

راسم ال ىلإ ةدنتسم ال VPN ةكبش نيوكت رادم ال FTD ىلع تباث ال راسم ال مادختساب FDM ةطساوب

تايوتحم ال

[ةمدقم ال](#)

[ةيساس ال ابلطت ال](#)

[تابلطت ال](#)

[ةمدختسم ال تانوكم ال](#)

[ةيساس ا تامولعم](#)

[FDM ىلع نيوكت ال تاوطخ](#)

[ةحصل ال نم ققحت ال](#)

[ةلص تاذا تامولعم](#)

ةمدقم ال

عقوم ال VPN قفن ىلإ راسم ىلإ دنتسم تباث عقوم نيوكت ةيفي ك دنتسم ال اذه حضوي
FDM ةطساوب هترادإ متت FTD ىلع

ةيساس ال ابلطت ال

تابلطت ال

ةيلات ال عيضاوم ال اب ةفرعم كي دل نوكت نأب Cisco ىصوت:

- (VPN) ةيره اظلا ةصاخ ال ةكبش ال قفن لمع ةيفي كل يساسأ مهف
- FirePOWER (FDM) ةزهجأ ري دم ربع لقننت ال اب ةقبسم ةفرعم

ةمدختسم ال تانوكم ال

ةيلات ال جمارب ال تارادصا ىلإ دنتسم ال اذه يف ةدراول تامولعم ال دنتست

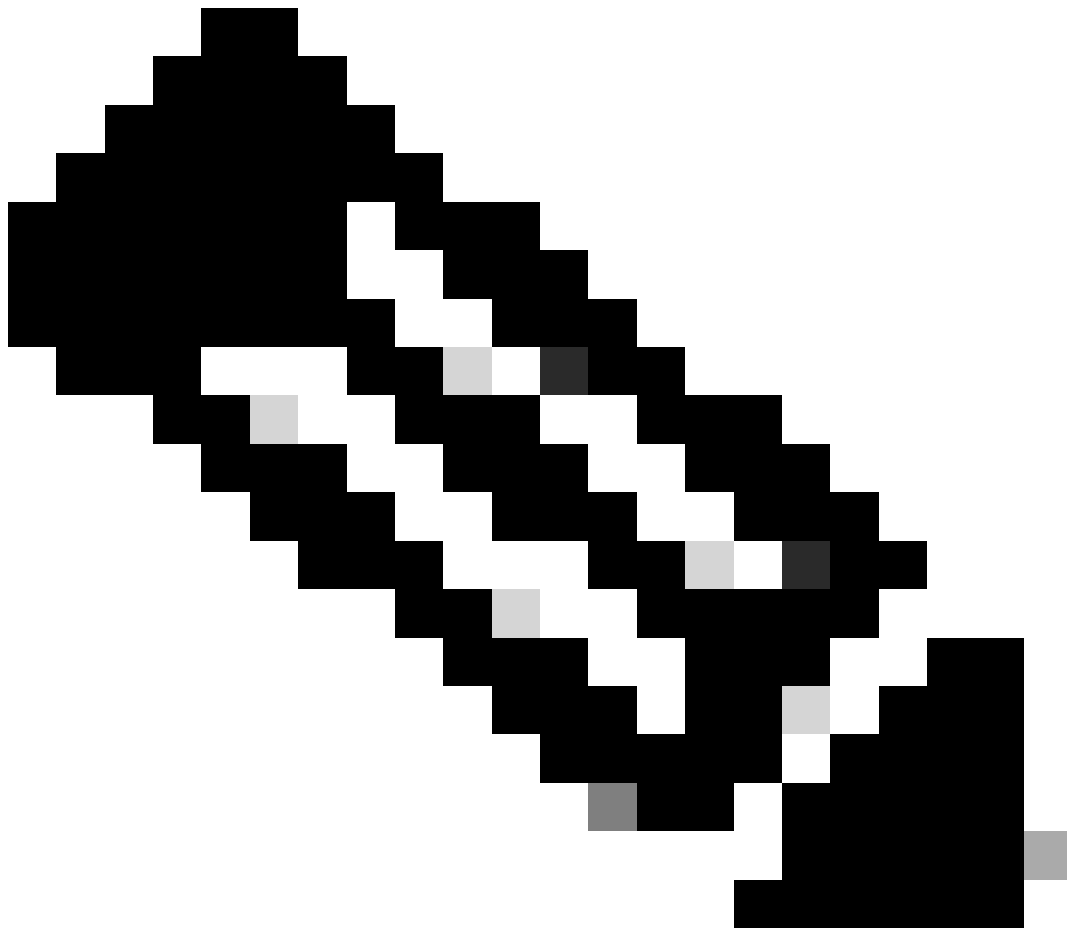
- لبق نم رادم ال 7.0 رادصا ال Cisco نم FirePOWER (FTD) ديدهت دص عافدل جمارب
FirePOWER Device Manager (FDM).

