

# هترادا متت FTD ىلع چودزم ISP VTI نيوكت FMC ةطساوب

## تايوت حمل

[ةمدقم](#)

[ةيساس الابلطت مل](#)

[ةيساس الابلطت مل](#)

[ةمدخت سمل تانوك مل](#)

[FMC ىلع تان نيوكت مل](#)

[ططخ مل نيوكت](#)

[ةياهن لة طقن نيوكت](#)

[IKE نيوكت](#)

[IPsec نيوكت](#)

[هيچوت مل نيوكت](#)

## ةمدقم

زاهج ىلع ىره اظلا ق فنل تاهجاو مادختساب چودزم ال ISP دادع رشن دنت سمل اذه حضوي  
FMC ةطساوب هترادا متت FTDdevice.

## ةيساس الابلطت مل

### ةيساس الابلطت مل

- عقوم ىل عقوم نم (VPN) ةيره اظلا ةصاخلا تاكبش لل يساسا مهف داچي دي فمل نمو.  
ةيسسيئرلا ميهافملا كلذ ي ف امب، VTI دادع ةيلمع باعيتسا ي ف ةيفللخال هذه دعاست  
ةينعمل تان نيوكت ل او.
- نمضتيو Cisco FirePOWER ةصنم ىلع VTIs ةراداو نيوكت تايساسا مهف يرورضال نم  
FMC ةهجاو لالخنم اهيف مكحتللا ةيفيكيو FTD لخاد VTIs لمع ةيفيكي ةفرعم كلذ.

### ةمدخت سمل تانوك مل

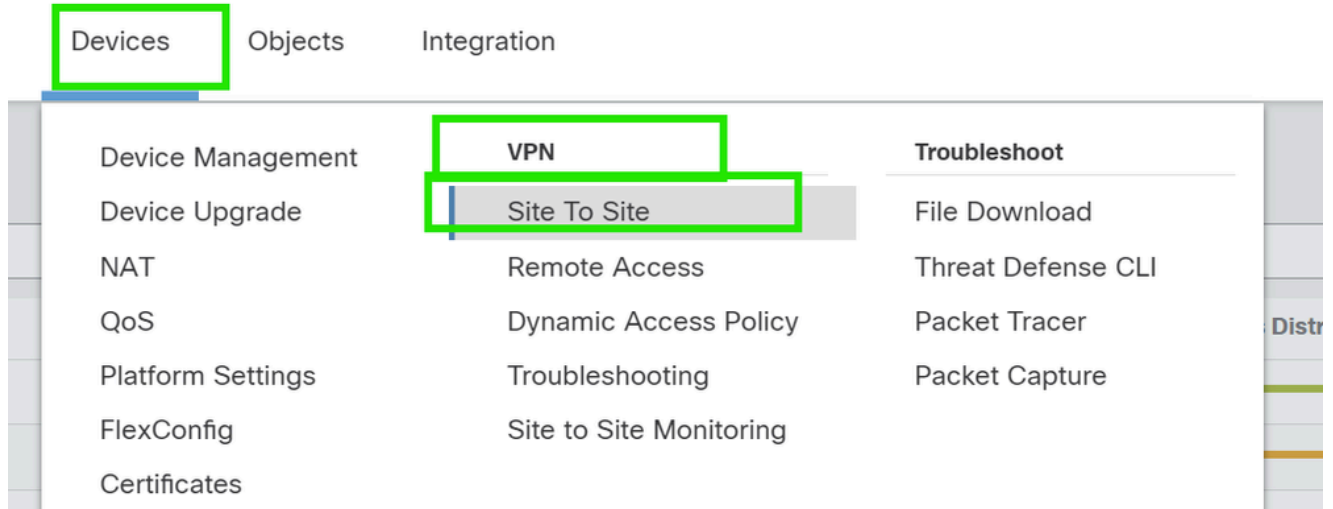
- 7.0.0 رادصلال VMware ل Cisco نم FirePOWER (FTD) ديدهت دض عافدل اجمانرب
- 7.2.4 رادصلال Firepower (FMC): ةرادا زكرم (169 ةينب)

ةصاخ ةيلمع مة ئيب ي ف ةدوچوملا ةزهجال نم دنت سمل اذه ي ف ةدراول تامولعمل اءاشن ا مت  
ت ناك اذا. (يضا رتفا) حوسمم نيوكت ب دنت سمل اذه ي ف ةمدخت سمل ةزهجال ا عيمج ت ادب  
رما ي ال لمحت حمل ريثا ل ل كمهف نم دكأت ف، ليغش تال دي ق ك تكبش

