لمعم ةئي ب ي ف ةدوجومل ةزهجال نم دنتسمل اذه ي ف ةدراول تامولعمل عاشنإ مت تناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسمل اذه ي ف ةمدختسمل ةزهجال عي مج تادب رما يال لمحتمل ريثأتلل كمهف نم دكأتف ،ليغشتل دي قكتك تش

ةزيمل تامولعمل

هي جوتلاو (VPN) ةيره اظلال ةصاخلا ةكبشل قافنأ نيوكت طيسبت ىلع ةرادإل زكرم لمعي SD- WAN جلام مادختساب (عورفال) ةديعبل عورفال عقاومو (عيزوتل تاحول) ةيزكرمل راقمل ني ب دي دجل WAN.

• قفنللة هجاو DVTI نم ةدافتسالا لال خ نم (VPN) ةيره اظلال ةصاخلا ةكبشل نيوكت ةتمتأ .
تالو حمل ىلع (ةتباثلل ةيره اظلال قفنللة هجاو) SVTI و روا حمل ىلع (ةيكيماني دلل ةيره اظلال BGP لال خ نم بكارتلل هي جوت ني كمت عم

• امب ،لماكل VTI نيوكت عفديو و تاحولل SVTI ب ةصاخلا IP نيوانع نييعتب ايئاقلت موقي .
ري فشتل تامولعمل كلذ ي ف

• فلامل هي جوتلل BGP ني كمتل جلامل س فن لخاد ةدحاو ةوطخ لهس هي جوت نيوكت رفوي .

• لو كوتوربل راسمل سكاع ةمس ةدايز لال خ نم ري و طتلل لباقلاو لثمألا هي جوتل ني كمت BGP.

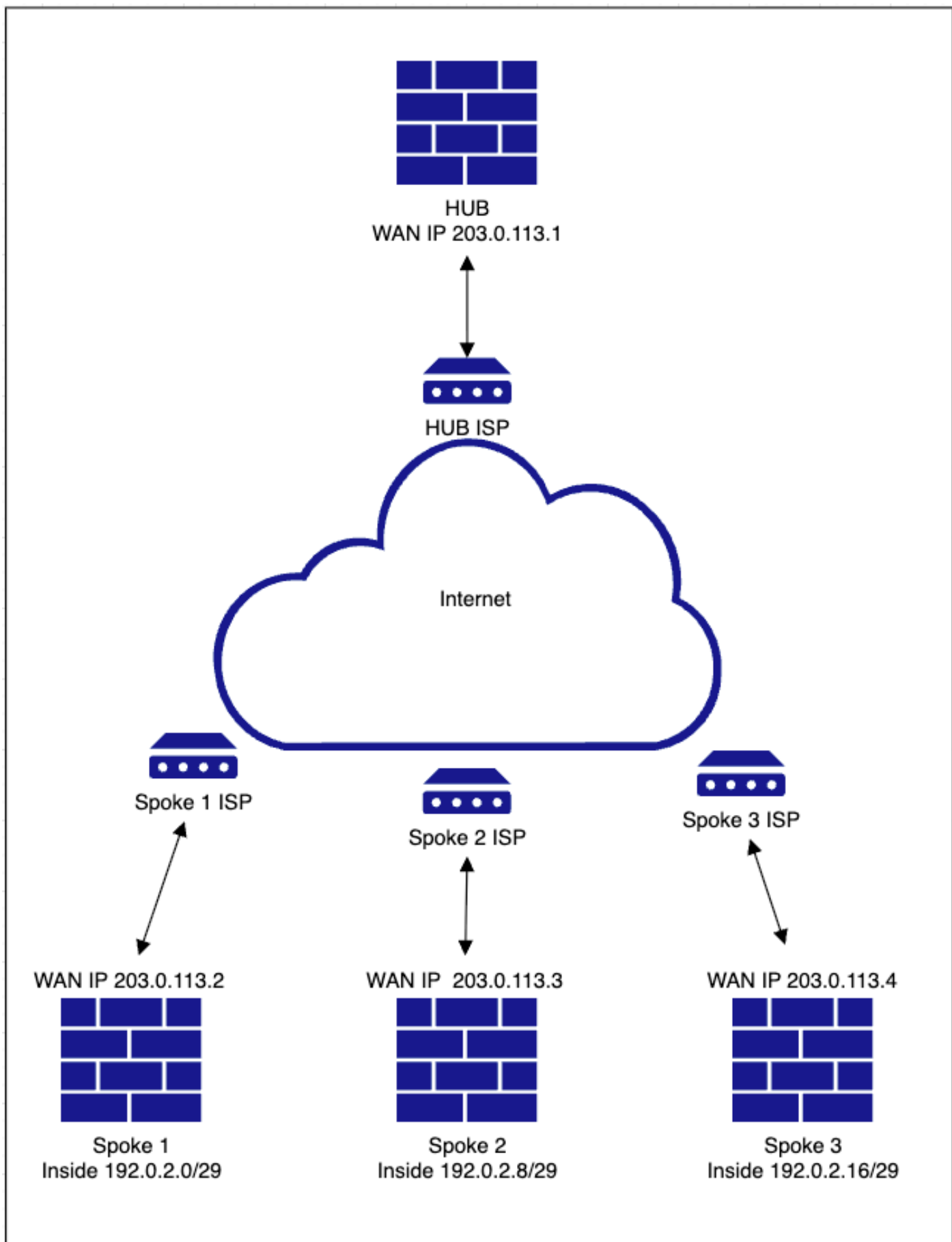
• م دختسمل ل خدت نم ىندألا دحل عم دحاو نآ ي ف تالو حمل نم دي دعلل ةفاضاب حمسي .