ةصاخ ةيلمعم ةئي ب يف ةدوجوم ال ةزهجأ ال نم دنتسم ال اذه يف ةدراول تامولعم ال عاشنإ مت
تناك اذا. (يضا رتفا) حوسمم نيوكت ب دنتسم ال اذه يف ةمدختسم ال ةزهجأ ال عي مج تأدب
رمأ يال لم تحم ال ري ثأتلل كم هف نم دكأت ف، لي غشت ال دي ق ك تكبش

ةيساسأ تامولعم

رورم ةكرح ريفشتب راسملا ىلإ ةدنتسملا (VPN) ةيرهاظلا ةصاخلا ةكبشلا حمست نم الدب رورملا ةكرح هيجوت مادختساو VPN قفن ربع اهلاسرا وأ مامت هالل ةريثملا تانايبلا ريفشتلا وأ ةسايسلا ىلإ ةدنتسملا VPN ةكبش ي ف لاجلا وه امك جهنلا/لوصولا ةمئاق ةكرح تاددحم نييعت مت IPsec قفن لخدت رورم ةكرح ي أب حامسلل ريفشتلا لاجم نييعت مت ىلإ اههيجوت متي رورم ةكرح ي أ نأ ينعى اذهو 0.0.0.0/0.0.0.0 ىل ع ةديعبل او ةيحمل IPsec رورم ةهوجل/ردصم لل ةيعرفلا ةكبشلا نع رظنلا ضغب اهريفت متي IPsec قفن

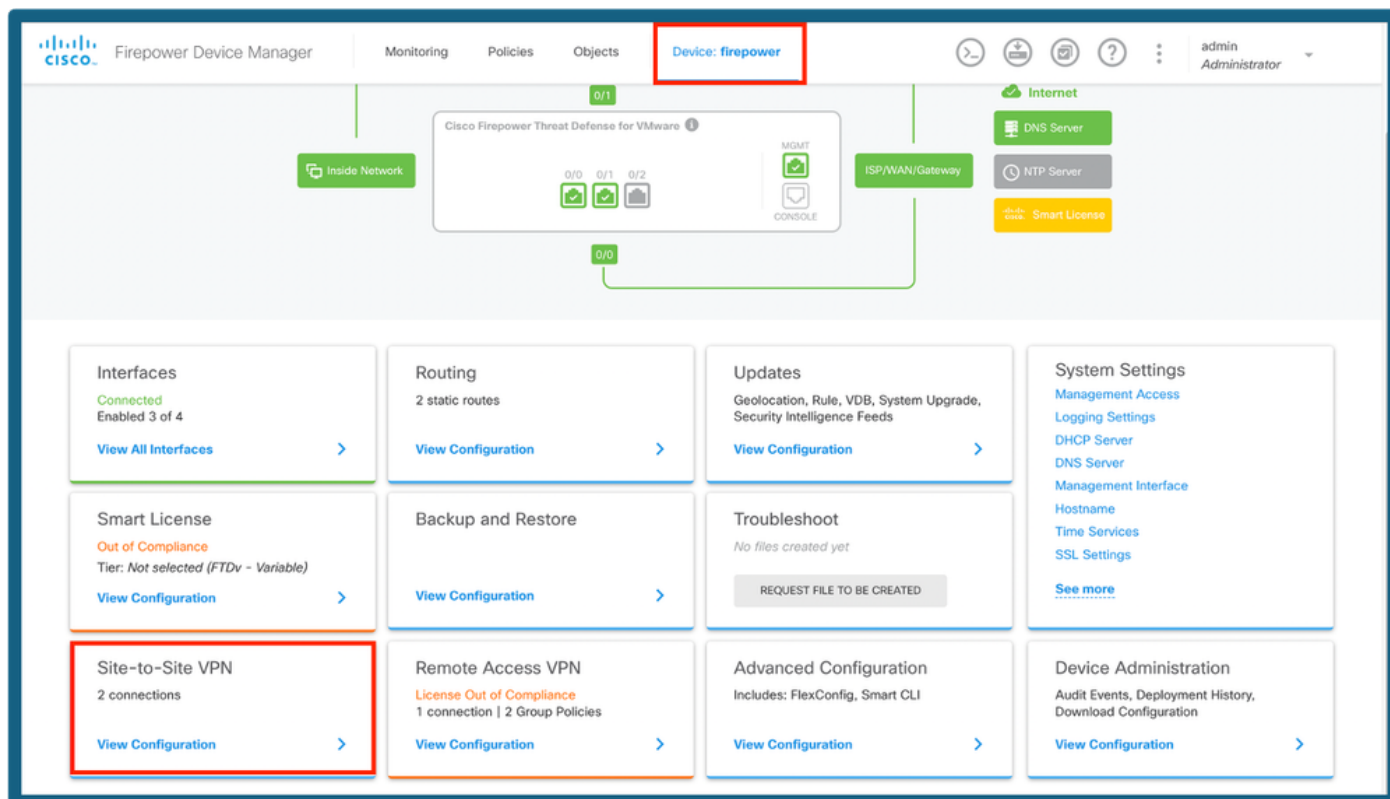
(SVTI) ةتباثلا ةيرهاظلا قفنلا ةهجاو نيوكت ىل ع دنتسملا اذه زكري



ىلإ ةدنتسملا VPN ةكبش نيوكت نكميو، يفاضل صيخرت ىلإ ةجاح دجوت ال: ةطحال م نيكم (ريفشتلا عم قفاوتلا نودب . م ي ققتلا ك ل ذك و صيخرتلا عاضو أ ي ف راسملا ةيمزراوخك طقف DES مادختسا نكمي)، (ريدصتلا لاهب مكحتلا متي يتلا تازيمل ريفشت

