

# ASA و FTD مادختساب نمآلا لوصول نيوكت NAT مادختساب صاخلا لوصول نمآلا

## تايوتحمل

[قمدملا](#)

[قيساسالا تابلطتلا](#)

[تابلطتلا](#)

[قمدختسملاتانوكملا](#)

[قيساسا تامولعم](#)

[كباشللطي طيختلالا مسرلا](#)

[نيوكتلا](#)

[\(VPN\) فيرهاطلا صاخلا كباشلا - فيامحلا رادج طيارت رشقم نع نمآلا عافدلاو نمآلا لوصوللا](#)  
[PBR عم هيچوتلا يلغ مئاقلا \(BGP\) فيكيما نيديلا](#)

[FTD قساي س يلغ مئاقلا هيچوتلا](#)

[FTD يلغ BGP نيوكت](#)

[قفنلا علاح نم ققحتلا](#)

[فيكتلل لباقلا نامآلا زاهج يلغ قتابثلا راسملا لادقتسمللا VPN IPsec كباش نيوكت](#)  
[PBR مادختساب \(ASA\)](#)

[نمآلا لوصول يلغ VPN نيوكت](#)

[ASA يلغ VPN نيوكت](#)

[قساي س لا يلغ مئاقلا هيچوتلا](#)

[قحصلا نم ققحتلا](#)

## قمدملا

عمجرت مادختساب نمآلا لوصول كباش قفن ةومجم نيوكت فيفيك دنتسملا اذه حضوي  
كباشلا ناونع

## قيساسالا تابلطتلا

### تابلطتلا

ةيلاتلا عيضاوملاب ةفرعم كيديل نوكت ناب Cisco ي صوت

- Cisco نم فيامحلا رادج ةرادا زكرم
- Cisco نم نمآلا فيامحلا رادج ديدهت دض عافدلا
- Cisco Secure Access

- Cisco نم فيكتلل لبلبال نامأل ةزهجأ
- ةكبشلا ناونع ةمچرت
- ةسايسلا ىلع مئاقلا هيچوتلا
- ةياملال راج ىلع ةمزلال طاقتلا

## ةمدختسملا تانوكمل

ىلإ دنتسملا اذه يف ةدراولا تامولعمل دنتست

- Cisco نم 7.10 ةياملال راج ةرادا زكرم
- Cisco نم 7.10 نامأل ةياملال راج ديدت دض عافدلا جم انرب
- Cisco Secure Access
- Cisco نم 9.22 فيكتلل لبلبال نامأل زاھج
- Cisco تاهجوم

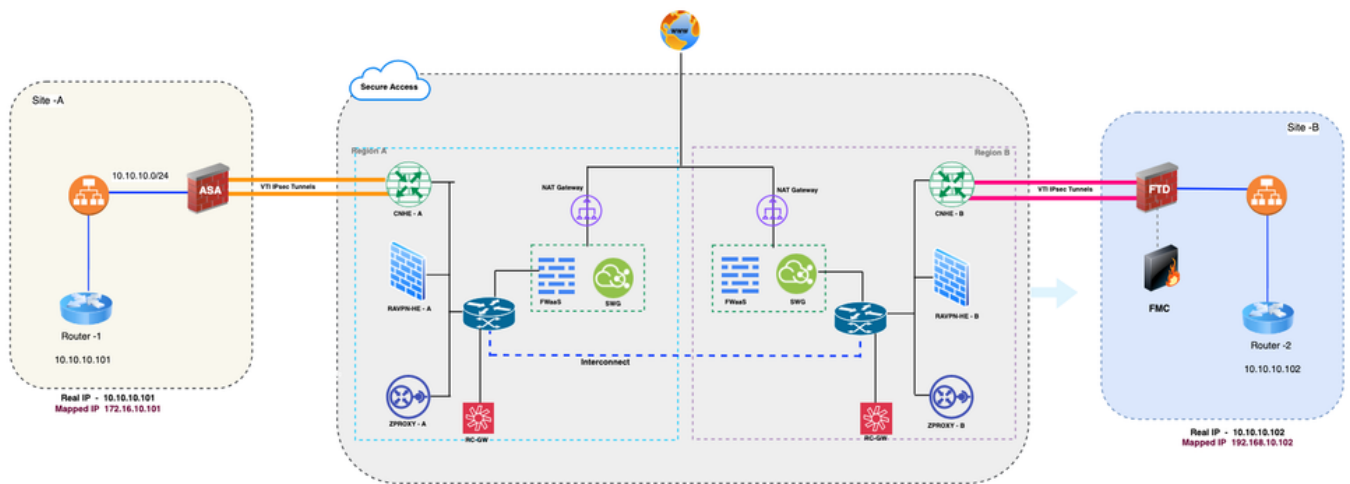
ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نام دنتسملا اذه يف ةدراولا تامولعمل عاشنإ مت تناك اذا. (يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجال عيجم تادب رما يأل لمحتحمل ريثأتلل كمهف نم دكأتف ،ليغشتلا ديقت كتكبش

## ةيساسا تامولعم

كلذ يف امب ةباحسلا ربع ةيلصلال ةنمأل ةمدخل فرط تانام Cisco نم نمأل لوصول رفوي يتلا تاسسؤملل ةبسنلاب (SPA) صاخلا نمأل لوصول او (SIA) تنرتنإلا ىلإ نمأل لوصول لقن نود نيديعبلا نيمدختسملا ىلإ ةصاخلا تاقيبطتلا ىلإ لوصول عيسوتب موقت تاعومجم نمأل لوصول مدختسي ،تانايب زكرم لالخ نم يسكع لكشب تانايبل رورم ةكرح Cisco لثم - ةيلخلال ةكبشلا ةزهجأ ني ب ةرفشم قافنا عاشنإل IPsec (NTGs) ةكبش قفن Cisco Secure Access cloud و Adaptive Security Appliance (ASA) و Firewall Threat Defense (FTD) Points-of-Presence (PoPs).

نيب IKEv2 مادختساب راسملا ىلإ دنتسم IPsec قفن عاشنإ ةيفيكت دنتسملا اذه حضوي لوصول ىلع (NAT) ةكبشلا ناونع ةمچرت حيتي امم ، Cisco Secure Access و ASA و Cisco FTD تانايبل رورم ةكرح هيچوتل ASA و FTD ىلع (PBR) ةسايسلا ىلإ دنتسملا هيچوتل و نمأل قفنلا ىلإ طقف صاخلا لوصولاب ةطبترملا

## ةكبشلا لطيطختلا مسرلا



ةكبشال ايچولوبوط

## نيوكتال

ةصاخال ةكبشال - ةيماحل رادج طبارت رشؤم نع نمآال عافدل او نمآال لوصول  
PBR عم هيچوتال ىل عمةئاقال (BGP) ةيكيمانديدل (VPN) ةيرهاظال

نمآال لوصولال ىل عمةكبشال قفنعومجم نيوكت

1. [نمآال لوصولال](#) تامولعم ةحول ىل لوخدل ليجست
2. ةفاضل+ قوف رقناو ةكبشال قفنعومجم > ةكبشال تالاصتال > لاصلتال ىل لقتنا

ةكبشال قفنعومجم - نمآال لوصولال

### 3. عمال تاداعإل - كبشال قف ن عومج م نيوك ت

- زاهال عونو قطنمل او قف نال عومج م سا نيوك ت
- يلاتال قوف رقا

← Network Tunnel Groups

#### Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

✓ General Settings

2 Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

#### General Settings

Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

Tunnel Group Name

Region

US (Pacific Northwest) ▾

Device Type

FTD ▾

Cancel

Next

كبشال قف نال عومج م عمل تاداعإل - نمل لوصول

### 4. رورمال عرابو قف نال فرعم نيوك ت م ق

- رورمال عرابو قف نال فرعم نيوك ت م ق
- يلاتال قوف رقا

← Network Tunnel Groups

#### Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

✓ General Settings

✓ Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

#### Tunnel ID and Passphrase

Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

Tunnel ID Format

☒ Email ☐ IP Address

Tunnel ID

@<org><hub>.sse.cisco.com

Passphrase

[Show](#)

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

Confirm Passphrase

[Show](#)

Cancel

Back

Next

## هيجوتلا نيوكت 5.

- مقررک زاہجلا نيوكت
- ظفح قوف رقنا

Tunnel ID and Passphrase

Routing

4 Data for Tunnel Setup

Internet Protocol Version Setting for Routing

☐ Enable IPv6 Routing in addition to IPv4

IPv4 is enabled by default.

Routing option

☐ Static routing

Use this option to manually add IP address ranges for this tunnel group.

☒ Dynamic routing

Use this option when you have a BGP peer for your on-premise router.

Device AS Number

65010

Advanced Settings

☐ Multihop BGP

Select this option to enable the ability for BGP peers to establish a connection (hop) when not directly connected.

☐ Override BGP route summarization

By default, advertised routes are summarized using the configured summary subnets in the Route Summarization page. Select this option to override route summarization.

☐ Block default route advertisement

Select to block the advertisement of the default route.