ةاطغملا اي جولوب و طلا

ةيارد ىلع ني م دختسمل نأ نامضل تاططخملا نم دي دعلل ةيطغت تمت ،ةلاقمل هذه ي ف رشنل تاهوي راني س فلتخم ب

(دحاو (ISP) تنرتنإلا ةمدخ دوزم) ملكتمل او عزومل

ةكبشلل يطي طختل مسرلا



تاني وكتال

- عاشن | > > SD-WAN ططخم > ةفاض | > عقوم ىل عقوم > VPN > ةزهأل ىل لقتنا

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy Search Settings Help 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](#)

نم دكأت ال عاجرل، DVTI نيوك ت نم عزك .لوصول ةحول ةيانه ي ف DVTI عاشن او روحم ةفاضل .
ططخملل اقفو ةحيحصلا قفنل ا رصم ةهجاو دي دحت .

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

- مداخلتسإ متي .ةفاضإ مث ظفح قوف رقناو قفنلإ ربع IP نيوانع عمجت عاشنإب مق عورفلإ ىلإ VTI قفنب ةصاخلا IP نيوانع نييعتل IP نيوانع عمجت

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

3 Authentication Settings 📘

4 SD-WAN Settings

Cancel Finish

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

HUB-Spoke-VPN-Single-ISP

Hub and Spoke Route-Based (VTI) VPN Topology

1 Hubs 📘

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

Add Hub

Next

2 Spokes 📘 Edit

3 Authentication Settings 📘 Edit

4 SD-WAN Settings Edit

Cancel Finish

- عفاضا راىخ نم ءءافءءءالا كنكمى .ءالءءلءءمءا ءفضاؤ رءءابى نأ كلذ ءعب ءقءقء لءالء ءفاضاىء ءمق وأ ءكرءءم قءانم / ءءاؤ ءامءأ كىءل ناك اذا ءرىبك ءاىمك

ي.درف لك ش ب

FMC Site To Site Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 13 ⚙️ ? 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 ⓘ

View Generated Tunnel Interfaces

Add Spokes (Bulk Addition)

Add Spoke

No spokes are configured. Add a spoke.

Next

3 Authentication Settings ⓘ Edit

4 SD-WAN Settings Edit

Cancel Finish

- في كرتشت ةزهجألا ت ناك اذا .ةيجراخلا ةهجاوول/WAN ةهجاوول ةي مست طمن ددحو ةزهجألا ددح ناك اذاو ،كلذ دع ب تقطقط .اي فاك نو كي لولوال فرحألا مادختسا نإف ،ةهجاوول مساسفن اضيأ كنكمي ،ةعمجمل تافاضلال ةبسنلاب .فيضي تقطقط ،حجان قيقدتلا ةقيرطال سفسن ةقطنملا مسامادختسا

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

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

Next

3 Authentication Settings Edit

4 SD-WAN Settings Edit

Cancel Back Add

Cancel Finish

- كلذ دعب ،تيقتنا حيحص نراقالنا نمضي نا ليصفت نراق فلغيونراقالنا تقق د
كلذ دعب تققط.

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

- صصخم تارفش دي دحت وأ IPsec ني وكتل ةي ضار ت فالال تامل عمل اب ظا ف ت حالال اما كن كم ي
تامل عمل م دخت ست ، دن تس م الا اذه ي ف . رشابي نأ كل ذ دعب تق ط ق ط . بولطم وه امك
ةي ضار ت فالال .

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

- لالځ نم اچولوب طال هډل چل اعمال س فن نمضه ښغ تال هچوت نښوکت کننکمي، اړيځ او عم تچم ل تامال عو ډي لځ ادل هه چ اول تانال ع او AS مقر لثم، ډس انم ل BGP تامل عم ډي دت ربع رورم ل ډکړه ډي فصت ډي ف نامال ډقطنم دعاست نا نکمي. تائ دابل ډي فصت ل اهم ادخت ساو تاه چ اول ل نئ اک عاشن اضي ا کننکمي امنښ ب لوصول ډي ف مکتحت ل تاسا ډس ريغ و ا ډي لځ ادل مسال نع افل تخم مسال ناک اډا ډلصت م ل تاه چ اول عيزوت ډداع ډي ف ططخم ل ډي ف ډزه چال ربع لثام ت.

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
Edit

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

2 Spokes
Edit

Device ftd2 VPN Interface VPN-OUT-1 Key ID: HUB-Spoke-VPN-Single-ISP_ftd2
Device ftd3 VPN Interface VPN-OUT-1 Local Tunnel (IKE) Identity Key ID: HUB-Spoke-VPN-Single-ISP_ftd3
Device ftd4 VPN Interface VPN-OUT-4 Key ID: HUB-Spoke-VPN-Single-ISP_ftd4

3 Authentication Settings
Edit

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

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

- ةيلعملعلا لامكإل رشن اريخأو، ءءان م ث ،يلاتل قوف رقنا .

ققحتل

- عقوم ىلإ عقوم > VPN > ةزهجألا ىلإ لاقتنالاب قفنللا ةلاح نم ققحتل كنكمي .

Firewall Management Center Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ? admin ▾ SECURE

Devices / VPN / Site To Site

Last Updated: 12:06 PM Refresh NAT Exemptions Add

Select... X Refresh

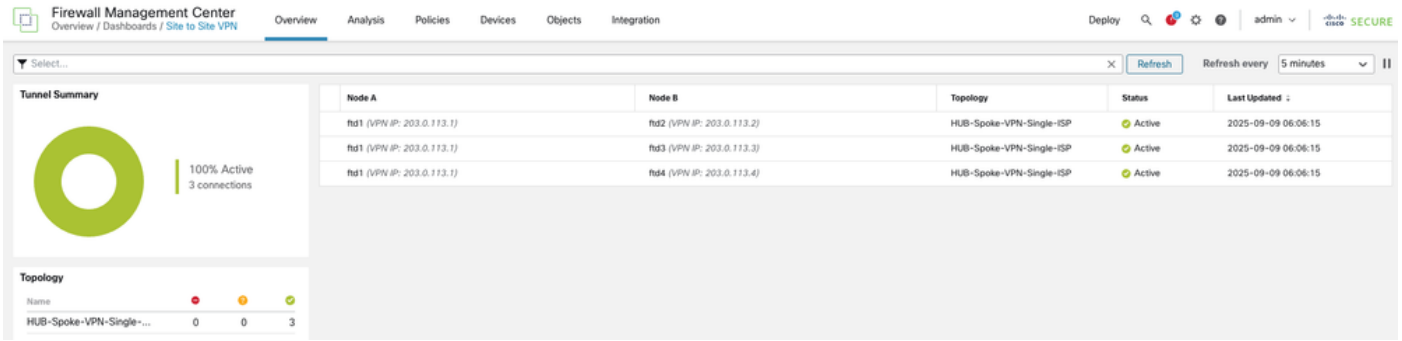
Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	BKEv1	BKEv2
HUB-Spoke-VPN-Single-ISP	Route Based (VTI)	SD-WAN Topology	Tunnels	✓	