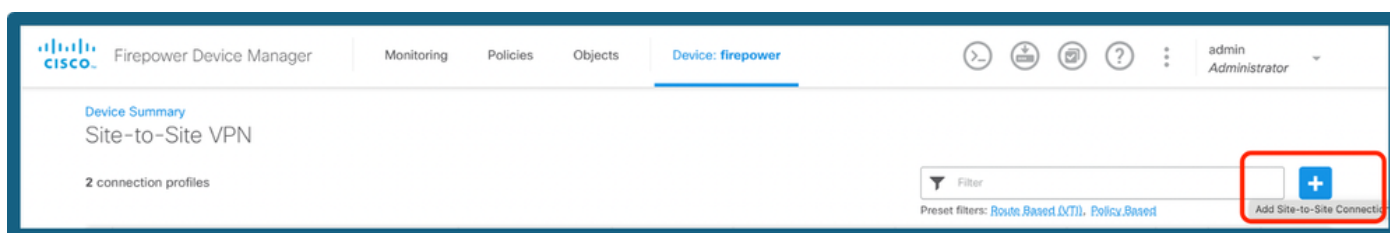
FDM ىل ع نيوك تال تاو طخ

ع قوم ىل ع قوم > زاه ىل لقتنا 1. ةوطخل



FDM تامولعم ةحول

ع قوم لاصتا ىل ديج ع قوم ةفاضل + زمر قوف رقنا 2. ةوطخل



S2S لاصتا ةفاضل

(VTI) راسم لىل دن تسم هنا ىل VPN عون دجو ططخم مسا لخدأ 3. ةوطخل

وأ ةديج يرهاظ قفن ةهجاو عاشن قوف رقنا م، ةي لحم ل VPN ىل لوصول ةهجاو قوف رقنا ةدوجوم ل ةمئاق ل نم ةهجاو دح.

Firepower Device Manager | Monitoring | Policies | Objects | Device: firepower

Local Network --- FIREPOWER --- VPN TUNNEL --- INTERNET --- OUTSIDE INTERFACE --- PEER ENDPOINT --- Remote Network

Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name: **vti-ipsec** Type: **Route Based (VTI)** Policy Based

Sites Configuration

LOCAL SITE

Local VPN Access Interface: Please select

Filter

Nothing found

[Create new Virtual Tunnel Interface](#)

REMOTE SITE

Remote IP Address:

NEXT

قفن ةهجاو ةفاضإ

OK. قوف رقفناو. ةديءال يرهاظال قفنل ةهجاو تاملعم دء. 4 ةوطخال

Create Virtual Tunnel Interface

Name

tunnel10

Status

Most features work with named interfaces only, although some require unnamed interfaces.

Description

Tunnel ID

10

0 - 10413

Tunnel Source

outside (GigabitEthernet0/0)

IP Address and Subnet Mask

192.168.1.1

/

255.255.255.252

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

CANCEL

OK

VTI نېوكت

ناونعلا دوزي. نراق ق فن يلعفل تحت دجاوتي نأ VTI وأ VTI newly created ل 5. ةوطخ ترتخأ ديغب.

New Site-to-site VPN

1 Endpoints 2 Configuration 3 Summary

Local Network FIREPOWER VPN TUNNEL INTERNET OUTSIDE INTERFACE PEER ENDPOINT Remote Network

Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name:

Type: ☒ Route Based (VTI) ☐ Policy Based

Sites Configuration

LOCAL SITE

Local VPN Access Interface:

REMOTE SITE

Remote IP Address:

ريظنن IP ةفاض

يف حضورم وه امك IPsec و IKE تامل عم نييعتل ريرحت رزلا رتخاو IKE رادصل رتخا. 6 ةوطخلال ةروصل.