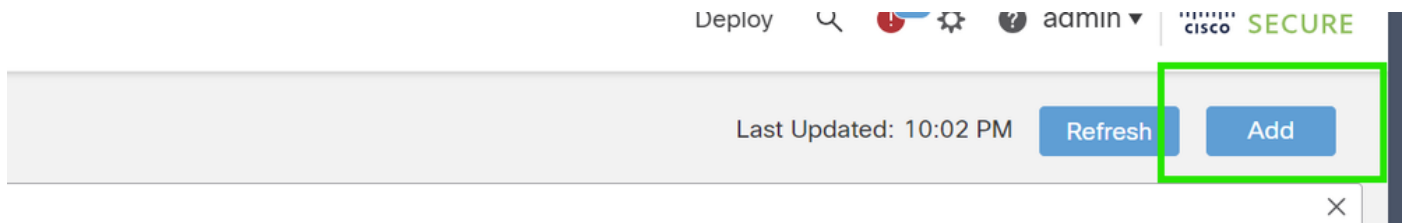
## FMC ىلع تان نيوكت مل

## ططخ ملام ني وكت

1. عقوم لىل عقوم >VPN > ةزهجال لىل لقتنا 1.



2. VPN ططخم ةفاضل ةفاضل قوف رقتنا 2.



3. (ةلجال هذه يف IKEv2) IKE رادصل ددو، ةطقن لىل ةطقن نم و VTI رتخاو، ططخم لىل امسا حنما 3.



## ةياهنلا ةطقن ني وكت

1. هيلع قفنلا ني وكت بجي يذلا زاهجال رتخا 1.

ديعبلا ريظنلا لىل صافات ةفاضل

نم ةهجال ديدحت و "+" زمرلا قوف رقتنلاب ةديدج يرهاظ بلالاق ةهجال ةفاضل اما كنكمي ةدوجوملا ةمئاللا

**Node A**

Device:\*  
New\_FTD

Virtual Tunnel Interface:\*  
[ ] +

Tunnel Source IP is Private [Edit VTI](#)

Send Local Identity to Peers

[+ Add Backup VTI \(optional\)](#)

Connection Type:\*  
Bidirectional

**Node B**

Device:\*  
Extranet

Device Name\*:  
VTI-Peer

Endpoint IP Address\*:  
10.10.10.2

Cancel

Save

"ok" ةق طقو، وه تنك م، ححص م لم عمل تفضاً كلذ دع ب، نراق VTI دي دج تنأ قلخي نإ  
ي ساسأل VTI وه اذه حب صي: ةظ حال م

## Add Virtual Tunnel Interface



### General

Name:\*

VTI-1

Enabled

Description:

This is the primary VTI tunnel.  
This VTI goes through ISP 1.

Security Zone:

OUT

Priority:

0

(0 - 65535)

### Virtual Tunnel Interface Details

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

Tunnel ID:\*

1

(0 - 10413)

Tunnel Source:\*

GigabitEthernet0/0 (outside1)

10.106.52.104

### IPsec Tunnel Details

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

IPsec Tunnel Mode:\*

IPv4  IPv6

192.168.10.1/30



Cancel

OK

3. يوناث VIT ةفاضال يطايتحال خسنلل VIT ةفاضال. "+" قوف رقونا.

Device:\*

10.106.50.55 ▼

Virtual Tunnel Interface:\*

VTI-1 (IP: 192.168.10.1) ▼ +

Tunnel Source: outside1 (IP: 10.106.52.104) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

+ Add Backup VTI (optional)

Connection Type:\*

Bidirectional ▼

Additional Configuration ⓘ

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

Permit VPN traffic : [AC Policy](#)

4. (لعفلاب اهنيوكت متي مل اذا) ةيوناثلا VTI ل ةملعم ةفاضل "+" قوف رقنا.



## Add Virtual Tunnel Interface



### General

Name:

VTI-2

Enabled

Description:

This is the secondary VTI tunnel..  
VTI goes through ISP 2.

Security Zone:

OUT

Priority:

0

(0 - 65535)

### Virtual Tunnel Interface Details

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

Tunnel ID:\*

2

(0 - 10413)

Tunnel Source:\*

GigabitEthernet0/1 (outside2)

10.106.53.10

### IPsec Tunnel Details

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

IPsec Tunnel Mode:\*

IPv4  IPv6

192.168.20.1/30



Cancel

OK

## IKE نيوكت


قوف رقنا اق بسم ةددم ةسايس مادختسا رايتخا كنكمي. IKE بيوبتلا ةمالع ىلإ لقتنا 1. ديحت وأ ةديج ةسايس عاشنإل "جهنلا" بيوبتلا ةمالع راوجب دوجوملا "صاصرلا ملقلا" رزلا كتابلطتم ىلع ءانب ةرفوتم ىرخأ ةسايس.