<

Cancel

Back

Save

ةكبشلا قفنلا تاعومجم هيجوت - نمآلا لوصولا

## ةكبشلا قافنة عومجم نيوكت ظفح 6.

## Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

- ✓ General Settings
- ✓ Tunnel ID and Passphrase
- ✓ Routing
- ✓ Data for Tunnel Setup

### Data for Tunnel Setup

Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

**Primary Tunnel ID:** ftdbgpvpn@  
**Primary Data Center IP Address:** 44.228.138.150 2603:5004:13:20e::110:1  
**Secondary Tunnel ID:** ftdbgpvpn@  
**Secondary Data Center IP Address:** 52.35.201.56 2603:5004:13:20c::110:1  
**Passphrase:**

Download CSV

Done

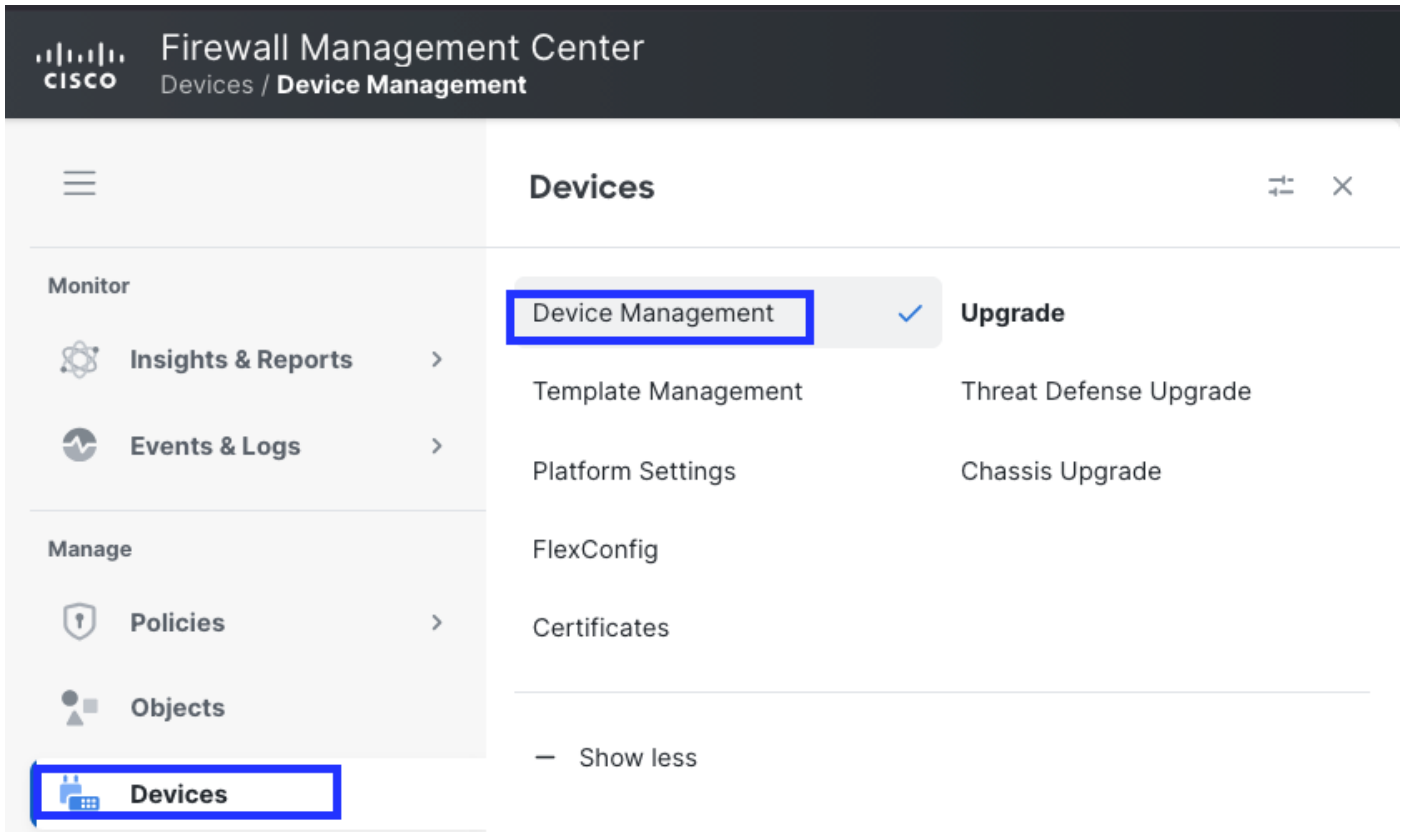
ةكبشلل ق فن تاعومجم - ن مآلا لوصولا

راج دېدهت ن ن مآلا عافدلا ىل ع IPsec ل راسملا ىل ع مئاقلا يكي ماني دل VPN نيوكت  
PBR مادختساب (FTD) ةيامل

1. (FMC) ةيامل ناردي ةراد زكرم ىل لولخدلا ليچست

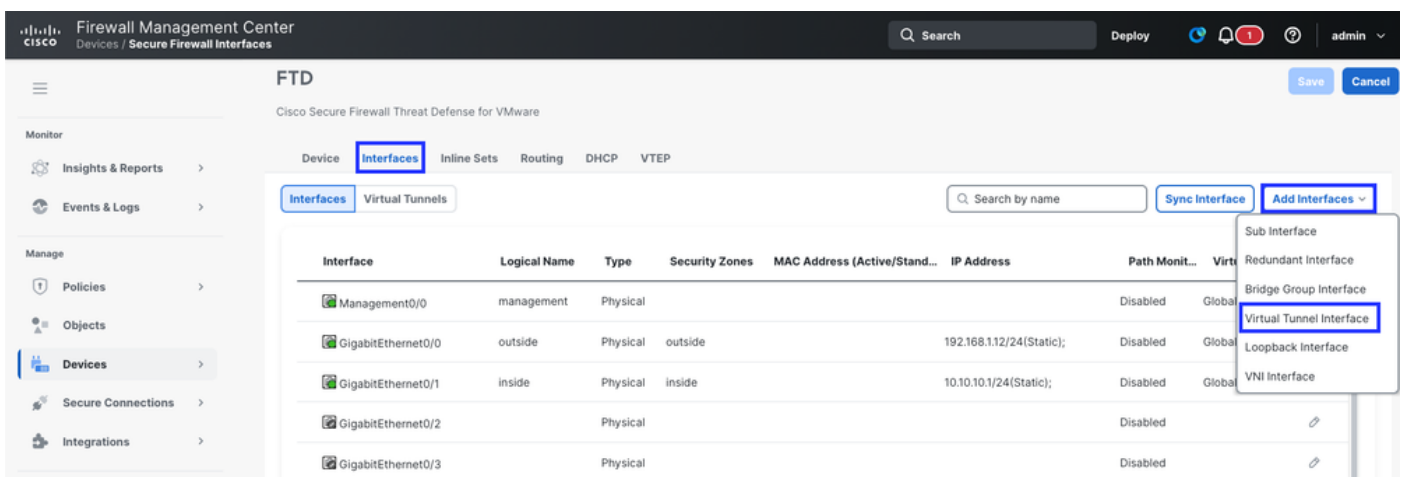
2. [VTI](#) ةيره اظلا ق فنللا ةهجاو نيوكت

• ةزهجالا ةراد > ةزهجالا ىل لولقتنا



تامولعمل حول - نةمآلا ةيامحل راج قراد

- ةهجالول مسق ىلإ حفصتو زاهجال راوجب صاصرلل ملقلا ةنوقيأ ىل ع رقنا
- يرهاظلا قفنلا ةهجاو دحو تاهجالول ةفاضل قوف رقنا



FTD VTI نيوكت - ةيامحل راجل نةمآلا قرادإلا

- VTI نيوكت

# Add Virtual Tunnel Interface



General

Path Monitoring

## Tunnel Type

☒ Static ☐ Dynamic

Name:\*

VTI-1

☒ Enabled

Description:

Virtual Tunnel interface for  
Primary VTI VPN

Security Zone:

vti

Priority:

0

(0 - 65535)

Propagate Security Group Tag: ☒

## Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:\*

1

(0 - 10413)

### Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:\*

1 (0 - 10413)

Tunnel Source:\*

GigabitEthernet0/0 (outside) 192.168.1.12

### IPsec Tunnel Details

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

IPsec Tunnel Mode:\*

☒ IPv4 ☐ IPv6

IP Address:\*

☒ Configure IP 169.254.2.1/30 ☐ Borrow IP (IP unnumbered) Select Interface +

Cancel

OK

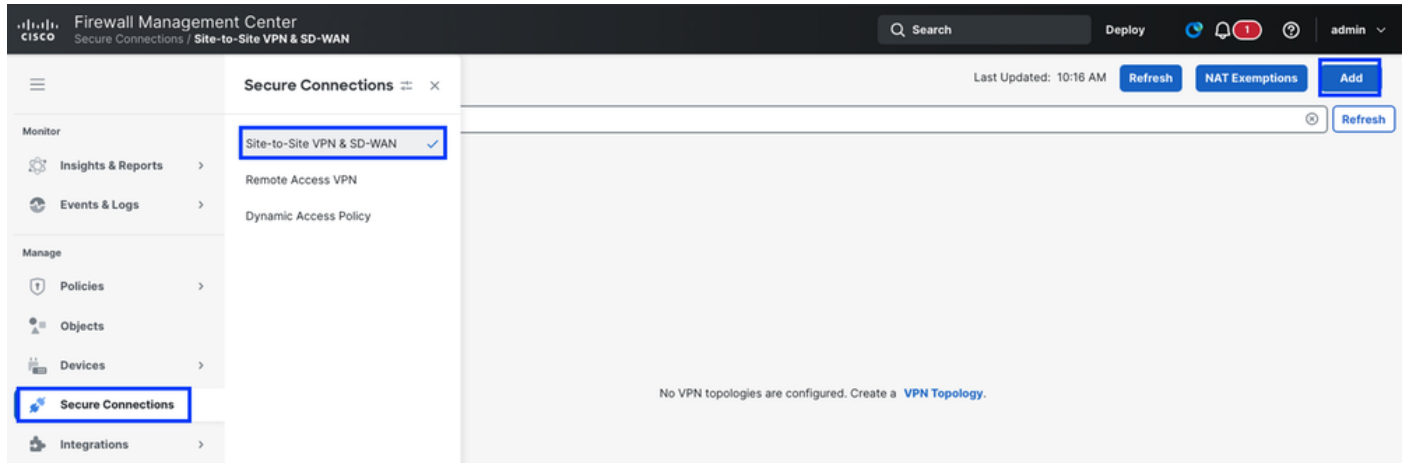
FTD VTI نيوكت - ةيماحل رادجل ةنمآل ةرادإل