IKE Policy

i IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

☒ IKE VERSION 2 ☐ IKE VERSION 1

IKE Policy

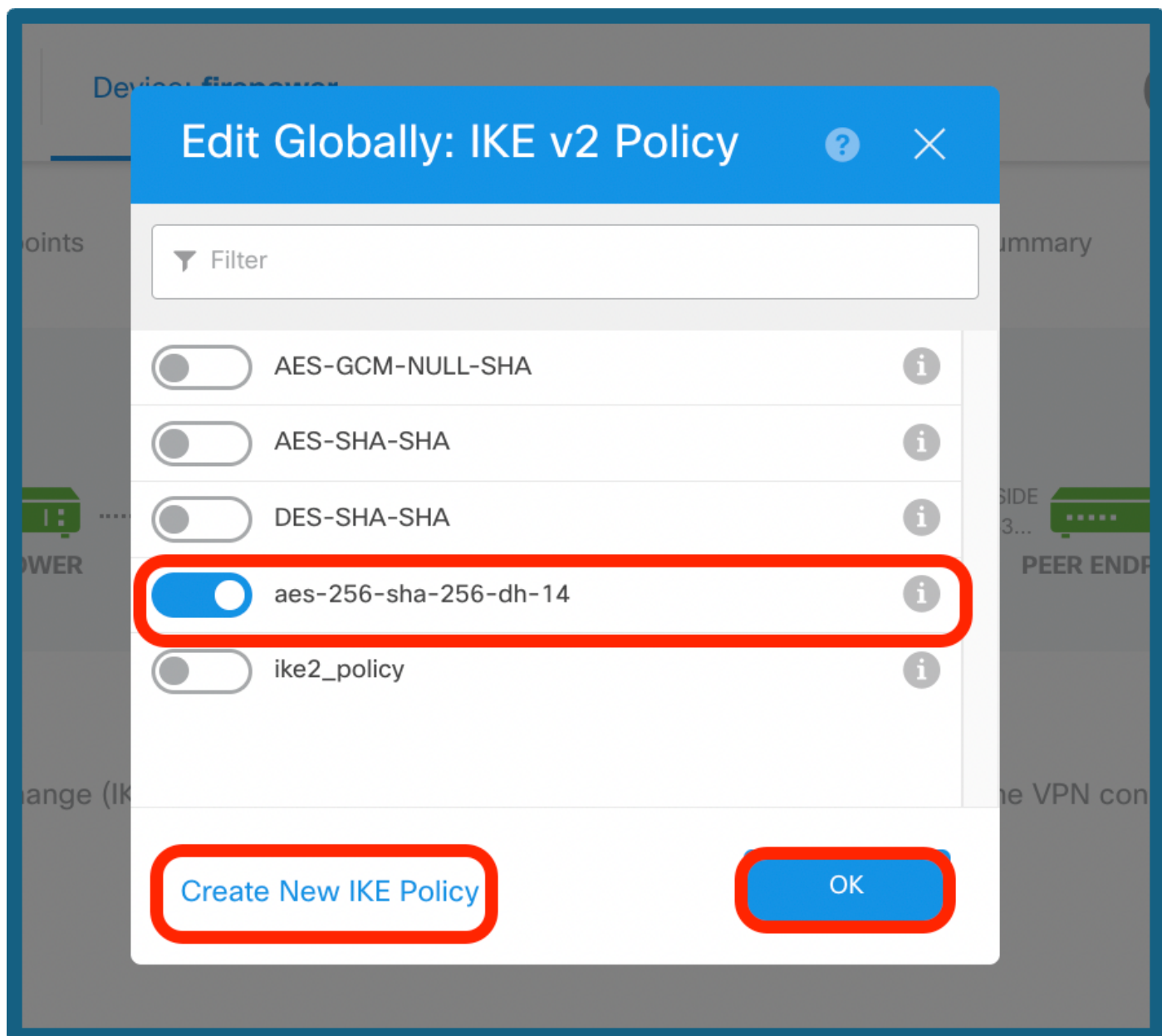
Globally applied

IPSec Proposal

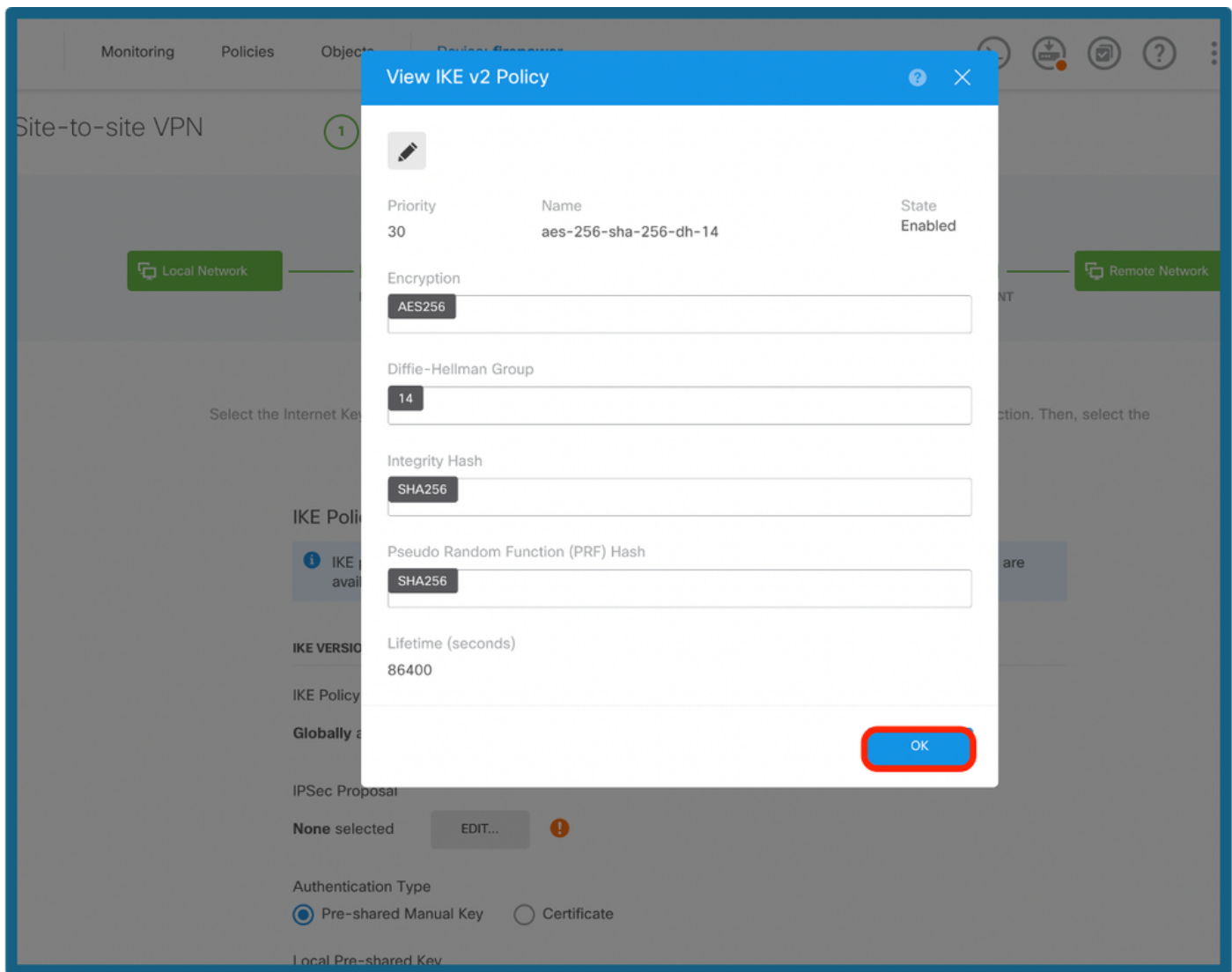
Custom set selected

IKE رادصل نيوكت

IKE چهن عاشنن و اقفاوم رزىل ع رقناو ةروصلال ي ف حضورم وه امك IKE چهن رز رتخا. 7 ةوطخلال ديديچ چهن عاشنن ي ف بغيرت تنك اذا، ديديچ.