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... (10.18.89.254)	FTD ftd2	VPN-OUT-1 (203.0.113.2)	VPN-OUT-1_static... (198.51.100.10)
FTD ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynamic... (10.18.89.254)	FTD ftd3	VPN-OUT-1 (203.0.113.3)	VPN-OUT-1_static... (198.51.100.11)
FTD ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynamic... (10.18.89.254)	FTD ftd4	VPN-OUT-4 (203.0.113.4)	VPN-OUT-4_static... (198.51.100.12)

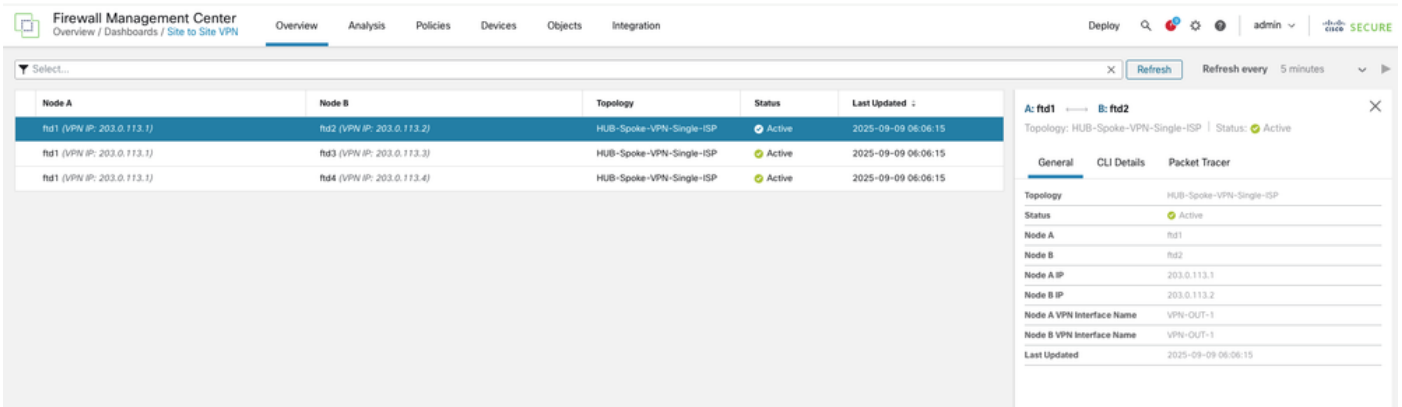
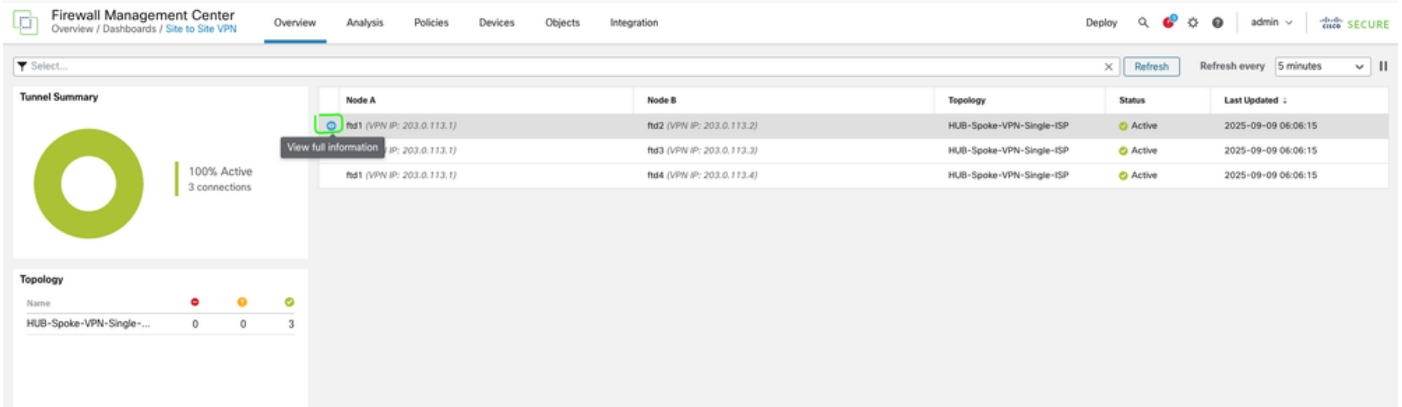
Viewing 1-3 of 3

- تاحول > ةماع ةرطن ىلإ لاقتنالالا لالخ نم ةيفاضإلا لىصافتلا نم ققحتل كنكمي .

VPN عقوم ىلا عقوم > تامولعمل



- قلمالكلا تامولعمل ضرع قوف رقناو قفنا دح، ىؤرلا نم ديزم ىلع لوصحلل



Firewall Management Center
Overview / Dashboards / Site to Site VPN

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin | **SECURE**

Select...