- نمآل لوصول عم IPsec ل ةيونال VPN تاكبش ىل ةفاضل اب VTI-2 نيوكت

| FTD                                                                     |              |          |                |                              |                         |               |                |
|-------------------------------------------------------------------------|--------------|----------|----------------|------------------------------|-------------------------|---------------|----------------|
| Cisco Secure Firewall Threat Defense for VMware                         |              |          |                |                              |                         |               |                |
| Device Interfaces Inline Sets Routing DHCP VTEP                         |              |          |                |                              |                         |               |                |
| Interfaces Virtual Tunnels Search by name Sync Interface Add Interfaces |              |          |                |                              |                         |               |                |
| Interface                                                               | Logical Name | Type     | Security Zones | MAC Address (Active/Stand... | IP Address              | Path Monit... | Virtual Router |
| Management0/0                                                           | management   | Physical |                |                              |                         | Disabled      | Global         |
| GigabitEthernet0/0                                                      | outside      | Physical | outside        |                              | 192.168.1.12(Static);   | Disabled      | Global         |
| Tunnel1                                                                 | VTI-1        | VTI      | vti            |                              | 169.254.2.1/30(Static); | Disabled      | Global         |
| Tunnel2                                                                 | VTI-2        | VTI      | vti            |                              | 169.254.2.5/30(Static); | Disabled      | Global         |
| GigabitEthernet0/1                                                      | inside       | Physical | inside         |                              | 10.10.10.1/24(Static);  | Disabled      | Global         |

FTD VTI نيوكت - ةيماحل راجل ةنمآلا ةرادإلا

3. Add قوف رقناو SD-WAN و عقوم ىلا عقوم نم VPN > ةنمآلا تالاصتالا ىلا لقتنا  
VPN ةكبش نيوكتل



FTD ل VPN نيوكت - ةنمآلا ةيماحل راج ةرادإ

• VPN ططخم عاشنإ

## Create VPN Topology

Topology Name \*

SecureAccess-VPN-Primary

VPN Type

**New**

☐ SD-WAN Topology  
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  
**Warning:** SASE Topology cannot be selected because Cisco Umbrella Connection is not configured.  
Prerequisites  
[Refresh](#)

[Cancel](#) [Create](#)

FTD ل VPN نيوكت - ةنمآلا ةيماحل راج ةرادإ

• تافرع ىلع لصحا ، نمآلا لوصولا ىلع ةكبشلا قفن ةعومجم نيوكت نم 6 ةوطخل نم

• ةيوناثلل او ةيساسأل تانايبال زكارمل IP نيوانعو قفنل

• ةياهنل طاقن قوف رقنا

• كب صاخال FTD زاهج ددحو زاهجل قوف رقنا A، ةدقعل تحت

• ةوطخل يف اهؤاشن مت يتل لولأل VTI ةهجاو ددحو ةيرهاظلل قفنل ةهجاو لعل رقنا  
• ةقباسل

• لخدأو، ينورتكللإل ديربل فرعم ددحو نارقأل ل ةيلحمل ةيوهل لاسرا رايل لعل رقنا  
• ةعومجم نيوكت نمض "ةكبشل قفن ةعومجم نيوكت ظفح" نم) يساسأل قفنل فرعم  
(نمأل لوصولل لعل ةكبشل قفن

• تنارتسل ددحو زاهجل قوف رقنا B، ةدقعل تحت

• امسا هطعأو زاهجل مسا لعل رقنا

• لوصولل ةيوناثلل او ةيساسأل IP نيوانعو لخدأو ةياهنل ةطقنل IP نيوانعو قوف رقنا

• نمض "ةكبشل قفن ةعومجم نيوكت ظفح" نم) ةلصافب اهلصف متي يتل نمأل

(نمأل لوصولل لعل ةكبشل قفن ةعومجم نيوكت

• يطايتحالل خسنلل VTI ةفاضل قوف رقنا

• ةوطخل يف اهؤاشن مت يتل ةيوناثلل VTI ةهجاو ددحو ةيرهاظلل قفنل ةهجاو قوف رقنا

• ةقباسل

• لخدأو، ينورتكللإل ديربل فرعم ددحو نارقأل ل ةيلحمل ةيوهل لاسرا رايل لعل رقنا

• ةعومجم نيوكت نمض "ةكبشل قفن ةعومجم نيوكت ظفح" نم) يوناثلل قفنل فرعم

(نمأل لوصولل لعل ةكبشل قفن

• ظفح لعل رقنا

## Edit VPN Topology



Topology Name:\*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map)

☒ Route Based (VTI)

Network Topology:

**Point to Point**

Hub and Spoke

Full Mesh

IKE Version:\*



IKEv1



IKEv2

**Endpoints**

IKE

IPsec

Advanced

### Node A

Device:\*

FTD

Virtual Tunnel Interface:\*

VTI-1 (IP: 169.254.2.1)



*Tunnel Source: outside (IP: 192.168.1.12)* [Edit VTI](#)



Tunnel Source IP is Private



Send Local Identity to Peers

Local Identity Configuration:\*

Email ID

ftdbgpvpn(

### Node B

Device:\*

Extranet

Device Name:\*

Secure Access

Endpoint IP Address:\*

44.228.138.150,52.35.201.56

Cancel

Save

VPN - نمآل FTD ةياهن ةطقن نيوكت

## Edit VPN Topology



Topology Name:\*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

**Point to Point** Hub and Spoke Full Mesh

IKE Version:\*

☐ IKEv1 ☒ IKEv2

### Endpoints

### IKE

### IPsec

### Advanced

Backup VTI:

Remove

Virtual Tunnel Interface:\*

VTI-2 (IP: 169.254.2.5) +

Tunnel Source: outside (IP: 192.168.1.12) [Edit VTI](#)

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration:\*

Email ID

tdbgpvpn@ 22-

Additional Configuration

Route traffic to the VTI : [Routing Policy](#)

Permit VPN traffic : [AC Policy](#)

Cancel

Save

VPN - نم آلا FTD ةياهن ةطقن نيوكت

- [قموعدملا IPsec تاملا عمل](#) اق فو IKEv2 تادادعإ نيوكت
- Umbrella-AES-GCM-256 اهنأ ىلع تاسايسلا ددح
- اق بسم كرتشم يودي حاتفمك ةقداصملا عون ددح

## Edit VPN Topology



Topology Name:\*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map)

☒ Route Based (VTI)

Network Topology:

**Point to Point**

Hub and Spoke

Full Mesh

IKE Version:\*

☐ IKEv1

☒ IKEv2

Endpoints

**IKE**

IPsec

Advanced

### IKEv2 Settings

Policies:\*

Umbrella-AES-GCM-256

Authentication Type:

Pre-shared Manual Key

Key:\*

.....

Confirm Key:\*

.....

☐ Enforce hex-based pre-shared key only

Cancel

Save

VPN - نمآلآ ل FTD ل IKE تادادع

- IPsec تادادع ل نيوكت
- Umbrella-AES-GCM-256 اهنأ لىل ل IKEv2 IPsec تاحرتقم ددح
- 20 ةئيه لىل ل تادحو ةعومجم ديدحت ةئيه لىل ل PFS نيكمت

## Edit VPN Topology



Topology Name:\*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

**Point to Point**

Hub and Spoke

Full Mesh

IKE Version:\*



IKEv1



IKEv2

Endpoints

IKE

**IPsec**

Advanced

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals\*

tunnel\_aes256\_sha

Umbrella-AES-GCM-...



Enable Security Association (SA) Strength Enforcement



Enable Perfect Forward Secrecy

Modulus Group:

20



Cancel

Save

VPN - نم آال FTD ب ةصاال IPsec تاداعا

- ةمدقتم تاداعا
- ظفح قوف رقنا

## Edit VPN Topology



Topology Name:\*

SecureAccess-VPN-Primary

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

☒ Point to Point ☐ Hub and Spoke ☐ Full Mesh

IKE Version:\* ☐ IKEv1 ☒ IKEv2

Endpoints IKE IPsec **Advanced**

IPsec

Tunnel

IKE Keepalive:

Threshold:  Seconds (Range 10 - 3600)

Retry Interval:  Seconds (Range 2 - 10)

Identity Sent to Peers:

Peer Identity Validation:

Cancel

Save

VPN - نم آلا FTD ل ةمدقتم تادادع

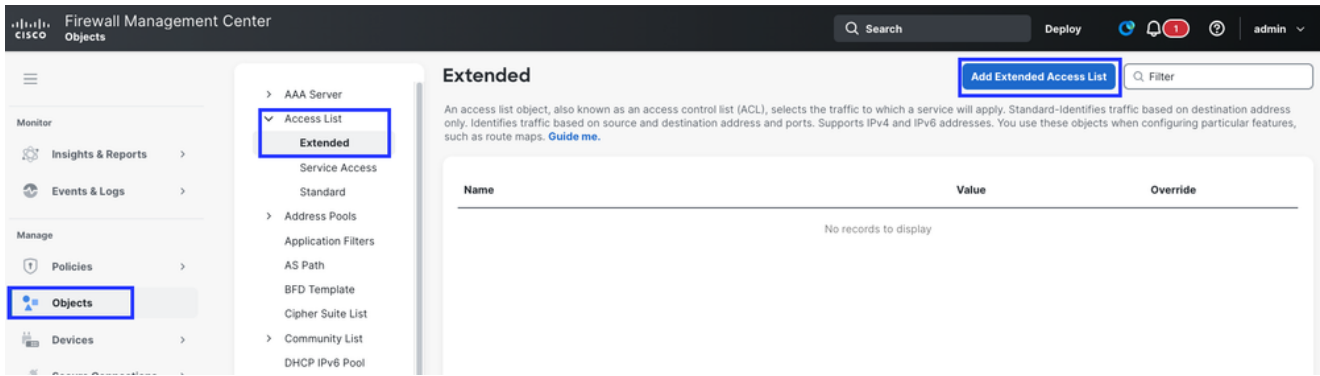
## FTD ةسايس ىلع مئاقلا هيچوتلا

رييغت بعصلال نم .ةهچولل IP ناونع ىلع ءانب مزحلل هيچوت متي ،يديلقتلا هيچوتلا يى  
ىلإ دننسملا هيچوتلا لمعي .ةهچولا ىلع مئاقلا هيچوتلا ماظن يى ةنيعم رورم ةكره هيچوت  
امم ،اهلامكإو هيچوتلا تالوكوتورب اهرفوت يتلا تايلاآل عيسوت ىلع (PBR) ةسايسلا  
هيچوتلا يى مكحتلا نم ديزملا كحنمي