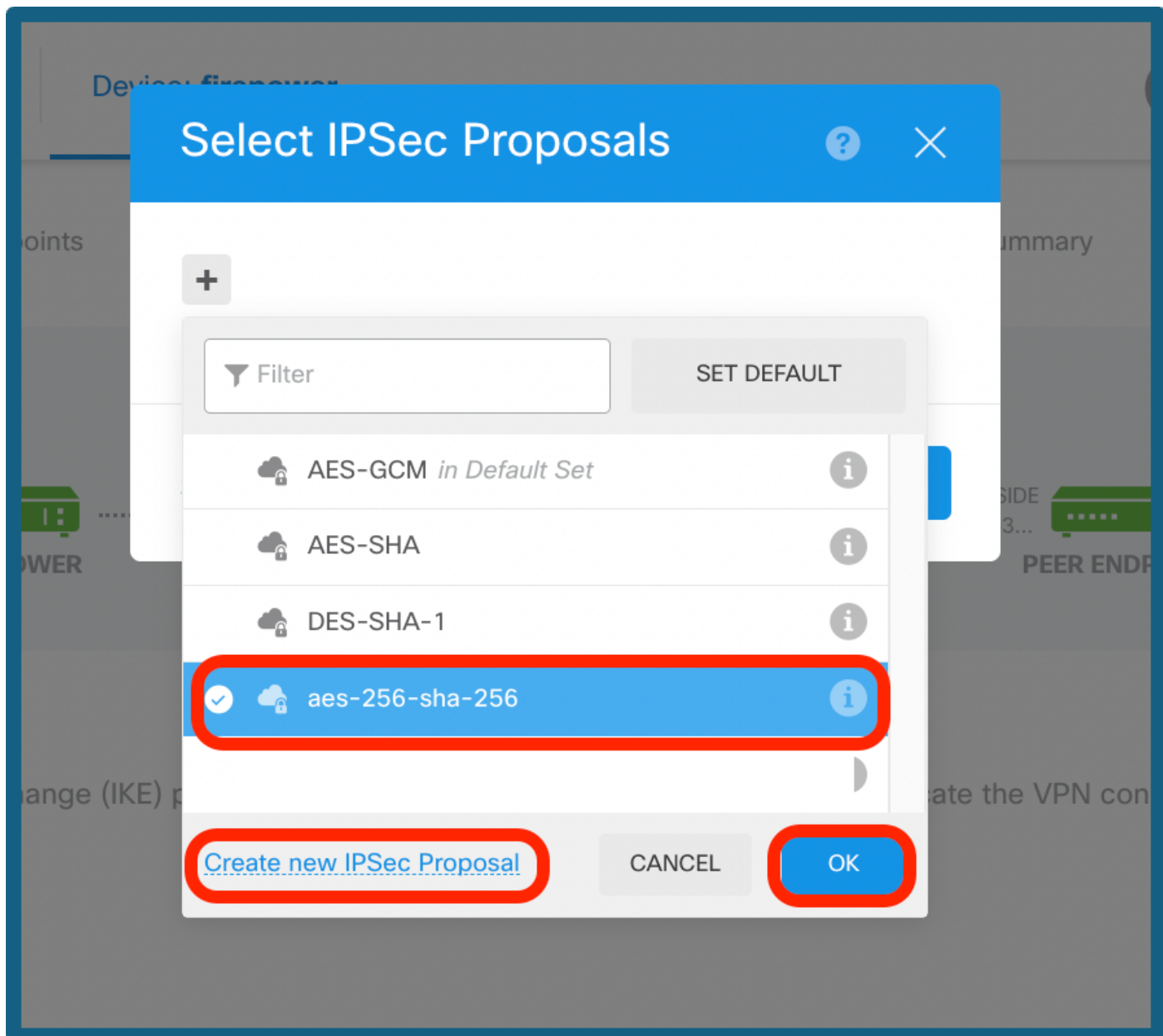


IKE چټن راپټځا



IKE ةسايس نيوكت

ءاشنإ وأ قفاوم رزلا قوف رقناو ةروصلإ ي ف حضوم وه امك IPSec جهن رزلا رتخأ. ب 7 ةوطخلإ
ءي دج حرتقم ءاشنإ ي ف ب غرت تنك اذا، ءي دج IPsec حرتقم



IPsec حرتقم دي دحت

IKE v2 IPSec Proposal

Name

aes-256-sha-256

Encryption

AES256

Integrity Hash

SHA256

OK

IPsec حترتقم نيوكت

مقف ،اقبسّم كترتشملا يوديلا حاتفملا مادختسا مت اذا .ةقداصملا عون ددح .أ 8 ةوطخل
دعب نع اقبسّم هتكراشم تمت يذلا حاتفملا ويلحملا حاتفملا ريفوتب

رمعلال ةدم نيوكتب مق .ةيلاثملا هيچوتلا ةداعا ةيرس تادادعلا رتخأ (يراي تخأ) .ب 8 ةوطخل
يالاتلا قوف رقنا م ث ،يضا رتفالال رمعلال مچحو IPsec لوكوتوربل يضا رتفالال

IKE VERSION 2

IKE VERSION 1

IKE Policy

Globally applied

EDIT...