Node A	Node B	Topology	Status	Last Updated
ftd1 (VPN IP: 203.0.113.1)	ftd2 (VPN IP: 203.0.113.2)	HUB-Spoke-VPN-Singl...	Active	2025-09-09 06:06:15
ftd1 (VPN IP: 203.0.113.1)	ftd3 (VPN IP: 203.0.113.3)	HUB-Spoke-VPN-Singl...	Active	2025-09-09 06:06:15
ftd1 (VPN IP: 203.0.113.1)	ftd4 (VPN IP: 203.0.113.4)	HUB-Spoke-VPN-Singl...	Active	2025-09-09 06:06:15

Refresh Refresh every 5 minutes

A: ftd1 → B: ftd2
Topology: HUB-Spoke-VPN-Single-ISP | Status: Active

General CLI Details Packet Tracer

Refresh Maximize view

Summary

Node A (203.0.113.1/500)	Node B (203.0.113.2/500)
Transmitted: 9.52 KB (9744 B)	Transmitted: 9.26 KB (9481 B)
Received: 12.33 KB (12628 B)	Received: 12.61 KB (12912 B)

IPsec Security Associations (1)

0.0.0.0/0.0.0.0/0 0.0.0.0/0.0.0.0/0

ftd1 (VPN Interface IP: 203.0.113.1)

```

show crypto ipsec sa peer 203.0.113.2
peer address: 203.0.113.2
interface: VPN-OUT-1_dynamic_vti_1_va9
Crypto map tag: VPN-OUT-1_dynamic_vti_1_vtemplate_dyn_map, seq num: 1, local addr: 203.0.113.1

Protected vrf (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

- اهتي دجت نكمي و FTD ب صاخلا (CLI) رم اوألا رطس ةهجاو نم ةرشابم جارخإلا ضرع متي (SPI) نامألا تامل علم سرهف لي صافات لثم ، ةمهمل تامولعمل او ةثدحمل تادادعل ضرعل

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)	ftd2 (VPN Interface IP: 203.0.113.2)
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: 100 Protected vrf (ivrf): Global local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 203.0.113.2 #pkts encaps: 155, #pkts encrypt: 155, #pkts digest: 155 #pkts decaps: 154, #pkts decrypt: 154, #pkts verify: 154 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 155, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reas: 0 #TFC rcvd: 0, #TFC sent: 0 #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0 #pkts not offload decrypted: 154 #send errors: 0, #recv errors: 0 local crypto endpt.: 203.0.113.1/500, remote crypto endpt.: 203.0.113.2/500 path mtu 1500, ipsec overhead 55(36), media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: 3EE69843 current inbound spi : D113FBF4 inbound esp sas: spi: 0xD113FBF4 (3507747828) SA State: active transform: esp-aes-gcm-256 esp-null-hmac no compression in use settings = {L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 9, crypto-map: VPN-OUT-1_dynamic_vti_1_vtemplate_dyn_map sa timing: remaining key