،ةنيعم رورم ةكرهل راسم نييعتب كل حمست اهانامك .IP ةيقيبسا نييعتب PBR كل حمسي  
يذل هيچوتلا ديدحت كنكمي ،PBR عم .ةفلكتلا يلاع طابترا ربع ةيولوالا رورم ةكره لثم  
ذفنم وأ ةهچولا ناونع وأ ردصملا ذفنم لثم ةهچولا ةكبش ريغ ىرخأ ريياعم ىلإ دننسي  
نم ديزم ىلع لوصحلل .تانئاكلا هذه نم ةعومجم وأ تاقيبطتلا وأ لوكوتوربالا وأ ةهچولا  
[ةسايسلا ىلإ دننسملا هيچوتلا](#) ىلإ عجرا ،تامولعمل

### لوصولا ةمئاق نيوكت 1.

- عسوم > لوصولا ةمئاق > تانئاك ىلإ لقتنا
- ةعسوملا لوصولا ةمئاق ةفاضل ىلع رقتنا



ةعسومل لوصول ةمئاق - نمآال FTD لوكوتورب

- لوصول ةمئاق مساعاطعإ
- عارجإل ديدحت
- IPsec قفن إلفرعمل رورمل ةكرح لاسرامتيس - جامس
- IPsec قفن نم رورمل ةكرح زواجت متيس - رطحال
- (يلعأ إلفلقأ) يلسلسلستال مقرلا إلفادانتسا ةدعاقال ةقباطم متتس
- ةفاضل لعل رقنا
- ظفح قوف رقنا

## Add Extended Access List Entry

**Action:** Allow

**Logging:** Default

**Log Level:** Informational

**Log Interval:** 300 Sec.

**Network** **Port** **Application** **Users** **Security Group Tag**

Available Networks +

10.10.10.0

obj\_10.10.10.0

Add to Source

Add to Destination

Source Networks (1)

obj\_10.10.10.0

Destination Networks (0)

any

Cancel Add

ةعسومل لوصول ةمئاق - نمآال FTD لوكوتورب

## New Extended Access List Object



Name

PBR

Entries (1)

Add

| Sequence | Action | Source         | Source Port | Destination | Destination Port | Application | Users | SGT |
|----------|--------|----------------|-------------|-------------|------------------|-------------|-------|-----|
| 1        | Allow  | obj_10.10.10.0 | Any         | Any         | Any              | Any         | Any   |     |

Displaying 1 - 1 of 1 rows < < Page 1 of 1 > >

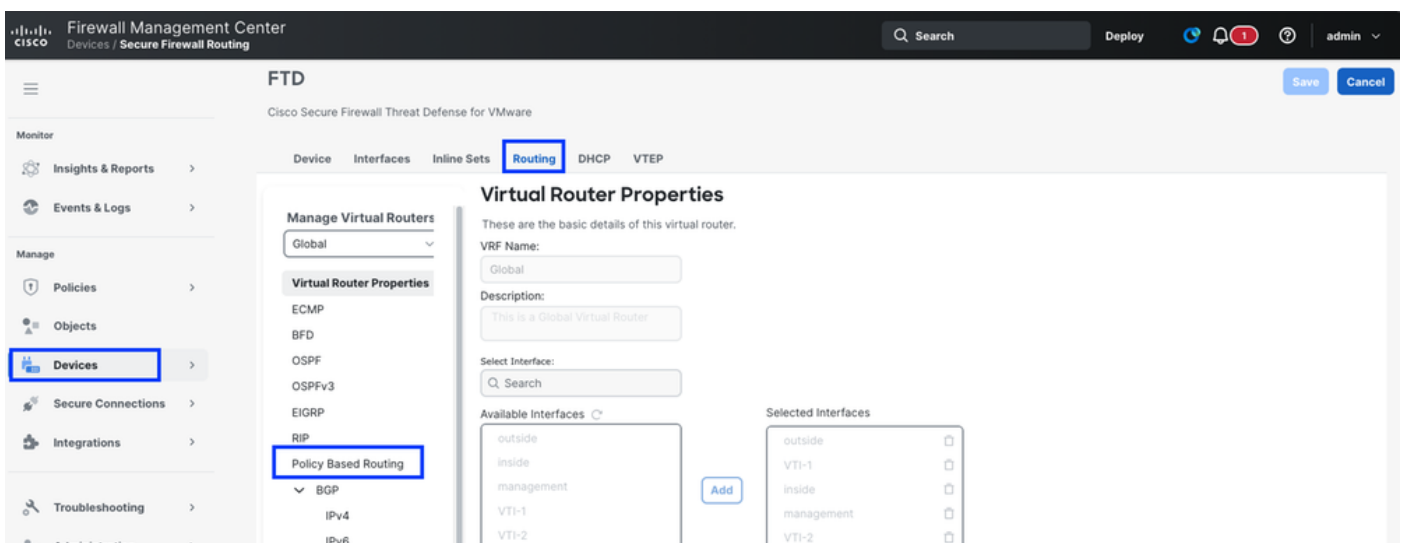
☐ Allow Overrides

Cancel Save

ةسومل لوصول ةمئاق - نمآال FTD لوكوتورب

ةسايسلال إلال دنتسمل هيچوتال نيوكت 2.

• هيچوتال > FTD > ةزهجأال ةرادإ > ةزهجأال إلال لقتنا



ةسايسلال إلال دنتسمل هيچوتال - نمآال FTD جمانرب

- ةفاضإ قوف رقنا
- ةمئاق يف اهفيرعتب انمق يتال ةيعرفال ةكبشلل لوخدلا ةهجاو - لوخدلا ةهجاو دح لوصول

## Add Policy Based Route



A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

### Ingress Interface \*

### Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Add

There are no forward-actions defined yet. Start by [defining the first one](#).

Cancel

Save

ةساي سلاىل دنن سمل هيجوتل - نملآل FTD جم انرب

- جورخلال ههجاووق باطمل ريياعم ديدحت
- ةفاضل عل رقنا
- ةباطمل (ACL) لوصولي ف مكحتل ةمئاق ديدحت
- IP ناوئك لاسرا ددح
- 169.254.2.130 VTIs ههجاوب ةصاخل IP نيوانع - ةيلال ةوطخلل IP ناوئع ةفاضل وه VTI-1 و VTI-2 ل ةيلال ةوطخلل IP ناوئع نوئيس، كلذل 169.254.2.5/30 و 169.254.2.2 و 169.254.2.6 يلاوتل عل ظفح عل رقنا

## Add Forwarding Actions



Match ACL: \*  +

Send To: \*

IPv4 Addresses:

IPv6 Addresses:

Don't Fragment:

☐ Default Interface

### IPv4 settings

### IPv6 settings

Recursive:

Default:

☐ Peer Address

Cancel

Save

ةسائسلا ىلإ دنتسملا هيچوتلا - نمآلا FTD چمانرب

## FTD

You have unsaved changes

Save

Cancel

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

EIGRP

RIP

**Policy Based Routing**

✓ BGP

### Policy Based Routing

Specify ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress interfaces accordingly

Configure Interface Priority

Add

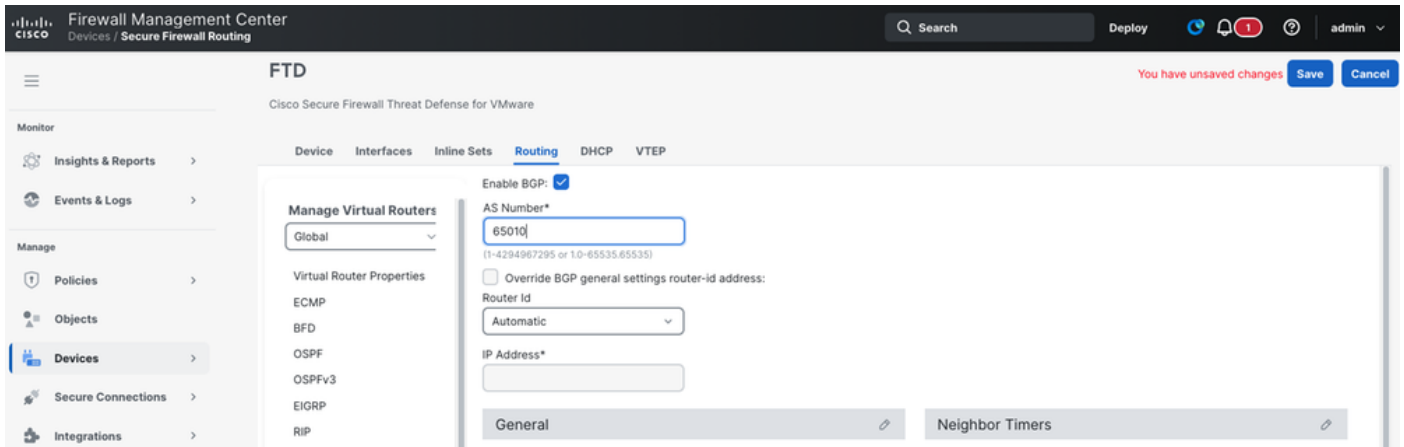
| Ingress Interfaces | Match criteria and forward action         |                                            |
|--------------------|-------------------------------------------|--------------------------------------------|
| inside             | If traffic matches the Access List<br>PBR | Send through<br>169.254.2.2<br>169.254.2.6 |
|                    |                                           |                                            |

ةسائسلا ىلإ دنتسملا هيچوتلا - نمآلا FTD چمانرب

FTD ىل ع BGP نيوكت

BGP ني كمت 1.