IPSec Proposal

Custom set selected

EDIT...

Authentication Type

☒ Pre-shared Manual Key

☐ Certificate

Local Pre-shared Key

Remote Peer Pre-shared Key

IPSEC SETTINGS

Lifetime Duration

28800

seconds

120 - 2147483647; (Default: 28800)

Lifetime Size

4608000

kilobytes

10 - 2147483647; (Default: 4608000).
Leave empty for Unlimited.

Additional Options

Diffie-Hellman Group for Perfect Forward Secrecy

No Perfect Forward Secrecy (turned off)

BACK

NEXT

Life و PSK نڀوڪٽ

ءاهان اڃا قوف رڃن او نڀوڪٽ ال عجار 9 ؤوطخل

Summary

Review your configuration. Click Finish to save the connection, or Back to edit settings. When you click Finish, this information will be copied to the clipboard so that you can save it and use it to configure the remote endpoint.

Vti-Ipsec Connection Profile

 Peer endpoint needs to be configured according to specified below configuration.

VPN Access
Interface IP

 tunnel10 (1.1.1.1)



Peer IP Address 10.106.63.23

IKE V2

IKE Policy aes-256-sha256-sha256-14

IPSec Proposal aes-256-sha-256

Authentication
Type Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime
Duration 28800 seconds

Lifetime Size 4608000 kilobytes

ADDITIONAL OPTIONS

Diffie-Hellman
Group Null (not selected)

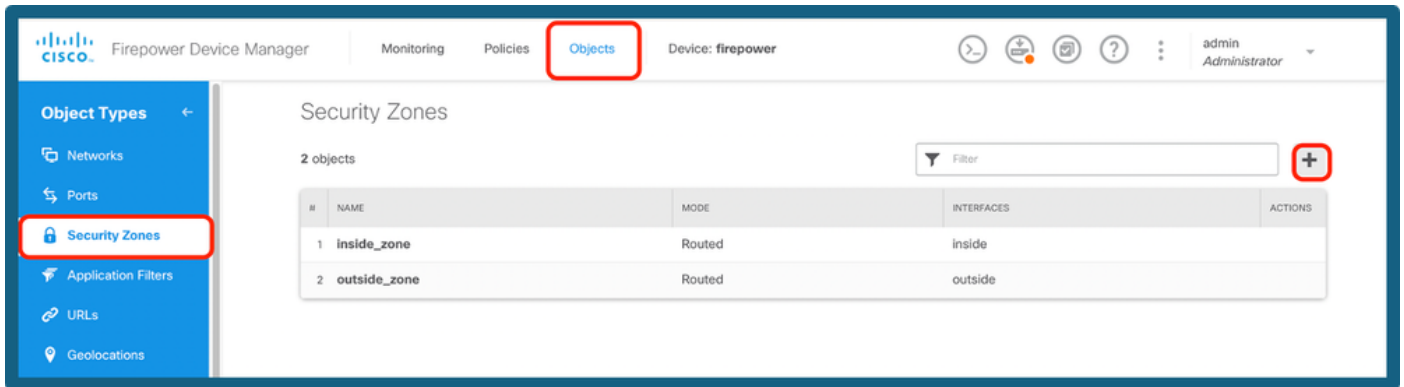
 Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

BACK

FINISH

نېوكټال صخلم

ةنوقيأ + ىلع رقنا م ث نامأ قطانم > تانئاك ىلإ لقتنا 10a ةوطخلا



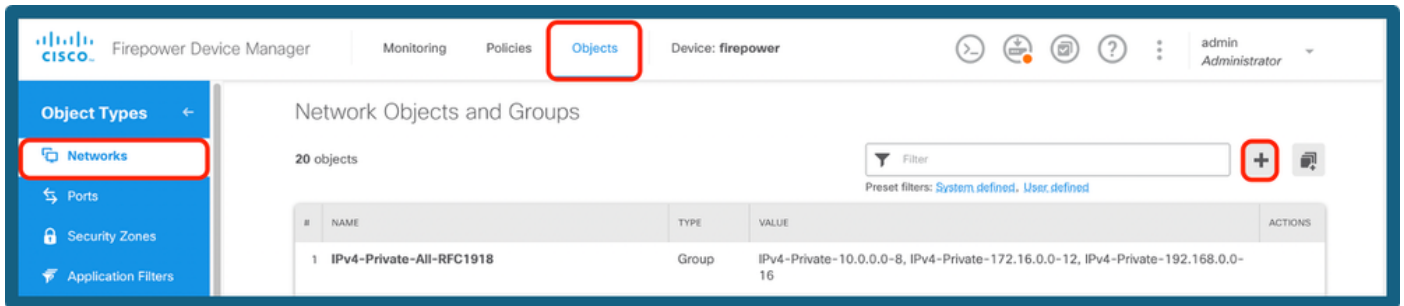
ناماً ةقطنم ةفاضلا

هاندأ حضوم وه امك VTI ةهجاو ددح م ث ،ةقطنم ءاشنإب مق 10b ةوطخلا

The screenshot shows the 'Add Security Zone' dialog box. The 'Name' field is highlighted with a red box and contains 'vti-zone'. The 'Description' field is empty. The 'Mode' section has 'Routed' selected. The 'Interfaces' section has a red '+' button and a list containing 'tunnel10 (Tunnel10)' which is highlighted with a red box. The 'OK' button is also highlighted with a red box.