lifetime (sec): 24309	show crypto ipsec sa peer 203.0.113.1 ⓘ peer address: 203.0.113.1 interface: VPN-OUT-1_static_vti_1 Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) Protected vrf (ivrf): Global local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 203.0.113.1 #pkts encaps: 154, #pkts encrypt: 154, #pkts digest: 154 #pkts decaps: 155, #pkts decrypt: 155, #pkts verify: 155 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 154, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reas: 0 #TFC rcvd: 0, #TFC sent: 0 #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0 #pkts not offload decrypted: 155 #send errors: 0, #recv errors: 0 local crypto endpt.: 203.0.113.2/500, remote crypto endpt.: 203.0.113.1/500 path mtu 1500, ipsec overhead 55(36), media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: D113FBF4 current inbound spi : 3EE69843 inbound esp sas: spi: 0x3EE69843 (1055299651) SA State: active transform: esp-aes-gcm-256 esp-null-hmac no compression in use settings = {L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1 sa timing: remaining key lifetime (sec): 24308

- **ةلاحو هيچوتلا تامولعم نم ققحتلل FTD ل (CLI) رماوالا رطس ةهجاو مادختسا نكمي امك BGP عىزجت.**

عزوم لا بناج یلع

<#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

ربكم بناج ىلع

دحا نم لاثم انه .اهب شذحتال متي يتال ةزهجال لىل ققحتال سفن ارجا اضيأ نكميو
نېببقال.

<#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

BBBBBBBB 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
*>192.0.2.8/29	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

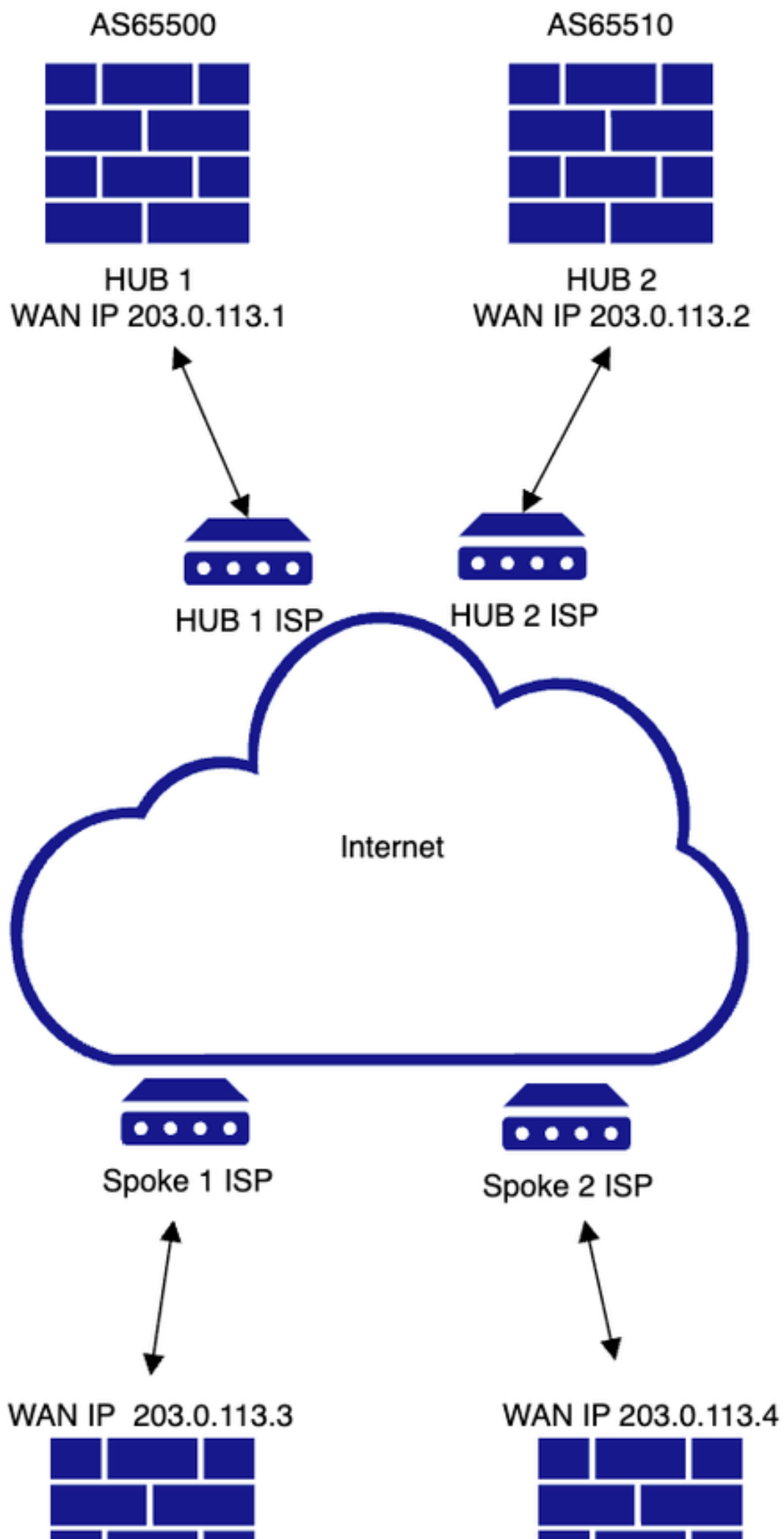
<<<<<< spoke 2 inside network

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

<<<<<< spoke 3 inside network

رَبْعَة طَيَّا حِإْ لَصَوَّة حَوْلِى إِي إِي ISP لَو كَوْت وِرْب لَخْدَا (عَجْو دَزَمَة ثِدَا حَمَو لَصَوَّة حَوْلِى
(عَي عَرَفَ لَ مَاس قَالَاوَة يَوْنَا ثَلَا لَصَوَلَا عَوْل نِي بَ eBGP لَو كَوْت وِرْب

ة كَبْ شَلَلِى طَيَّا خَتَلَا مَسَرَلَا



تاوطلخال س فن مادختساب ينثال ع زومال عفاضا الى لقتنا ،لوال ع زومال عفاضا دعب
HUB1. ل اقباس ةمدختسمل

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

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: 198.51.100.10-198.51.100.11

Next

- (DVTI) ةيكيما ني دل ةيره اطلال ق فنل ةهجاو عاشنل ةعبات ملاب مق

Firewall Management Center 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