- BGP > عمال اتاداعإل > هيجوتل > FTD > عزهألأ قرادإ > عزهألأ ىلإ لقتنا
- (AS يلمل FTD مقر) AS مقر ةفاضل و BGP نيكمت
- ظفح قوف رقنا



BGP هيجوت - نملألأ FTD لوكوتورب

- BGP > IPv4 ىلإ لقتنا

169.254.0.9 و 169.254.0.5 وه نملألأ لوصولل BGP ريطن - BGP راج ةفاضل 2.

## Add Neighbor



IP Address\*

169.254.0.5

Remote AS\*

64512

(1-4294967295 or 1.0-65535.65535)

BFD Fallover

none

Update Source:

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

Description

Filtering Routes

Routes

Timers

**Advanced**

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☐ Allow connections with neighbor that is not directly connected

☒ Limited number of TTL hops to neighbor

TTL Hops

254

(1-254)

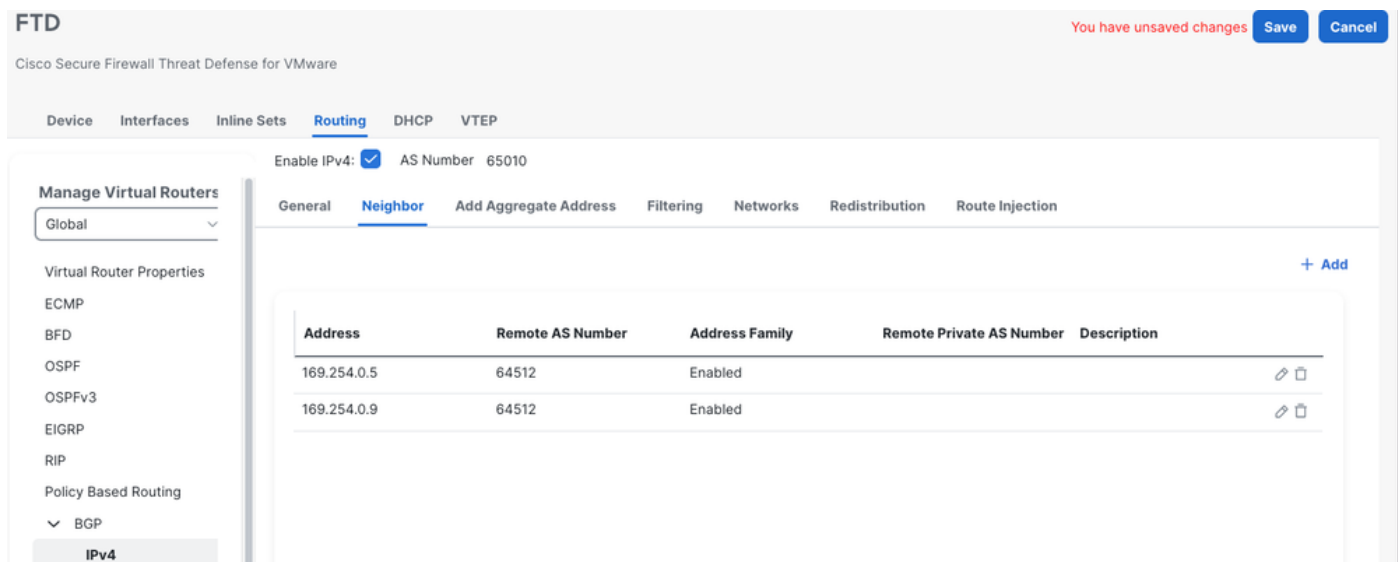
☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

OK

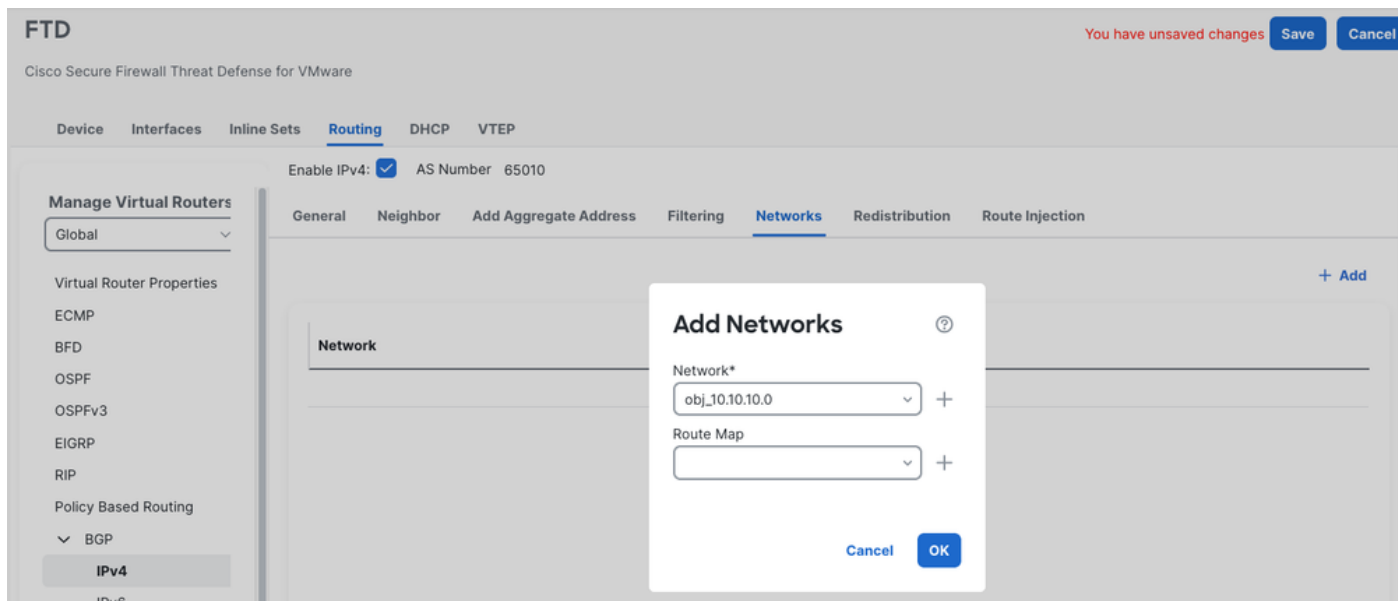
BGP هي جوت - نم آلا FTD لوكوت ورب



BGP هيجوت - نمآلا FTD لوكوتورب

لوصولا نيّمأتل اهنع نالعالإ مزلي يتلا تاكبشلا - تاكبشلا ةفاضإ 3.

• قفاوم قوف رقنا مث



BGP هيجوت - نمآلا FTD لوكوتورب

• اهرشنو تاريغيغتلا ظفح

قفنلا ةلاح نم ققحتلا

## نم آلا لوصولا دنع

**FTD-BGP**

[Edit Configuration](#)

Details for the Auto VPN tunnels added to this group are listed including which tunnel hub it is a member of.

**Summary** [See Logs](#)

Connected

Region: US (Pacific Northwest) | Routing Type: Dynamic Routing (BGP) | Route summary subnets (0)

Device Type: FTD | Device BGP AS: 65010

Last Status Update: Jun 08, 2026 3:53 AM | Peer (Secure Access) BGP AS: 64512

BGP Peer (Secure Access) IP Addresses: 169.254.0.9, 169.254.0.5, 2a04:e4c4:b:c723:b67:0000/120

Multihop BGP Addresses: —

Multihop TTL: —

[View advanced settings](#)

**Primary Tunnel Hub** [See Logs](#)

Hub Up

1 Active Tunnels

Tunnel Group ID: ftdbgvpn@

Data Center: sse-usw-2-1-1

IP Address: 44.228.138.150 2603:5004:13:20e::110:1

**Secondary Tunnel Hub** [See Logs](#)

Hub Up

1 Active Tunnels

Tunnel Group ID: ftdbgvpn@

Data Center: sse-usw-2-1-0

IP Address: 52.35.201.56 2603:5004:13:20c::110:1

IPsec - نم آلا FTD ق فن ةلاح

## FMC ىلع

**Firewall Management Center**

Secure Connections / Site-to-Site VPN & SD-WAN

Search | Deploy | Last Updated: 11:56 PM | Refresh | NAT Exemptions | Add

Monitor

Insights & Reports | Events & Logs

Manage

Policies | Objects | Devices | **Secure Connections** | Integrations

Select...

Topology Name: SecureAccess-VPN | VPN Type: Route Based (VTI) | Network Topology: Point-to-Point | Tunnel Status Distribution: 2 Tunnels | IKEv1: ✓ | IKEv2: ✓

**Node A**

| Device   | VPN Interface | VTI Interface                   |
|----------|---------------|---------------------------------|
| EXTRANET | Extranet      | 44.228.138.150 (44.228.138.150) |
| EXTRANET | Extranet      | 52.35.201.56 (52.35.201.56)     |

**Node B**

| Device | VPN Interface          | VTI Interface       |
|--------|------------------------|---------------------|
| FTD    | outside (192.168.1.12) | VTI-1 (169.254.2.1) |
| FTD    | outside (192.168.1.12) | VTI-2 (169.254.2.5) |

Viewing 1-2 of 2

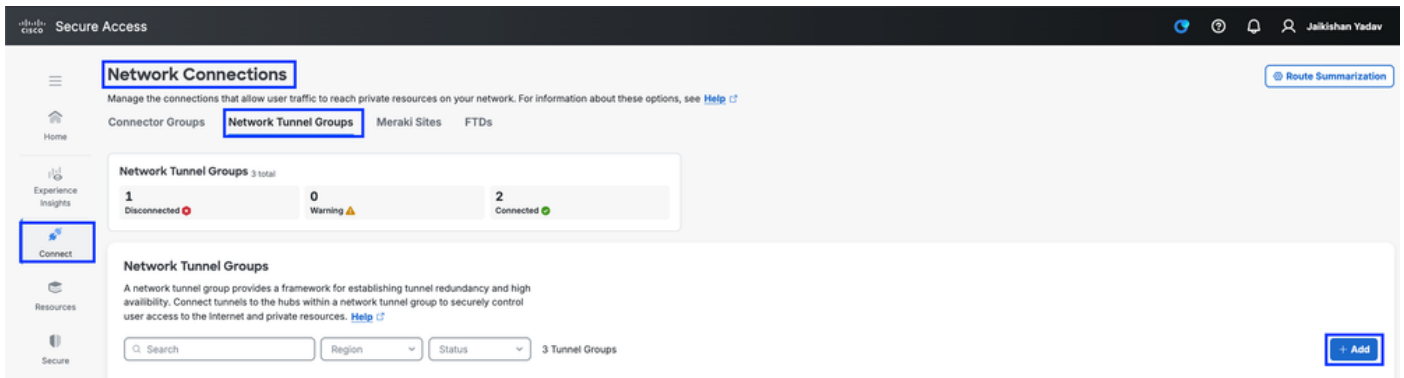
IPsec ق فن ةلاح - نم آلا FMC

نام آلا زاهج ىلع ةتباتلا راسملا ىلإ ةدنتسملا VPN IPsec ةكبش نيوكت  
PBR مادختساب (ASA) فيكتلل لباقلا

## نم آلا لوصولا ىلع VPN نيوكت

- نم آلا لوصولا تامولعم ةحول ىلإ لوخذلا ليچست
- ةفاضلا قوف رقناو ةكبشلا ق فن تاعومجم > ةكبشلا تالاصتا > لاصتالا ىلإ لوقتنا

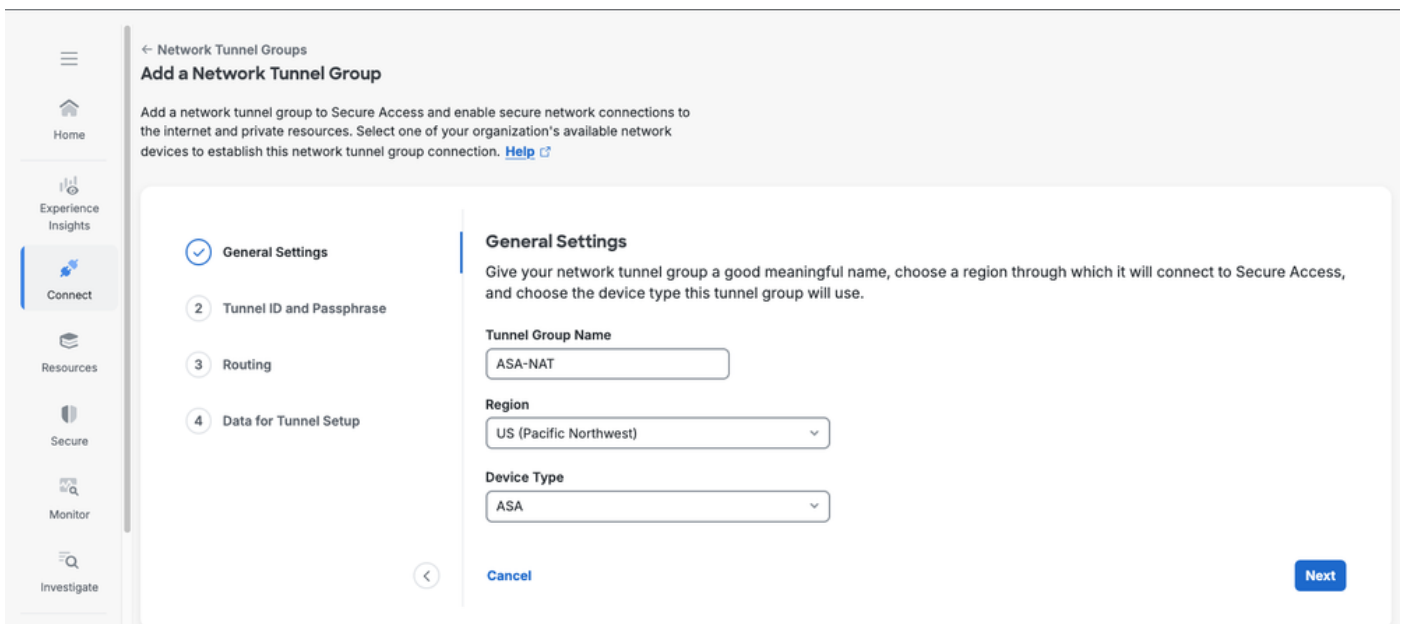
## ةكبشال ق فن ةعومجم نيوكتل



ةكبشال ق فن تاعومجم - ن مآل لوصول

### ةماعال تادادعإل - ةكبشال ق فن ةعومجم نيوكتل 3.

- زاهجال عونو ةقطنمل او ق فنل ةعومجم مسا نيوكتل
- يلاتل قوف رقنا



ةكبشال ق فنل تاعومجم لةماعال تادادعإل - ن مآل لوصول

### رورمل ةرابعو ق فنل فرعم نيوكتب مق 4.

- رورمل ةرابع ق فنل فرعم نيوكتب مق
- يلاتل قوف رقنا

← Network Tunnel Groups

## Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

Routing

Data for Tunnel Setup

**Tunnel ID and Passphrase**

Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

**Tunnel ID Format**

☒ Email ☐ IP Address

**Tunnel ID**

asahomevpn @<org><hub>.sse.cisco.com

**Passphrase**

..... [Show](#)

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

**Confirm Passphrase**

..... [Show](#)

[Cancel](#) [Back](#) [Next](#)

ةكبشلا قف ناعومجم - نمآلا لوصولا

## (NAT) ةكبشلا ناو نع ةمچرت نيكم ت 5.

← Network Tunnel Groups

## Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

Routing

Data for Tunnel Setup

**Routing options and network overlaps**

Configure routing options for this tunnel group.

☒ **Network Address Translation (NAT)**

Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

**Source Mappings**

**Site → Secure Access**

Source NAT

All source IP addresses translate to range:

100.96.0.0/16

☐ Translate to Secure Access NAT subnet

**Secure Access → Site**

Source NAT

Add a destination mapping to enable this rule

**Destination NAT Mappings**

| Name                                                                                                                                 | Direction | Original CIDR | Translated CIDR | ... |
|--------------------------------------------------------------------------------------------------------------------------------------|-----------|---------------|-----------------|-----|
| <p><a href="#">+ Add Mappings</a></p> <p>Configure full bi-directional granular control over destination IP address translation.</p> |           |               |                 |     |

**Internet Protocol Version Setting for Routing**

☐ Enable IPv6 Routing in addition to IPv4

[Cancel](#) [Back](#) [Save](#)

ةكبشلا قف ناعومجم NAT تادادع | Secure Access

## ةهچولل NAT نييغت ةفاضإ 6.

(نمآلا لوصولا إلقوملا ) 2 هچوملا إلقوملا 1 - 1 قفدتلا

## عقووملا یلا نملآلا لوصولا 1 هجوملا یلا 2 هجوملا - 2 قفدتلا

Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

Routing

Data for Tunnel Setup

Routing options and network overlaps

Configure routing options for this tunnel group.

Network Address Translation (NAT)

Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

Source Mappings

Site → Secure Access

All source IP addresses translate to range:

100.96.0.0/16

Translate to Secure Access NAT subnet

Secure Access → Site

Add a destination mapping to enable this rule

Destination NAT Mappings

| Name       | Direction            | Original CIDR   | Translated CIDR   |                                     |
|------------|----------------------|-----------------|-------------------|-------------------------------------|
| ASA-To-FTD | Site → Secure Access | 10.10.10.102/32 | 192.168.10.102/32 | <input checked="" type="checkbox"/> |

Rows per page 30 < 1 >

+ Add Mappings

Internet Protocol Version Setting for Routing

☐ Enable IPv6 Routing in addition to IPv4

ةكبشلل قفنلا تاعومجمل NAT تادادع | Secure Access

يكي تاتاسا نكاس VPN تلکش، اضيأ . انك مم BGP نوکي ال، NAT نيکمت دنع :ريذحت اضيأ ةادأ ةفاح نوبز یلع

مجرتملا IP لاصتا رابتخا امئاد ركذت :حيملت . CIDR ي لصلألا ي ف بهذي IP يقي قح و CIDR مجرتي ي ف IP مجرتي

## Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

General Settings

Tunnel ID and Passphrase

Routing

Data for Tunnel Setup

### Routing options and network overlaps

Configure routing options for this tunnel group.

☒ **Network Address Translation (NAT)**

Select to add NAT mapping configurations that resolve overlapping subnet IP address ranges, including networks with conflicting IP address spaces.

**Source Mappings**

**Site → Secure Access** ⓘ  
Source NAT  
All source IP addresses translate to range:  
  
☐ Translate to Secure Access NAT subnet

**Secure Access → Site** ⓘ  
Source NAT  
All source IP addresses translate to range:  
  
☒ Translate to Secure Access NAT subnet

**Destination NAT Mappings**

| Name         | Direction ⓘ          | Original CIDR   | Translated CIDR     |                                     |
|--------------|----------------------|-----------------|---------------------|-------------------------------------|
| > ASA-To-FTD | Site → Secure Access | 10.10.10.102/32 | → 192.168.10.102/32 | <a href="#">✕</a> <a href="#">+</a> |
| > FTD-To-ASA | Secure Access → Site | 10.10.10.101/32 | → 172.16.10.101/32  | <a href="#">✕</a> <a href="#">+</a> |

Rows per page

[+ Add Mappings](#)

**Internet Protocol Version Setting for Routing**

[Cancel](#) [Back](#) [Save](#)

ةكش ل ق ف ن ل ا ت ا ع و م ج م NAT ت ا د ا د ع | Secure Access

Save قوف ر ق ن ا

ن ا ف ، " ب ع ق و م ل ا " ل ا " ا ع ق و م ل ا " ن م ل ق ت ن ت ي ت ل ا ر و ر م ل ا ة ك ر ح ل ة ب س ن ل ا ب : ح ي م ل ت "Site-> SecureAccess" وه CNHE-1 ر ط ن ل ا ة ه ج و ه ا ج ا ت ا ه ا ج ا ت ا ن و ك ي ، " ا ع ق و م ل ا " ل ا " ب ع ق و م ل ا " ن م ل ق ت ن ت ي ت ل ا ر و ر م ل ا ة ك ر ح ل ة ب س ن ل ا ب "SecureAccess -> Site" وه CNHE-1 ر ط ن ة ه ج و

ASA ل ع VPN ن ي و ك ت

ه ا ج ا ت ا ب ي س ا س ا ل ا IP ل ا ص ت ا ن م ق ق ح ت و ن ي ك م ت ل ا ع ض و ل خ د ا و ، ASA CLI ل ا ل و خ د ل ا ل ج س . 1 ت ن ر ت ن ل ا

ASA# sh ip

م ا ط ن ل ل IP ن ي و ا ن ع

ة ه ج ا و ا ل م س ا ن ا و ن ع ل ة ي ع ر ف ل ا IP ة ك ب ش ع ا ن ق ة ق ي ر ط  
GigabitEthernet0/0 ل ي ل د ج ر ا خ 192.168.1.40 255.255.255.0  
GigabitEthernet0/1 ل ي ل د ل خ ا د 10.10.10.1 255.255.255.0

ة ي ل ا ح ل ا IP ن ي و ا ن ع

ة ه ج ا و ا ل م س ا ن ا و ن ع ل ة ي ع ر ف ل ا IP ة ك ب ش ع ا ن ق ة ق ي ر ط  
GigabitEthernet0/0 ل ي ل د ج ر ا خ 192.168.1.40 255.255.255.0

GigabitEthernet0/1 10.10.10.1 255.255.255.0

ASA# ping 8.8.8

ضاهجإلل بورهال لسلسلست بكتا

:ناتيناث يه ةلهملا ،8.8.8.8 إلى تياب 100 و 5 ةعس ICMP لوكوتورب ءادصأ لاسرا

!!!!

= ةريدتسملا ةلحرلل ىصقألا دحل/طسوتملا/ىندألا دحل ،(5/5) ةئاملاب 100 وه حاجنلا لدعم

ةيناث يلللم 20/28/30

ASA#

ةيجراخلا ةهجاوالا ىلع IKEv2 نيكمتو IKEv2 ةسايس نيوكت .2

10 crypto ikev2 جهن

aes-gcm-256 ريفشت

لماكلل ةميق ال

19 ةعومجملا

86400 رمعلا يئاوث

جراخ crypto ikev2 نكمي

IPSec حرتقم نيوكت .3

crypto ipSec ikev2 ipSec-primary ل IPsec حرتقم

aes-GCM-256 ريفشتلل ESP لوكوتورب

IPsec فيرعت فلم نيوكت .4

ipSec إلى ريفشتلل ىساسألا CSA-profile فيرعت فلم

ىساسأ ipSec ل IPsec IKEv2 حرتقم دادعإ

<primary tunnel-id> set ikev2 ةيلحمل ةيوهلل ينورتكلإلا ديربلا فرعم

.ةمسلا تحت IKEv2 لوكوتورب نيكمتو "ةعومجملا جهن" نيوكتب مق .5

ىلخاد csa-policy-basic جهن

csa-policy-group-policy ل ةىساسأ تامس

vpn-tunnel-protocol ikev2

قفنلا ةعومجم نيوكت .6

ipSec-l2l عون 44.228.138.150 tunnel-group

44.228.138.150 قفنلا ةعومجملا ةماع تامس

group-policy csa-policy-primary  
Tunnel-group 44.228.138.150  
<pre-shared-key> IKEv2  
<اقبس م كرتشم حاتفم> IKEv2  
<اقبس م كرتشم حاتفم> ل اقصم اقبس م كرتشم حاتفم

## 7. (VTI) ةيره اظلال قفنللا ةهجاو نيوكت

- وه كرايخ ناك اذا
- ASA يلع ىرخأ ةهجاو يا عم VTIs ىلى لني عمل IP ناو نع لخداتي ال ابجي
- ةيامل راجل ةيجراخللا ةهجاو قفنللا ردصم
- تانايب ل زكرم ل IP ناو نع قفنللا ع قوم ديدحت

### 1 ةهجاو قفن

#### VTI-1 فييمان

255.255.255.252 169.254.2.1 IP ناو نع

جراخ قفنللا ردصم ةهجاو

44.228.138.150 قفنللا ةهجو

قفنللا عضول IPv4 لوكوتورب

قفنللا ةيامل حل ياساس ال CSA-profile فيرعت فلم

8. و لني عمل IP ناو نع ىلى رورملا ةكرح هيجوت اهب متي ةقيرطب هيجوت ل نيوكتب مق .  
VTI. ىدم نمض ip ب ىلى لجاتحت ةيلاتلا ةلحرم ل VTI. ةهجاو لخداتي عرفلا ةكبش ل

CGNAT رورم ةكرح و RAPN عمجت و تنرتنللا ءاس رال ) 5. 169.254.2.2 0.0.0.0.0 VTI-1 قيرط ل

و

Route VTI-1 172.16.10.101 255.255.255.255 169.254.2.2 5

## ةساي سلا ىلع مئاقلا هيجوت ل

### 1. لوصول ةمئاق

يأ 255.255.255.0 IP 10.10.10.0 PBR Access-list ل ع سومل حامس ل

### 2 - قيرطلا ةطي رخ

10 قيرطلا ةطي رخ ب صاخال RM-CSA حيرصت

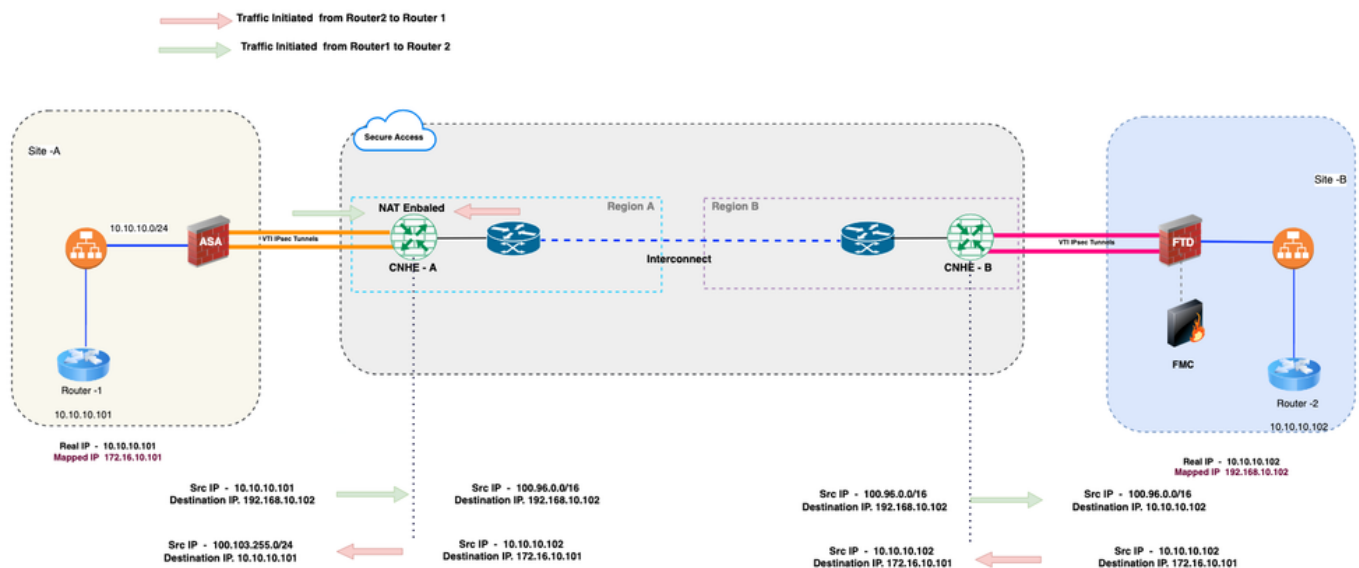
PBR IP ناو نع ةقباطم

169.254.2.2 169.254.2.6 ةيلاتلا ةوطخل set ip

### لوخدلا ةهجاو ىلع راسملا ةطيخ قيبطت 3.

interface GigabitEthernet0/1  
 لخد م سا  
 ينمألا ىوتسملا نم 100  
 ip address 10.10.10.1 255.255.255.0  
 policy-route-map RM-CSA

### ةحصلال نم ققحتلا



### ىلإ لوصول ةيناكم ةلاحو هجوملا ةهجاو GW

```
Router1#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet1   192.168.1.101   YES NVRAM    down        down
GigabitEthernet2   10.10.10.101    YES NVRAM    up          up
GigabitEthernet3   unassigned      YES NVRAM    administratively down down
GigabitEthernet9   unassigned      YES unset  administratively down down
Router1#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

### Ping رابتخا - 1. هجوملا → 2. هجوملا - 1 رابتخا

```

Router1#ping 192.168.10.102
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.102, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 207/211/223 ms
Router1#

```

(يحلح م ASA (FW لى ع م زح ل طاق ت ل

```

ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA#
ASA#
ASA# ter pag 20
ASA# sh cap capin

10 packets captured

  1: 10:56:45.024244      10.10.10.101 > 192.168.10.102 icmp: echo request
  2: 10:56:45.231143      192.168.10.102 > 10.10.10.101 icmp: echo reply
  3: 10:56:45.232470      10.10.10.101 > 192.168.10.102 icmp: echo request
  4: 10:56:45.441856      192.168.10.102 > 10.10.10.101 icmp: echo reply
  5: 10:56:45.443122      10.10.10.101 > 192.168.10.102 icmp: echo request
  6: 10:56:45.652477      192.168.10.102 > 10.10.10.101 icmp: echo reply
  7: 10:56:45.653423      10.10.10.101 > 192.168.10.102 icmp: echo request
  8: 10:56:45.875397      192.168.10.102 > 10.10.10.101 icmp: echo reply
  9: 10:56:45.876450      10.10.10.101 > 192.168.10.102 icmp: echo request
 10: 10:56:46.082301      192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

  1: 10:56:45.024458      10.10.10.101 > 192.168.10.102 icmp: echo request
  2: 10:56:45.230914      192.168.10.102 > 10.10.10.101 icmp: echo reply
  3: 10:56:45.232516      10.10.10.101 > 192.168.10.102 icmp: echo request
  4: 10:56:45.441795      192.168.10.102 > 10.10.10.101 icmp: echo reply
  5: 10:56:45.443153      10.10.10.101 > 192.168.10.102 icmp: echo request
  6: 10:56:45.652432      192.168.10.102 > 10.10.10.101 icmp: echo reply
  7: 10:56:45.653454      10.10.10.101 > 192.168.10.102 icmp: echo request
  8: 10:56:45.875351      192.168.10.102 > 10.10.10.101 icmp: echo reply
  9: 10:56:45.876480      10.10.10.101 > 192.168.10.102 icmp: echo request
 10: 10:56:46.082240      192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown

```

(دع ب نع FW) FTD لى ع م زح ل طاق ت ل

```
ftd# sh cap
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd# sh cap vti
```

10 packets captured

```
1: 16:06:41.122292      100.96.2.0 > 10.10.10.102 icmp: echo request
2: 16:06:41.124856      10.10.10.102 > 100.96.2.0 icmp: echo reply
3: 16:06:41.329557      100.96.2.0 > 10.10.10.102 icmp: echo request
4: 16:06:41.330442      10.10.10.102 > 100.96.2.0 icmp: echo reply
5: 16:06:41.546327      100.96.2.0 > 10.10.10.102 icmp: echo request
6: 16:06:41.547106      10.10.10.102 > 100.96.2.0 icmp: echo reply
7: 16:06:41.752036      100.96.2.0 > 10.10.10.102 icmp: echo request
8: 16:06:41.752814      10.10.10.102 > 100.96.2.0 icmp: echo reply
9: 16:06:41.967891      100.96.2.0 > 10.10.10.102 icmp: echo request
10: 16:06:41.968501     10.10.10.102 > 100.96.2.0 icmp: echo reply
```

10 packets shown

```
ftd# sh cap capin
```

10 packets captured

```
1: 16:06:41.123299      100.96.2.0 > 10.10.10.102 icmp: echo request
2: 16:06:41.124825      10.10.10.102 > 100.96.2.0 icmp: echo reply
3: 16:06:41.330000      100.96.2.0 > 10.10.10.102 icmp: echo request
4: 16:06:41.330396      10.10.10.102 > 100.96.2.0 icmp: echo reply
5: 16:06:41.546800      100.96.2.0 > 10.10.10.102 icmp: echo request
6: 16:06:41.547090      10.10.10.102 > 100.96.2.0 icmp: echo reply
7: 16:06:41.752448      100.96.2.0 > 10.10.10.102 icmp: echo request
8: 16:06:41.752783      10.10.10.102 > 100.96.2.0 icmp: echo reply
9: 16:06:41.968242      100.96.2.0 > 10.10.10.102 icmp: echo request
10: 16:06:41.968486     10.10.10.102 > 100.96.2.0 icmp: echo reply
```

10 packets shown

1 هجوم الى —> 2 هجوم الى لاصتا رابتخا - 2. رابتخا الى

```
Router2#sh ip int br
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet1   unassigned      YES NVRAM    administratively down down
GigabitEthernet2   10.10.10.102    YES NVRAM    up          up
GigabitEthernet3   unassigned      YES NVRAM    administratively down down
Router2#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

(يحمل FW) FTD ةمزع طاقا الى

```

ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decryptd [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd#
ftd#
ftd#
ftd# sh cap vti

10 packets captured

  1: 16:11:45.622450      10.10.10.102 > 172.16.10.101 icmp: echo request
  2: 16:11:45.823825      172.16.10.101 > 10.10.10.102 icmp: echo reply
  3: 16:11:45.825762      10.10.10.102 > 172.16.10.101 icmp: echo request
  4: 16:11:46.045667      172.16.10.101 > 10.10.10.102 icmp: echo reply
  5: 16:11:46.046857      10.10.10.102 > 172.16.10.101 icmp: echo request
  6: 16:11:46.252321      172.16.10.101 > 10.10.10.102 icmp: echo reply
  7: 16:11:46.253572      10.10.10.102 > 172.16.10.101 icmp: echo request
  8: 16:11:46.453803      172.16.10.101 > 10.10.10.102 icmp: echo reply
  9: 16:11:46.454764      10.10.10.102 > 172.16.10.101 icmp: echo request
 10: 16:11:46.664119      172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

  1: 16:11:45.622083      10.10.10.102 > 172.16.10.101 icmp: echo request
  2: 16:11:45.823886      172.16.10.101 > 10.10.10.102 icmp: echo reply
  3: 16:11:45.825442      10.10.10.102 > 172.16.10.101 icmp: echo request
  4: 16:11:46.045697      172.16.10.101 > 10.10.10.102 icmp: echo reply
  5: 16:11:46.046582      10.10.10.102 > 172.16.10.101 icmp: echo request
  6: 16:11:46.252352      172.16.10.101 > 10.10.10.102 icmp: echo reply
  7: 16:11:46.253313      10.10.10.102 > 172.16.10.101 icmp: echo request
  8: 16:11:46.453849      172.16.10.101 > 10.10.10.102 icmp: echo reply
  9: 16:11:46.454596      10.10.10.102 > 172.16.10.101 icmp: echo request
 10: 16:11:46.664150      172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown

```

(ديعب FW) ASA ةمزنح طاقتلا

```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA# sh cap capin
```

10 packets captured

|                     |                                |                    |
|---------------------|--------------------------------|--------------------|
| 1: 11:08:30.288391  | 100.103.255.195 > 10.10.10.101 | icmp: echo request |
| 2: 11:08:30.289123  | 10.10.10.101 > 100.103.255.195 | icmp: echo reply   |
| 3: 11:08:30.504566  | 100.103.255.195 > 10.10.10.101 | icmp: echo request |
| 4: 11:08:30.504963  | 10.10.10.101 > 100.103.255.195 | icmp: echo reply   |
| 5: 11:08:30.710992  | 100.103.255.195 > 10.10.10.101 | icmp: echo request |
| 6: 11:08:30.711404  | 10.10.10.101 > 100.103.255.195 | icmp: echo reply   |
| 7: 11:08:30.917112  | 100.103.255.195 > 10.10.10.101 | icmp: echo request |
| 8: 11:08:30.917402  | 10.10.10.101 > 100.103.255.195 | icmp: echo reply   |
| 9: 11:08:31.128243  | 100.103.255.195 > 10.10.10.101 | icmp: echo request |
| 10: 11:08:31.128640 | 10.10.10.101 > 100.103.255.195 | icmp: echo reply   |

10 packets shown

ASA# sh cap tunnel

10 packets captured

|                     |                                |                    |
|---------------------|--------------------------------|--------------------|
| 1: 11:08:30.287964  | 100.103.255.195 > 10.10.10.101 | icmp: echo request |
| 2: 11:08:30.289322  | 10.10.10.101 > 100.103.255.195 | icmp: echo reply   |
| 3: 11:08:30.504505  | 100.103.255.195 > 10.10.10.101 | icmp: echo request |
| 4: 11:08:30.505009  | 10.10.10.101 > 100.103.255.195 | icmp: echo reply   |
| 5: 11:08:30.710961  | 100.103.255.195 > 10.10.10.101 | icmp: echo request |
| 6: 11:08:30.711434  | 10.10.10.101 > 100.103.255.195 | icmp: echo reply   |
| 7: 11:08:30.917066  | 100.103.255.195 > 10.10.10.101 | icmp: echo request |
| 8: 11:08:30.917417  | 10.10.10.101 > 100.103.255.195 | icmp: echo reply   |
| 9: 11:08:31.128197  | 100.103.255.195 > 10.10.10.101 | icmp: echo request |
| 10: 11:08:31.128685 | 10.10.10.101 > 100.103.255.195 | icmp: echo reply   |

10 packets shown

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 چ 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 چ ر ت ل ض ف ا ن ا ة ظ 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 چ 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 چ 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 چ 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