Endpoints **IKE** IPsec Advanced

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:\* 24 Characters (Range 1-127)

IKEv2 Settings



Policies:\* AES-GCM-NULL-SHA-LATEST 

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:\* 24 Characters (Range 1-127)

Cancel Save


### IKEv2 Policy ?

Available IKEv2 Policy  

- AES-GCM-NULL-SHA
- AES-GCM-NULL-SHA-LAT...
- AES-SHA-SHA
- AES-SHA-SHA-LATEST
- Arko\_Test\_IKEv2
- DES-SHA-SHA

Add

Selected IKEv2 Policy

AES-GCM-NULL-SHA-LATEST 

Cancel OK

حاجات فم لاري فوتب مقف، اق بس م كرت شم يودي حاجات فم مادخت سا مت اذا. عق داصم ل عون دح 2.  
حاجات فم ل دي كأت و حاجات فم لاي ع برم ي ف



## IKEv2 Settings

Policies:\* AES-GCM-NULL-SHA-LATEST

Authentication Type: Pre-shared Manual Key

Key:\* .....

Confirm Key:\* .....

 Enforce hex-based pre-shared key only

Cancel

Save

## IPsec نيوكت

رقنلا قيرط نع اق بس م دحم ضرع مادختسا رايخا كنكمي IPsec بيوبتلا عمال عىل لقتنا رخا ضرع ديحت وا ديچ ضرع عاشنلا ضرعلا بيوبت راجب دوجوملا صاصللا ملقلا رز قوف كتابلطتم لىع انب رفوتم.

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals\*

tunnel\_aes256\_sha

AES-GCM

 Enable Security Association (SA) Strength Enforcement Enable Reverse Route Injection Enable Perfect Forward Secrecy

## هيچوتلا نيوكت

1. (FTD) زاهجلا ريرحتل صاصللا ملقلا زمز قوف رقنلا و زهجالا ارادا > زاهجلا لىل لقتنا.

Firewall Management Center  
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

View By: Group

All (4) Error (2) Warning (0) Offline (2) Normal (0) Deployment (0)

Collapse All

Name	Model	Version	Platform	OS	Deployment
Ungrouped (4)					
...	FTDv for VMware	7.0.0	N/A	Base, AnyConnect Plus (1 more...)	new_pol

Device Management

- Device Upgrade
- NAT
- QoS
- Platform Settings
- FlexConfig
- Certificates
- VPN
- Site To Site
- Remote Access
- Dynamic Access Policy
- Troubleshooting
- Site to Site Monitoring
- Troubleshoot
- File Download
- Threat Defense CLI
- Packet Tracer
- Packet Capture

Deployment History

Search Device Add

Access Control Policy Auto RollBack

2. يساسأل VTI إلى راسم ةفاضإل "+" رزلا قوف رقناو تباثل راسملا > هيچوتلا إلى لقتنا 2. يوناثل او

ربع رورم لل كب ةصاخلا رورملا ةكرجل ةبسانملا هيچوتلا ةقيرط نيوكت كنكمي: ةظحالم ةتباثل تاراسملا مادختسا مت، ةلاجل هذه يف. قفلنلا ةهجاو

The screenshot shows the Cisco IOS configuration interface. The 'Routing' tab is selected. On the left, the 'Manage Virtual Routers' menu is open, with 'Static Route' highlighted. In the main interface, the '+ Add Route' button is highlighted. The table below shows the configuration of static routes.

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
IPv6 Routes						

3. راسم لل (2 ةلاجل هذه يف) إلى ع AD ةميقي نييعتب مقو ةيحمملا كتكبشل ني راسم فضا 3. يوناثل او

VTI-2 ةهجاو يوناثل راسملا مدختسي، و VTI-1 ةهجاو لوال راسملا مدختسي

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric
IPv4 Routes					
protected-network	VTI-1	Global	VTI-1-Gateway	false	1
protected-network	VTI-2	Global	VTI-2-Gateway	false	2

## ةحصلنم ققحتلا

1. عقوملا إلى عقوملا ةبقارم > VPN > ةزهجال إلى لقتنا 1.

Devices

Objects

Integration

Device Management

Device Upgrade

NAT

QoS

Platform Settings

FlexConfig

Certificates

VPN

Site To Site

Remote Access

Dynamic Access Policy

Troubleshooting

Site to Site Monitoring

Troubleshoot

File Download

Threat Defense CLI

Packet Tracer

Packet Capture

قفلن لة لوج لوصاف تال نم ديزم نم ققحت لل نع ل قوف رقنا .



View full information

Dual-ISP-VTI

Active

2024-06-11 06:55:26

Dual-ISP-VTI

Active

2024-06-12 14:27:22

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء ان ا عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و  
امك ة ق ي قد ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ حال 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 مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
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 دن تسمل ا