Device: ftd1 Threat Defense

Add Virtual Tunnel Interface

General Path Monitoring

Tunnel Type: ☒ Static ☒ Dynamic

Name: VPN-OUT-1_dynamic_vti_1

☒ Enabled

Description:

Security Zone:

Priority: 0 (0 - 65535)

Virtual Tunnel Interface Details

An interface named TunnelID* 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) 203.0.113.2

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: 169.254.2.1/30

☐ Configure IP

☒ Borrow IP (IP unnumbered) Select Interface +

Add Loopback Interface

General IPv4 IPv6

Name: VPN-OUT-LOOPBACK

☒ Enabled

Loopback ID: 1 (1 - 1024)

Description

Cancel OK

- مق .لصتمل بانجال الى ع 2 هجوم لاب ةصاخال VTI قافنأل دي دج IP ناو نع عمجت دوجو مزلي .تاري غتال ظفح م ث ،هني وكتو دي دجال عمجتال عاشنل اب

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 VPN Interface VPN-OUT-1 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 VPN Interface VPN-OUT-1 Local Tunnel (IKE Identity) Key ID: HUB-Spoke-VPN-Single-ISP_ftd3

Device ftd4 VPN Interface VPN-OUT-4 Local Tunnel (IKE Identity) 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

- في SD-WAN تاداعإ ليدعتب مق ،يديخالو يوناثال روحملا ني ب eBGP ريظن ني وكتل ماطنل تنيعو فلتخم لقتسم ماطن ي ف ةرص يوناث راخال تنكم .ةيئاهنل ةوطخل دح كانه نكي مل اذا اضيأ iBGP مادختسإ نكمي .ةرص يوناثال ل مقرر (AS) يتاذل ماطن ي ف يوناثال HUB راخال كرت قي رط نع كتئي ب يل ع فلتخم AS مقرر مادختسال .اضيأ يوناث روحملا AS مقرر عم تجملا مقرر سفن اذه ع فدي .ددحم ريغ فلتخم لقتسم ي.لحال دادعإل eBGP يل ع ةلاقملا زكرت

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 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.

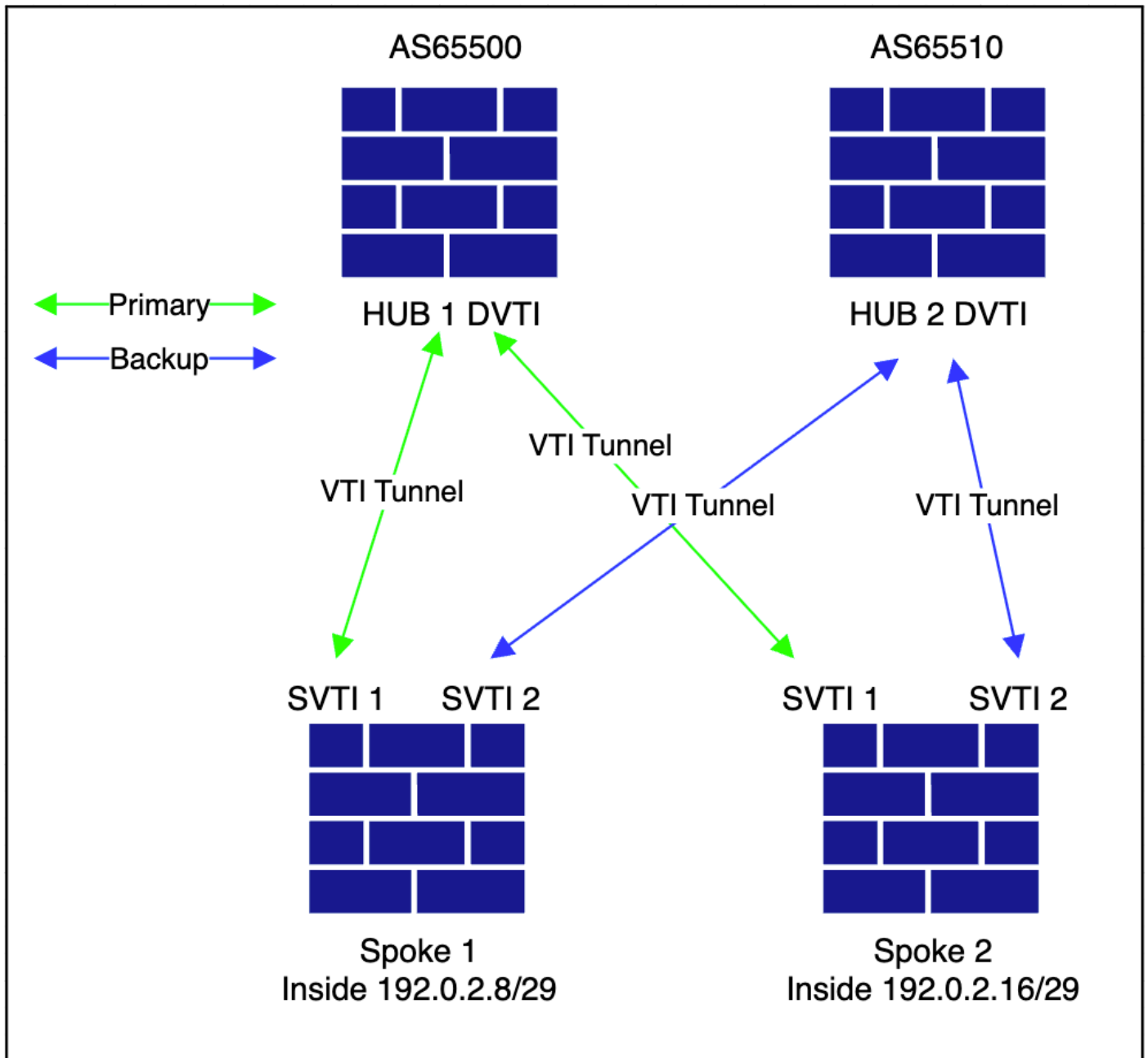
Next You have unsaved changes

Cancel Finish

نيوكتالا اذه في ناتديرف عم تجملة مالعو (AS) يتاذلا ماظنلا مقرر نم لك نأ نم دكأت

ققحتلا

نيمضتلا يطي طختلا مسرلا اذه حضوي



- عقوم ىلا عقوم > VPN > ؤهؤال اللى لقتنا، FMC ي ف

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾ Cisco **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	✓	

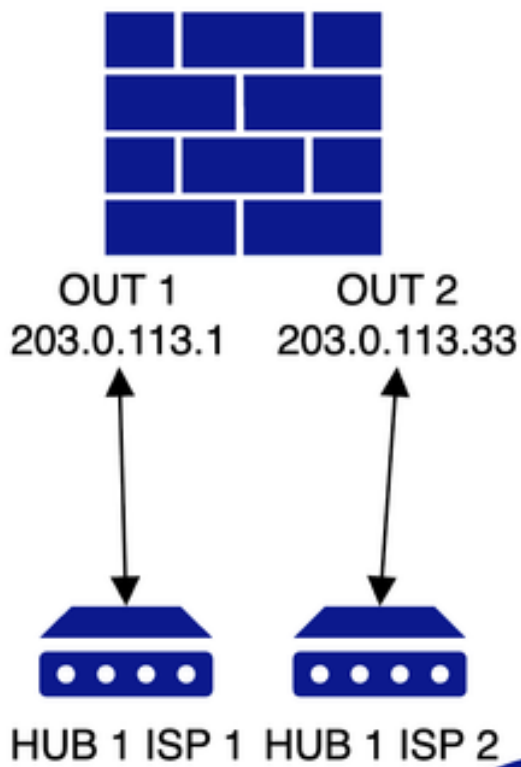
Hub			Spoke		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
FTD ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynam... (198.51.100.1)	FTD ftd3	VPN-OUT-1 (203.0.113.3)	VPN-OUT-1_static... (198.51.100.10)
FTD ftd1	VPN-OUT-1 (203.0.113.1)	VPN-OUT-1_dynam... (198.51.100.1)	FTD ftd4	VPN-OUT-4 (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 >>