ةقطنم لال ةقطنم لال نيوكت

ةنوقيأ + ىلع رقنا ،تاكبش > تانئاك ىلإ لقتنا 11a. ةوطخلا



ةكبش تانئاك ةفاضإ

ةطقنب صاخلا قفنلل IP ناو نع مادختساب ةباوب ءاشنإو ،فيضم نئاك ةفاضإ 11b. ةوطخلا ريظنل ةياهن

Edit Network Object

Name

vpn-gateway

Description

Type

☐ Network

☒ Host

☐ FQDN

☐ Range

Host

192.168.1.2

e.g. 192.168.2.1 or 2001:DB8::0DB8:800:200C:417A

CANCEL

OK

VPN ةباوب نيوكت

ةي عرفل ةكبشلاو ةديعبلا ةي عرفل ةكبشلا ةفاضل 11c. ةوطخل

Edit Network Object

Name

remote-vpn-network

Description

Type

☒ Network

☐ Host

☐ FQDN

☐ Range

Network

172.16.10.0/24

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

ديعبلا IP نيوكت

Edit Network Object

?

×

Name

inside-network

Description

Type

☒ Network

☐ Host

☐ FQDN

☐ Range

Network

10.10.10.0/24

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

يحلحالم IP نيوكت

لوصولو لافي مكحتال جهن نيوكتب مقو، تاسايسال > زاهال الى لقتنا 12. ةوطخال

Add Access Rule

Order: 1 | Title: vti-acl | Action: Allow

Source/Destination | Applications | URLs | Users | Intrusion Policy | File policy | Logging

SOURCE

Zones	Networks	Ports	SGT Groups
inside_zone	inside-network	ANY	ANY
vti-zone	remote-vpn-...		

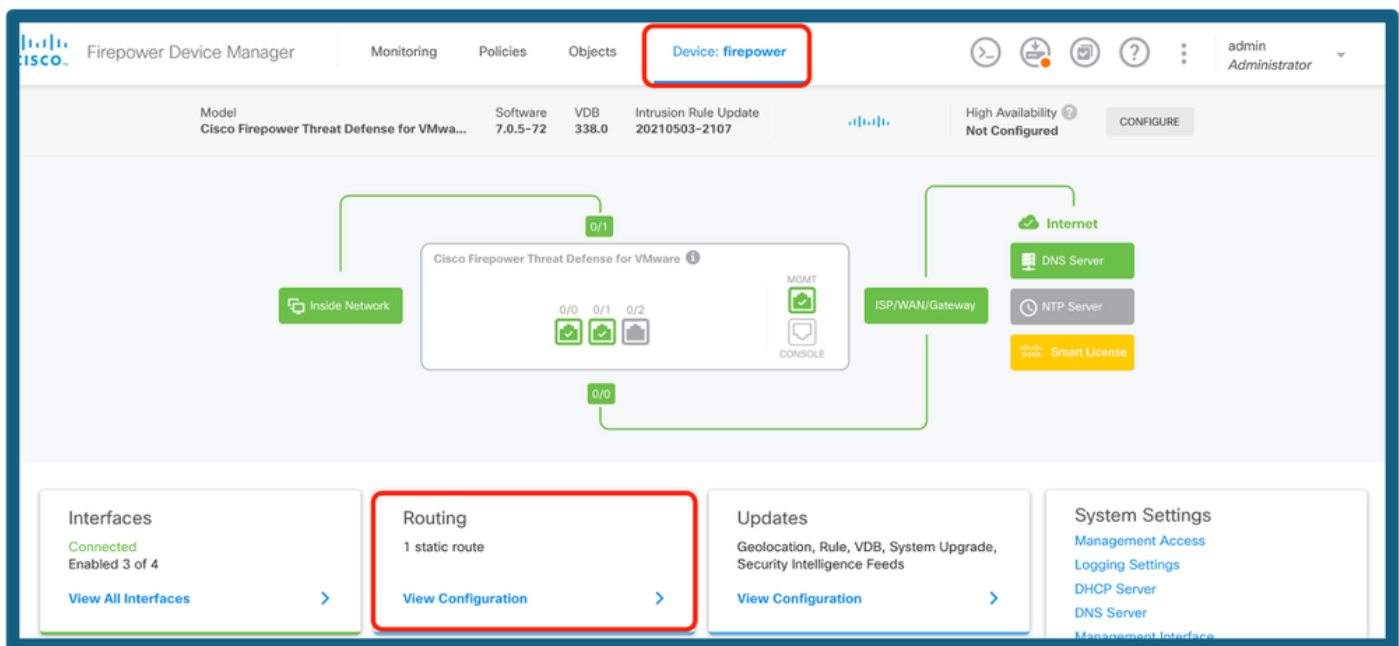
DESTINATION

Zones	Networks	Ports	SGT Groups
inside_zone	inside-network	ANY	ANY
vti-zone	remote-vpn-...		

Show Diagram: ☐ | CANCEL | OK

لوصولاب مكحتال جهن ةفاضإ

هيجوتال > زاهجال إلی لقتنا VTI. قفن ربع هيجوتال ةفاضإب مق 13a. ةوطخل



هيجوت ديحت

+ قوف رقنا. هيجوتال بيوبتال ةمالع نمض تباثال راسمال إلی لقتنا. ب 13 ةوطخل ةنوقيال.

Device Summary

Routing

Add Multiple Virtual Routers

Commands

BGP Global Settings

Static Routing

BGP

OSPF

EIGRP

ECMP Traffic Zones

1 route

Filter

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	default	outside	IPv4	0.0.0.0/0	10.106.52.1		1	

راسم ءفاضإ

OK. قوف رقناو .ءباوبلا مءءقو ؁ءكبشلا رءءاو ؁ءءءاولا رءفوءب مق .13c ءوطللا

Add Static Route

Name

vti-route

Description

Interface

tunnel10 (Tunnel10)

Protocol

☒ IPv4 ☐ IPv6

Networks

+

remote-vpn-network

Gateway

vpn-gateway

Metric

1

SLA Monitor

Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

تبادل ال راسم ال نيوك

نآال رشن ال قوف رقا مآ تاريخي غتل عجار . رشن ال إل لقتنا . 14 ةوطخل

Pending Changes

✓

Last Deployment Completed Successfully

26 Jun 2025 05:27 PM. [See Deployment History](#)

Deployed Version (26 Jun 2025 05:27 PM)	Pending Version																												
+ Static Route Added: <i>vti-route</i> <table> <tr><td>-</td><td>metricValue: 1</td></tr> <tr><td>-</td><td>ipType: IPv4</td></tr> <tr><td>-</td><td>name: vti-route</td></tr> <tr><td>iface:</td><td></td></tr> <tr><td>-</td><td>tunnel10</td></tr> <tr><td>gateway:</td><td></td></tr> <tr><td>-</td><td>vpn-gateway</td></tr> <tr><td>networks:</td><td></td></tr> <tr><td>-</td><td>remote-vpn-network</td></tr> </table>		-	metricValue: 1	-	ipType: IPv4	-	name: vti-route	iface:		-	tunnel10	gateway:		-	vpn-gateway	networks:		-	remote-vpn-network										
-	metricValue: 1																												
-	ipType: IPv4																												
-	name: vti-route																												
iface:																													
-	tunnel10																												
gateway:																													
-	vpn-gateway																												
networks:																													
-	remote-vpn-network																												
+ Access Rule Added: <i>vti-acl</i> <table> <tr><td>-</td><td>logFiles: false</td></tr> <tr><td>-</td><td>eventLogAction: LOG_NONE</td></tr> <tr><td>-</td><td>ruleId: 268435458</td></tr> <tr><td>-</td><td>name: vti-acl</td></tr> <tr><td>sourceZones:</td><td></td></tr> <tr><td>-</td><td>vti-zone</td></tr> <tr><td>-</td><td>inside_zone</td></tr> <tr><td>destinationZones:</td><td></td></tr> <tr><td>-</td><td>vti-zone</td></tr> <tr><td>-</td><td>inside_zone</td></tr> <tr><td>sourceNetworks:</td><td></td></tr> <tr><td>-</td><td>remote-vpn-network</td></tr> <tr><td>-</td><td>inside-network</td></tr> <tr><td>destinationNetworks:</td><td></td></tr> </table>		-	logFiles: false	-	eventLogAction: LOG_NONE	-	ruleId: 268435458	-	name: vti-acl	sourceZones:		-	vti-zone	-	inside_zone	destinationZones:		-	vti-zone	-	inside_zone	sourceNetworks:		-	remote-vpn-network	-	inside-network	destinationNetworks:	
-	logFiles: false																												
-	eventLogAction: LOG_NONE																												
-	ruleId: 268435458																												
-	name: vti-acl																												
sourceZones:																													
-	vti-zone																												
-	inside_zone																												
destinationZones:																													
-	vti-zone																												
-	inside_zone																												
sourceNetworks:																													
-	remote-vpn-network																												
-	inside-network																												
destinationNetworks:																													

MORE ACTIONS ▾

CANCEL

DEPLOY NOW ▾

نويوكتال رشن

ةحصلال نم ققحتال

رماوأل مادختساب CLI ىلع قفنال ةلاح نم ققحتال كنكمي ،رشنال لامتك درجمب

1. show crypto ikev2 sa
2. show crypto ipSec sa <peer-ip>

```
> show crypto ikev2 sa
```

```
IKEv2 SAs:
```

```
Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

Tunnel-id	Local	Remote	Status	Role
3294213359	10.106.52.222/500	10.106.63.23/500	READY	INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK				
Life/Active Time: 86400/141 sec				
Child sa:	local selector 0.0.0.0/0 - 255.255.255.255/65535			
	remote selector 0.0.0.0/0 - 255.255.255.255/65535			
	ESP spi in/out: 0x26a14554/0xd5db88bc			

```
> show crypto ipsec sa
```

```
interface: tunnel10
```

```
Crypto map tag: __vti-crypto-map-5-0-10, seq num: 65280, local addr: 10.106.52.222
```

```
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: 10.106.63.23
```

رم اوألا راهظا

ةلص تاذا تامولعم

ةطساوب هترادإ متت يذلا FTD ىلع عقوم ىلإ عقوم نم VPN تاكبش لوح تامولعملا نم ديزمل
انه لماكلا نيوكتل ليلد ىلع روثعل كنكمي FDM:

[FDM لبق نم رادملا FTD نيوكتل ليلد](#)

ةمچرتل هذه ل و ح

ةيلآل تاي نقتل 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 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 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