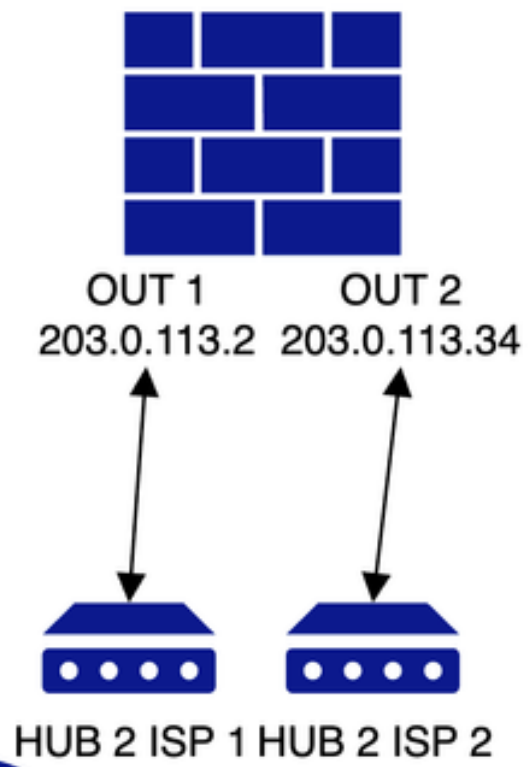
- رىىغت نود ىرؤال ا تاوطؤال اىمؤ لظتو

ررکتملا عزوملل جودزم (ISP) تنرتنإلا ةمدخ دوزم ةجودزم ةثداحم و لصو ةحول
(ةعرفلا ماسقألاو يوناتلا عزوملا نیب eBGP لوكوتورب رب ع ISP لصومو
ةكبشلل یطیطختلا مسرلا

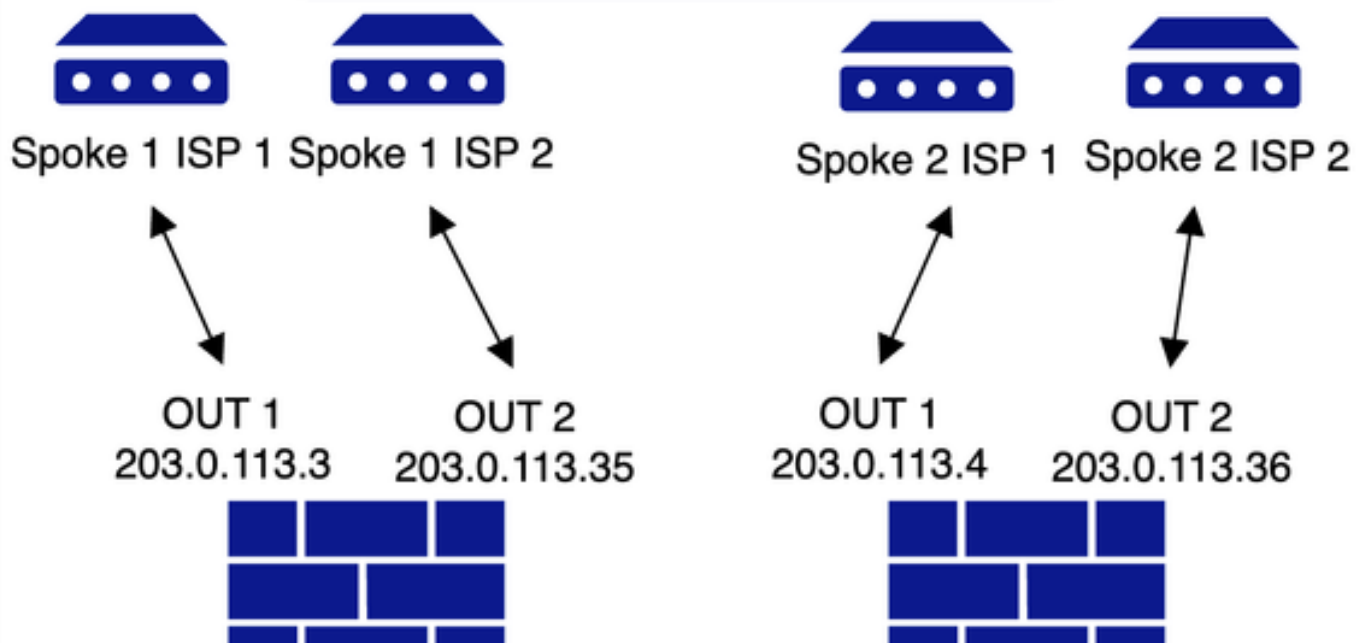
AS65500



AS65510



Internet



يقيمت التاني وكالتا نكلو فلتختم انا ق طانم اي جولو بطلال مدخت ست .ةق باسل
يمازل اذه .اهس فن يه عم تجم ال تامال ع عم ةي وناثال او ةي ساس ال زكارم ال ماقرأ لثم
ططخم ال ةحص نم ققحت ال لامك ال مدخت سمل ةه جاول

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
Gateway IP Address 203.0.113.33
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
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

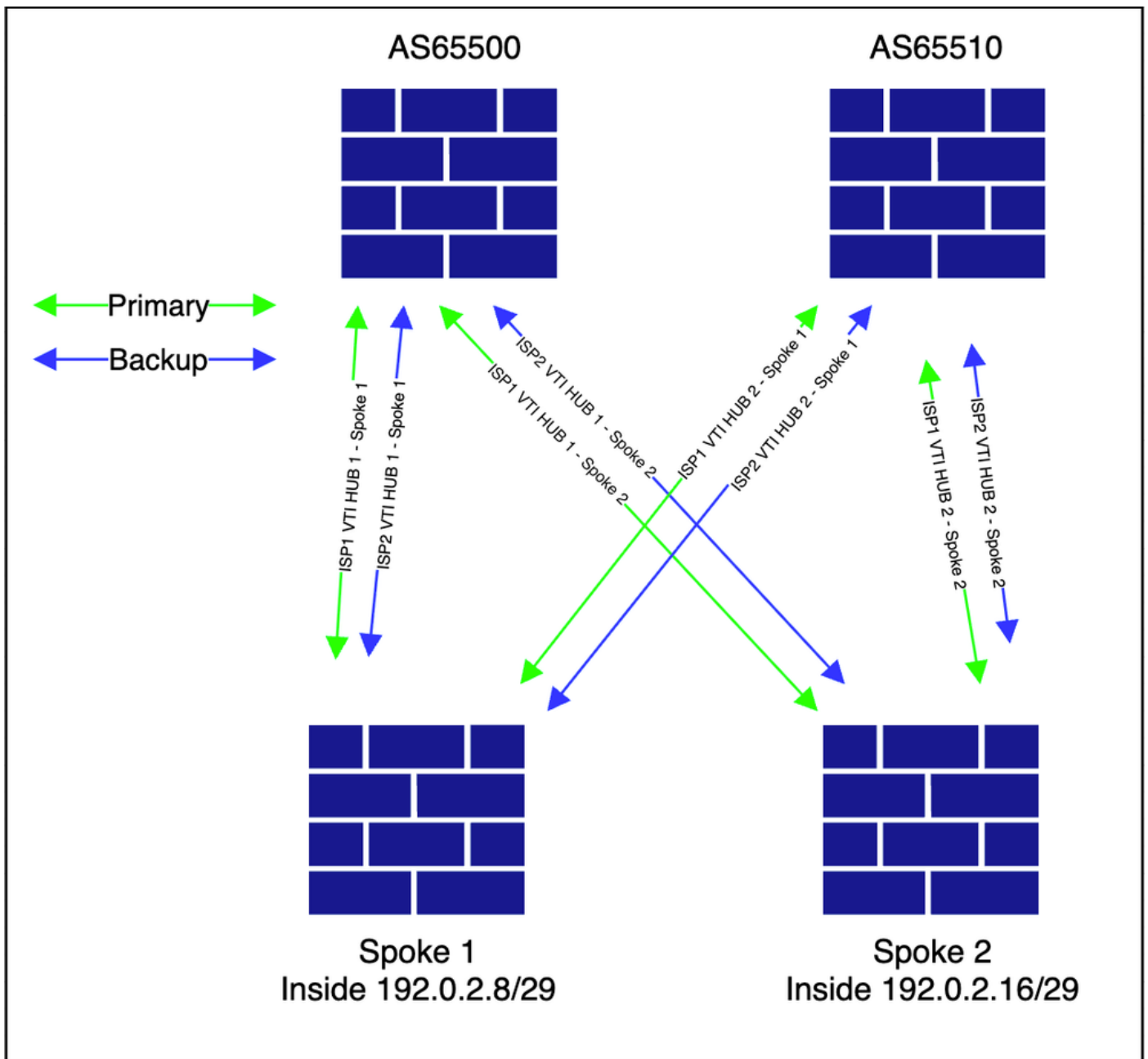
Cancel

Finish

- رشنن ال ةي لمع عبات و جال عم ال لمك أ .ريي غت نودب ى رخ ال ا تادادع ال ةفاك ى قبت

ققحت ال

- حضوم وه امك ططخم ال ره ظي



- ططخم لا ضرعل عقوم ىلإ عقوم > VPN > ةزهجألا ىلإ لقتنا

Firewall Management Center
Devices / VPN / Site To Site

Overview Analysis Policies **Devices** Objects Integration Deploy Settings Admin Cisco **SECURE**

Last Updated: 03:26 PM Refresh NAT Exemptions Add

Select... X Refresh

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)	HUB 1 ISP 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)	HUB 2 ISP 1	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 >>

Hub				Spoke			
Device	VPN Interface	VTI Interface		Device	VPN Interface	VTI Interface	
FTD ftd1	VPN-OUT-2 (203.0.113.33)	HUB 1 ISP 2	VPN-OUT-1_dynam... (198.51.100.3)	FTD ftd3	VPN-OUT-2 (203.0.113.35)	VPN-OUT-2_static_... (198.51.100.70)	
FTD ftd1	VPN-OUT-2 (203.0.113.33)		VPN-OUT-1_dynam... (198.51.100.3)	FTD ftd4	VPN-OUT-2 (203.0.113.36)	VPN-OUT-2_static_... (198.51.100.71)	
FTD ftd2	VPN-OUT-2 (203.0.113.34)	HUB 2 ISP 2	VPN-OUT-1_dynam... (198.51.100.4)	FTD ftd3	VPN-OUT-2 (203.0.113.35)	VPN-OUT-2_static_... (198.51.100.100)	
FTD ftd2	VPN-OUT-2 (203.0.113.34)		VPN-OUT-1_dynam... (198.51.100.4)	FTD ftd4	VPN-OUT-2 (203.0.113.36)	VPN-OUT-2_static_... (198.51.100.101)	

<< Viewing 1-4 of 4 >>

تاراسمىل نېملىككىمىل نىم دىخاۋىلىكى، زىھى لىكى BGP تامالىغى بىر نىيىۋىكىلى اىزى نىچىتىنىۋى دىخاۋى نىم تىخىمىل عىچىرتىلىكىنىكىمى، لىكىمى لىبىسىلىغى. بىرلىكلىغى عىرلىلى لىلىۋىلى بىسلىنىمىل عىرلىلى.

1 شذحت نمل

<#root>

Spoke1#show bgp summary

```
BGP router identifier 203.0.113.35, local AS number 65500
BGP table version is 4, main routing table version 4
2 network entries using 400 bytes of memory
7 path entries using 560 bytes of memory
1 multipath network entries and 2 multipath paths
3/2 BGP path/bestpath attribute entries using 624 bytes of memory
1 BGP rrinfo entries using 40 bytes of memory
1 BGP AS-PATH entries using 40 bytes of memory
2 BGP community entries using 48 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 1712 total bytes of memory
BGP activity 2/0 prefixes, 7/0 paths, scan interval 60 secs
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
198.51.100.1	4	65500	229	226	4	0	0	04:07:22	1

<<<<<<<<< HUB 1 ISP 1 VTI

198.51.100.2	4	65510 226	230	4	0	0 04:06:36	2
--------------	---	-----------	-----	---	---	------------	---

<<<<<<<<< HUB 2 ISP 1 VTI

198.51.100.3	4	65500	182	183	4	0	0	03:16:45	1
--------------	---	-------	-----	-----	---	---	---	----------	---

<<<<<<<<< HUB 1 ISP 2 VTI

198.51.100.4 4 65510 183 183 4 0 0 03:16:30 2

<<<<<<<< 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 receieved 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

الك نيب لمحلل انزاوم متت رورمالا كرح نا دكوي امام حضوم وه امك هي جوتال لودج رهظي
توصلال بناج في ني طببرل

<#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

رارقلا

ةلوه سب اهذي فنت نكمي ةفل تخم رشن تاهوي راني س حرش وه ةلاقم لا هذه نم ضرغل
دحاو دادعلا جلاع م مادختساب

ةلص تاذا م ولعم

- [تاهج](#): حل اص معد دقع مزلي. TAC ب لاصتالا يجري، ةيفاضا ةدعاسم يلعل لوصحلل
[Cisco نم ةيملاعلا مع دلا لاصتا](#)
- [انه](#) Cisco VPN عم تجم ةرايز اضيأ كنكمي

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م ج ر ت
م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م ج ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م م ج ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م ج ر ت ل ا ع م ل ا ح ل ا و ه
ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م ج ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems
(ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا