

# راسم لى لى ة دن تسم لى VPN ة ك ب ش ني وكت ة ط سا وب ة رادم لى FTD لى لى ة دن تسم لى FDM

## تايوت حمل لى

[ة م د ق م لى](#)

[ة ي س اس ا ل ا ت ا ب ل ط ت م لى](#)

[ت ا ب ل ط ت م لى](#)

[ة م د خ ت س م لى ت ا ن و ك م لى](#)

[ة ي س اس ا ت ا م و ل ع م](#)

[ن ي و ك ت لى](#)

[ة ك ب ش ل ل ي ط ي ط خ ت ل ا م س ر لى](#)

[F T D ن ي و ك ت](#)

[A S A ن ي و ك ت](#)

[ة ح ص ل ل ا ن م ق ق ح ت لى](#)

[ا ه ج ا ل ص ا و ا ط خ ا ل ا ف ا ش ك ت س ا](#)

[ع ج ر م لى](#)

## ة م د ق م لى

ع قوم لى لى ع قوم ن م راسم لى لى ة دن تسم لى VPN ة ك ب ش ني وكت ة ي ف ي ك دن تسم لى اذه حضوي  
FDM ة ط سا وب ة رادم لى FTD لى لى

## ة ي س اس ا ل ا ت ا ب ل ط ت م لى

### ت ا ب ل ط ت م لى

ة ي ل ل ا ت ل ع ي ض ا و م ل ا ب ة ف ر ع م ك ي د ل ن و ك ت ن ا ب C i s c o ي ص و ت

- (VPN) ة ي ر ه ا ظ ل ا ة ص ا خ ل ا ة ك ب ش ل ل ي س اس ا ل ا م ه ف ل ا
- (VRF) ه ي ج و ت ل ا ة د ا ع ا و ي ر ه ا ظ ل ا ه ي ج و ت ل ل ي س اس ا ل ا م ه ف ل ا
- f d m ة ر ا د ا ة ب ر ج ت

### ة م د خ ت س م لى ت ا ن و ك م لى

ة ي ل ل ا ت ل ا ة ي د ا م ل ا ت ا ن و ك م ل ا و ج م ا ر ب ل ا ت ا ر ا د ص ل لى لى دن تسم لى اذه ي ف ة د ر ا و ل ا ت ا م و ل ع م لى دن ت س ت

- C i s c o F T D v ، ر ا د ص ل ا 7.4.2
- C i s c o F D M ، ر ا د ص ل ا 7.4.2
- C i s c o A S A v ، ر ا د ص ل ا 9.20.3

ةصاخ ةي لمعم ةئيب يف ةدوجوملا ةزهجال نم دنتسملا اذه يف ةدراول تامولعمل عاشنإ مت تناك اذا .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجال عيمج تآدب رما يأل لمحتحمل ريثأتلل كمهف نم دكأتف ،ليغشتلا ديقتك تكتبش

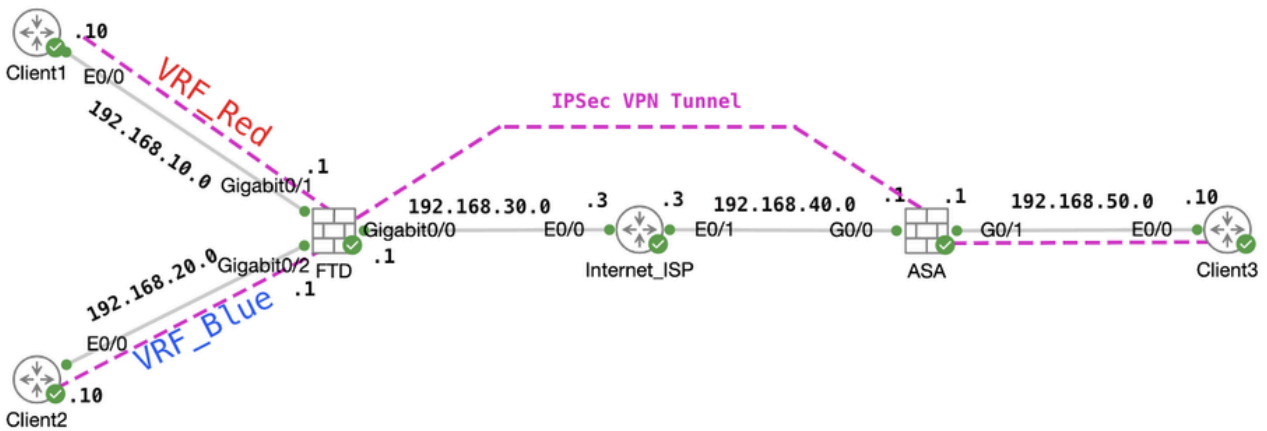
## ةيساسأ تامولعم

FirePOWER Device Manager (FDM) لىع (VRF) يرهاظلا هيچوتلا ةداعإو هيچوتلا كل حمسي ةيرانلا ةقاطلا ديدهت نع عافدلل دحاو زاهج لىع ةلوزعمل هيچوتلا تاليثم نم ديدعل عاشنإب لودجب دوزم لصفنم يضرارتفا هجومك (VRF) يكلساللا ددرتلا تالاح نم ةلاح لك لمعت (FTD) رفويو ةكبشلا رورم ةكرحل يقطنملا لصفلا ةيناكمإ حيتي امم ،هه صاخلا هيچوتلا تانايبل رورم ةكرح ةرادإو نامألل ةنسمح تاناكمإ

ةكبش دجوت VTI مادختساب VRF ل ةكردملا VPN ةكبش نيوكت ةيفيك دنتسملا اذه حرشي ةصاخلا ءارمحل ةكبشلا يف 1 ليمعمل لصفتي دق .FTD فلخ ءاقرزل VRF ةكبشو ءارمحل VRF قفن لالخنم 3 ليمعمل VRF Blue لوكوتورب يف 2 ليمعمل VRF لوكوتورب IPsec VPN.

## نيوكتلا

ةكبشلا ليطيختلا مسرلا

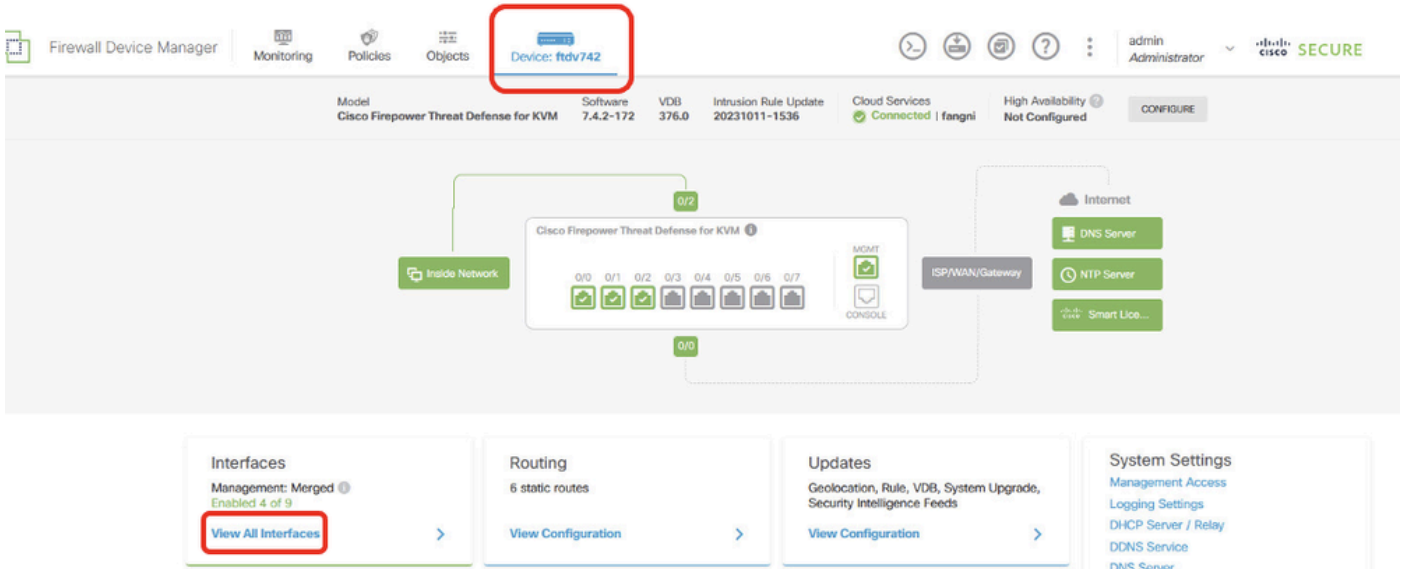


طاطخملا

## FTD نيوكت

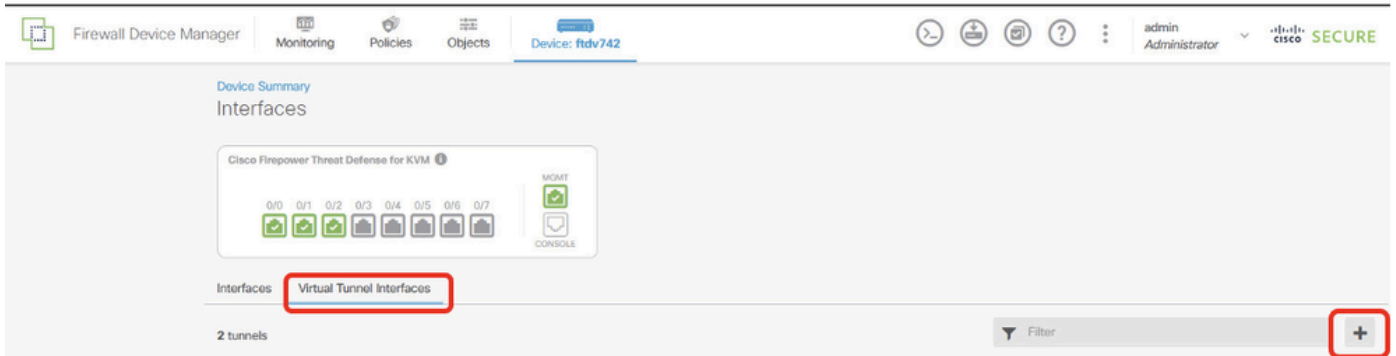
لكشب دقعل نيبي IP لاصلتال يلوألا نيوكتلا لامتك نم دكأتلا يوررضلا نم 1. ةوطخل لخد ASA عم 3 ليمعمل نوكي . ةبوابك FTD ل يلخد IP ناوئع عم Client1 و Client2 نوكي .حيحص ةبوابك IP ناوئع

ةيموسرلا مدختسملا ةهجاو لوخد ليجستب مق .ةيرهاظلا قفنلا ةهجاو عاشنإب مق 2. ةوطخل . تاهجاو ل عيمج ضرع لىع رقنا . تاهجاو ل > زاهجال لىل لقتنا .FTD ل FTD ل (GUI)



تاهجاو FTD\_VIEW\_INTERFACES

رز + قوف رقا .يره اظال ق فنل ل تاهجاو بي وبت ل ة مال ع قوف رقا 2.1 ة واطخ ل



FTD\_Create\_VTI

رز ok تق طقط . ة مال ل تامول عمل ري فوت -2-2 ة واطخ ل

- يت فوم يد : م سال ل
- ق فنل ل فرعم 1
- جراخ : ق فنل ل رصم (GigabitEthernet0/0)
- ة ي عرف ل ة كبش ل ل عانق و IP ناو نع : 169.254.10.1/24
- حاتم ل ل عضوم ل ل ع ق ل ز ن م ل رقا : ة ل ا ح ل

Name  
demovti

Status

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

Description

Tunnel ID  
1

Tunnel Source  
outside (GigabitEthernet0/0)

0 - 10413

IP Address and Subnet Mask

169.254.10.1 / 24

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

CANCEL

OK

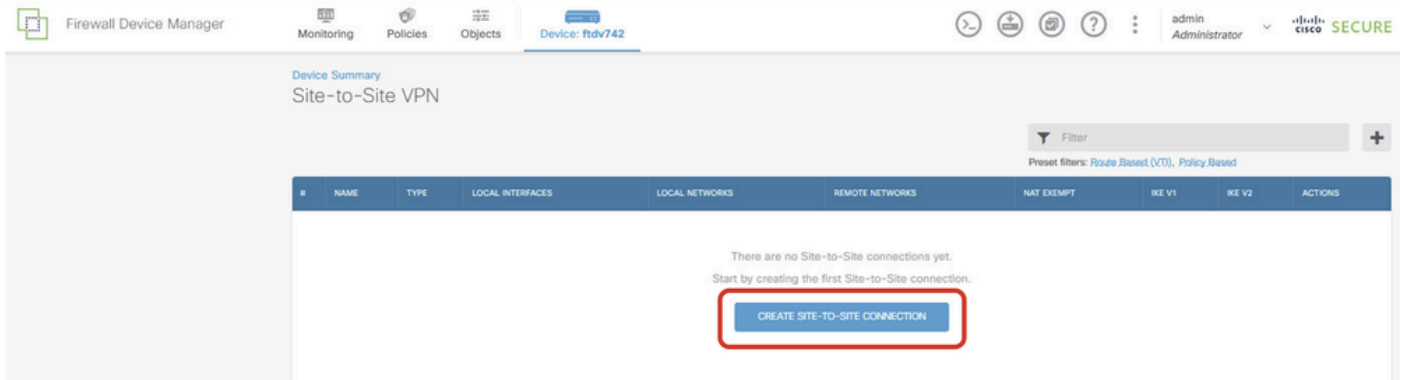
FTD\_Create\_VTI\_Details لي صرافت

نيوكتال لضرع رزلا قوف رونا . عقوم يلا عقوم نم VPN ةكبش > زاھ يلا لقتنا 3. ةوطخل



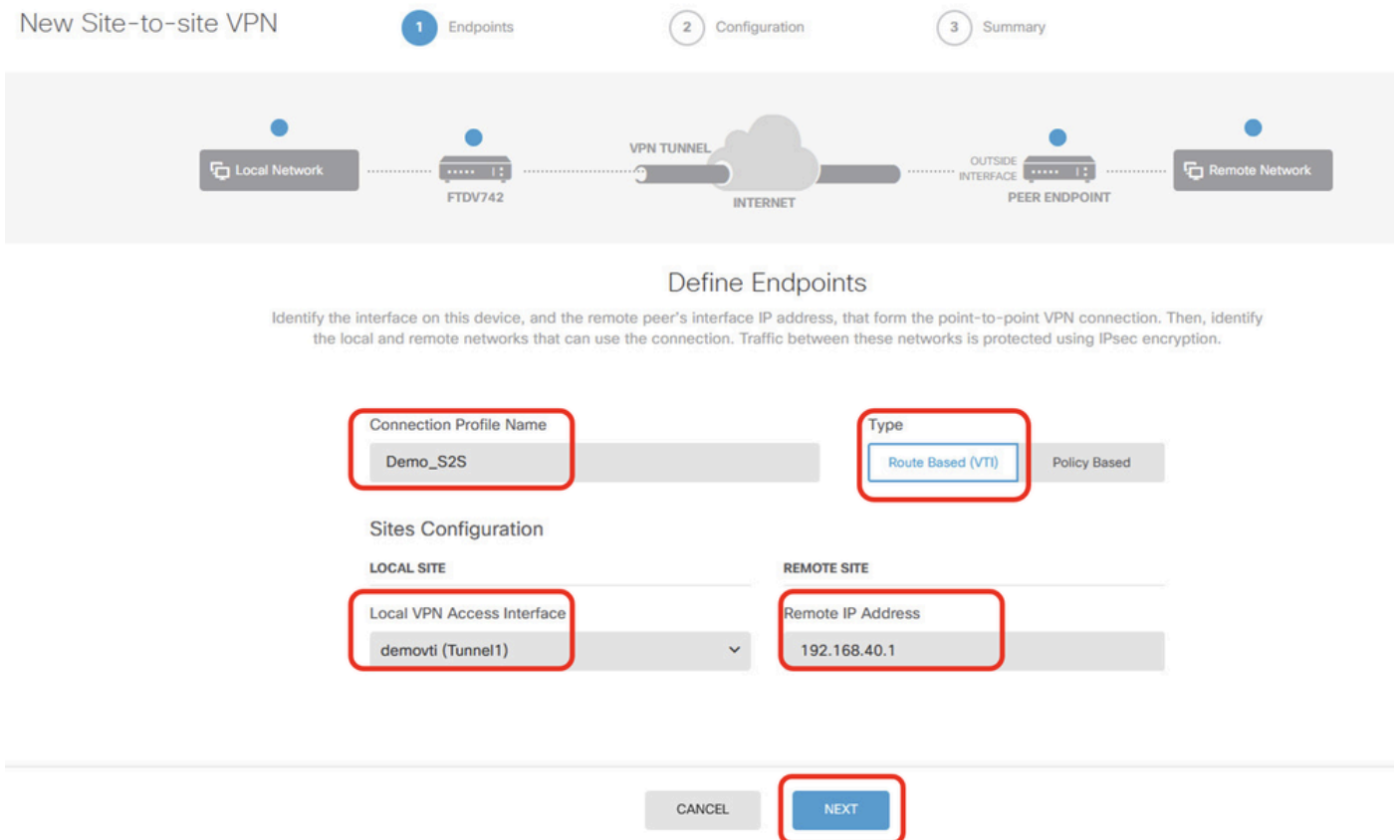
<b>Interfaces</b> Management: Merged Enabled 4 of 9 <a href="#">View All Interfaces</a>	<b>Routing</b> 1 static route <a href="#">View Configuration</a>	<b>Updates</b> Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds <a href="#">View Configuration</a>	<b>System Settings</b> <a href="#">Management Access</a> <a href="#">Logging Settings</a> <a href="#">DHCP Server / Relay</a> <a href="#">DDNS Service</a> <a href="#">DNS Server</a> <a href="#">Hostname</a> <a href="#">Time Services</a> <a href="#">SSL Settings</a> <a href="#">See more</a>
<b>Smart License</b> Registered Tier: FTDv50 - 10 Gbps <a href="#">View Configuration</a>	<b>Backup and Restore</b> <a href="#">View Configuration</a>	<b>Troubleshoot</b> No files created yet REQUEST FILE TO BE CREATED	
<b>Site-to-Site VPN</b> There are no connections yet <a href="#">View Configuration</a>	<b>Remote Access VPN</b> Requires Secure Client License No connections   1 Group Policy <a href="#">Configure</a>	<b>Advanced Configuration</b> Includes: FlexConfig, Smart CLI <a href="#">View Configuration</a>	<b>Device Administration</b> <a href="#">Audit Events, Deployment History, Download Configuration</a> <a href="#">View Configuration</a>

نم لاصتا عاشن رز یل عرقوم یل عرقوم نم ةدیج VPN ةكبش عاشن ادب 3.1 ةوطخل رز + قوف رقا وا عرقوم یل عرقوم

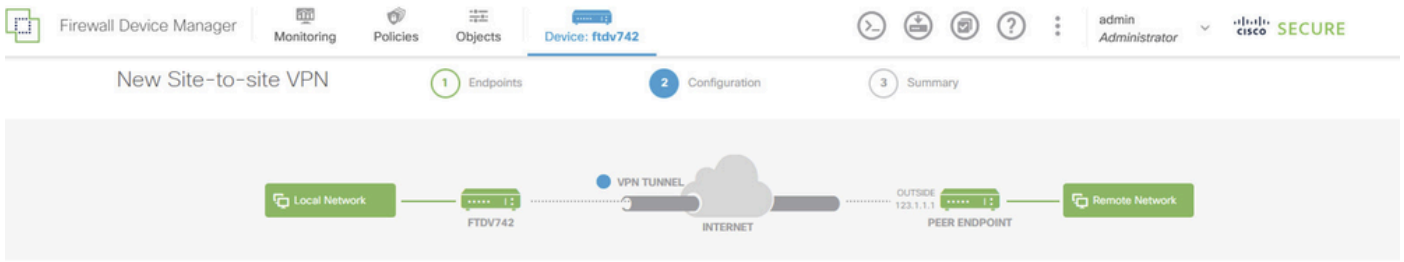


رز كلذ دعب تقطقط .ةرررضلا تامولعمل ريفوت 3.2 ةوطخل

- S2S\_يحيضوتلا ضرعلا :لاصتالا فيرعت فلم مسا
- (VTI) راسملا یل دنتم :عونلا
- (2 ةوطخل یف اهؤاشن م) Demovti :ةيحمل VPN ةكبش یل لوصولا ةهجاو
- (IP ناونع چراخ ريظنلا ASA وه اذه) 192.168.40.1 :ديعلل IP ناونع



رز ررحي ةقطقط .IKE ةسايس یل لقتنا 3.3 ةوطخل



### Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

#### IKE Policy

**1** 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

None selected

FTD\_Edit\_IKE\_Policy

رقن لابل دي دج جهن عاشن اكنكمي و اقبسم فرعم مادختس اكنكمي، IKE جهن ل 3.4 ةوطخل  
 . دي دج IKE جهن عاشن ا قوف

ظحلل قفاوم رزلا قوف رقنا . AES-SHA دوچوم IKE ةسايس مسا لي دبت ، لاثملا اذه ي

Filter

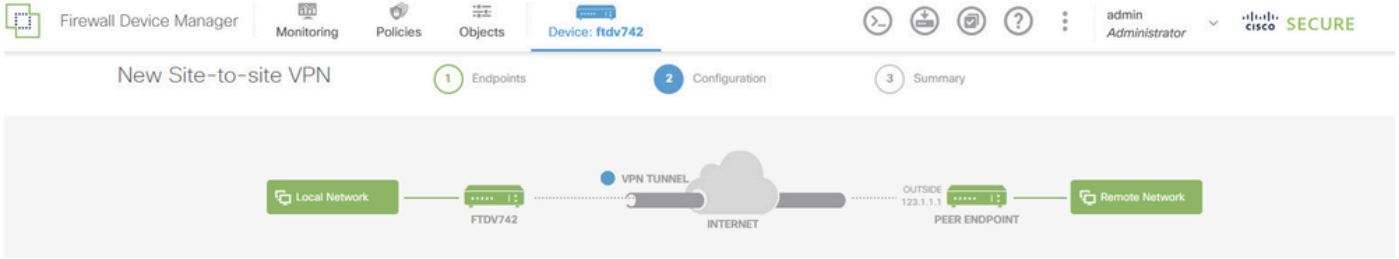
<input type="checkbox"/>	AES-GCM-NULL-SHA	i
<input checked="" type="checkbox"/>	AES-SHA-SHA	i
<input type="checkbox"/>	DES-SHA-SHA	i

Create New IKE Policy

OK

FTD\_ENABLE\_IKE\_POLICY

رز ررچي ةق طق ط . IPsec حارتقا ىل لقتنا . 3.5 ةوطخلا



### Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

#### IKE Policy

1 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

None selected  1

FTD\_Edit\_IPSec\_Proposal

حارتقا عاشنإ كنكمي وأ اقبسم فرعم مادختسإ كنكمي، IPsec حارتقال ةبسنلاب .3.6 ةوطخلال ديذج IPsec حرتقم عاشنإ قوف رقنلال لالخنم ديذج .

ظحللرز قفاوم رقنا . AES-SHA دوومل IPsec حارتقاسا لدب، لاثملا اذيف .



# Select IPsec Proposals



Filter

SET DEFAULT

 AES-GCM *In Default Set* 



 AES-SHA



 DES-SHA-1 

Create new IPsec Proposal

CANCEL

OK

FTD\_ENABLE\_IPsec\_Proposal

تقطوط. اقبس م كرتشم الحاتفم لانيوكتو ةحفص ل لفسأل ريرمتلاب مق 3.7 ةوطخلال  
رز كلذ دعب.

اقحال ASA لىع هنيوكتو اقبس م كرتشم الحاتفم ل اذ ةظالم عاجرلا.



### Demo\_S2S Connection Profile

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

**VPN Access Interface** demovti (169.254.10.1) ↔ **Peer IP Address** 192.168.40.1

**IKE V2**

**IKE Policy** aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14

**IPSec Proposal** aes,aes-192,aes-256-sha-512,sha-384,sha-256,sha-1

**Authentication Type** Pre-shared Manual Key

**IKE V1: DISABLED**

**IPSEC SETTINGS**

**Lifetime Duration** 28800 seconds

**Lifetime Size** 4608000 kilobytes

**ADDITIONAL OPTIONS**

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.

Diffie-Hellman Null (not selected)

Group

**BACK** **FINISH**

FTD\_REVIEW\_VPN\_CONFIGURATION

اذه في ف TD ربع رورملا ةكرحل حامسلل لوصولا في م كحتلا ةدعاق عاشناب مق 3.9 ةوطخلل كب صاخلل جهنلل ليدعت اعارلا .يحوضوتلا ضرعلا فدهب عيمجلل حامسلاب مق ،لائملا ةيلعلل كئاجايتحإ لىل اءانسا .

Firewall Device Manager Monitoring Policies Objects Device: ftdv742 admin Administrator cisco SECURE

### Security Policies

SSL Decryption → Identity → Security Intelligence → NAT → Access Control → Intrusion

1 rule

#	NAME	ACTION	SOURCE			DESTINATION			APPLICATIONS	URLS	USERS	ACTIONS
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS				
1	Demo_allow	Allow	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY		

Default Action Access Control Block

FTD\_ACP\_Example

ناك اذ TD لىل ليمعلا رورم ةكرحل NAT اءانسا ةدعاق نيوكتب مق (يرايئا). 3.10 ةوطخلل

دجوت ال، لاثملا اذه يف .تنرتنإلإ لوصولل ليمع ل هنيوكت مت يكيمايدي NAT كانه  
FTD. ىلع يكيمايدي NAT نيوكت مدع ببسب NAT اناثتسا ةدعاق نيوكتل ةجاح

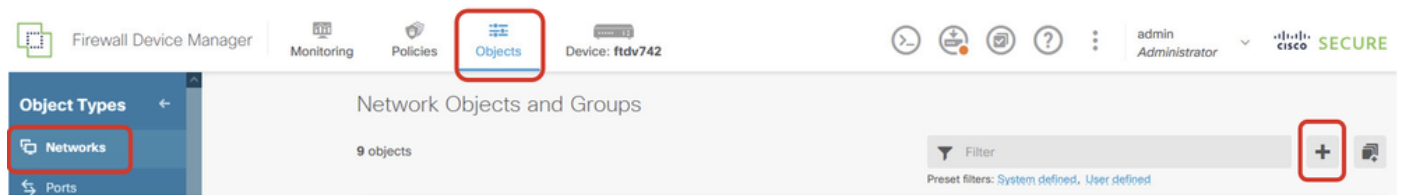
نيوكتل تاريخي رغت رشن .3.11 ةوطخال



FTD\_DEPLOYMENT\_CHANGES

ةيرهاظلا تاهجوملا نيوكت .4 ةوطخال

قوف رقنا ، تاكبش > تانئاك ىلإ لقتنا .تباثلا راسم لل ةكبش تانئاك عاشنإ .4.1 ةوطخال  
رز .+



FTD\_Create\_NetObjects

رز .ok تقطقط .ةكبش نئاك لك ل ةمزاللا تامولعمل ري فوت .4.2 ةوطخال

- مسالا : local\_blue\_192.168.20.0
- ةكبشلا : عونلا
- ةكبشلا : 192.168.20.0/24

## Add Network Object



Name

local\_blue\_192.168.20.0

Description

Type



Network



Host

Network

192.168.20.0/24

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

CANCEL

OK

FTD\_VRF\_BLUE\_Network

- مرسال: local\_red\_192.168.10.0
- ةكبشلا: عونلا
- ةكبشلا: 192.168.10.0/24

## Add Network Object



Name

local\_red\_192.168.10.0

Description

Type



Network



Host

Network

192.168.10.0/24

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

CANCEL

OK

FTD\_VRF\_RED\_Network

- مرسال: remote\_192.168.50.0
- ةكپشلا: عونلا
- ةكپشلا: 192.168.50.0/24

## Add Network Object



Name

remote\_192.168.50.0

Description

Type



Network



Host



FQDN



Range

Network

192.168.50.0/24

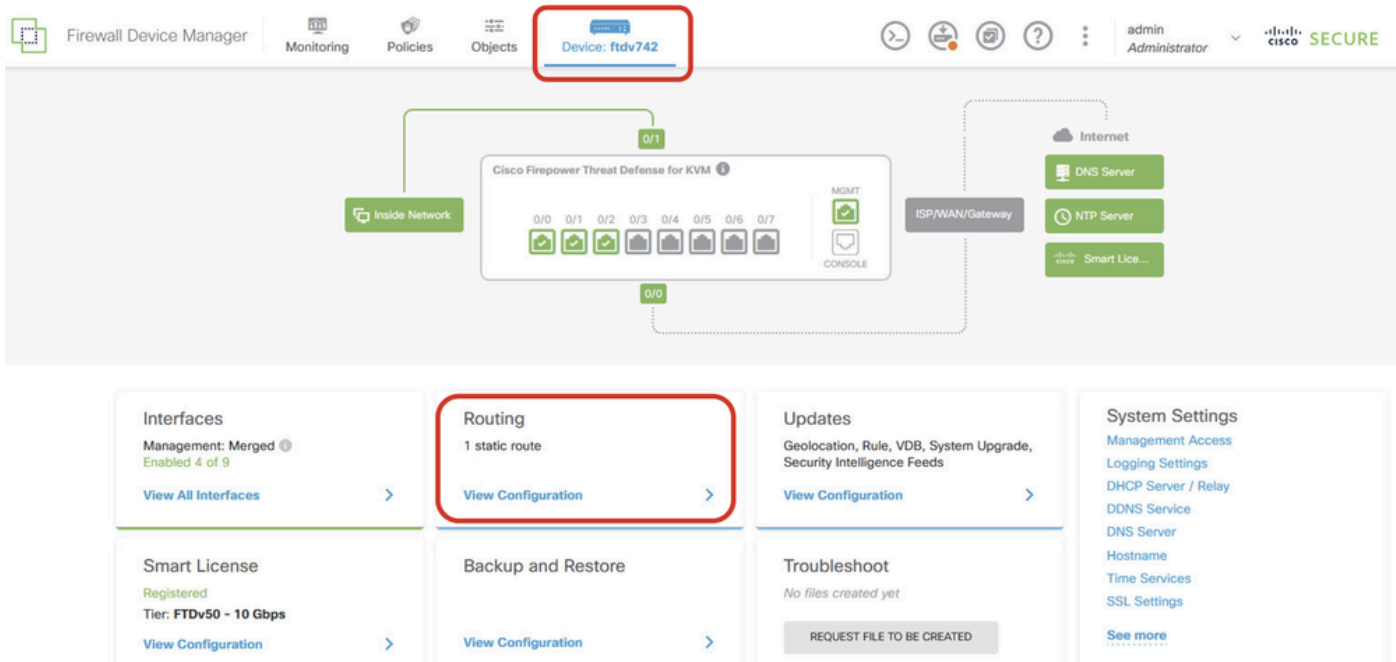
*e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60*

CANCEL

OK

FTD\_REMOTE\_NETWORK

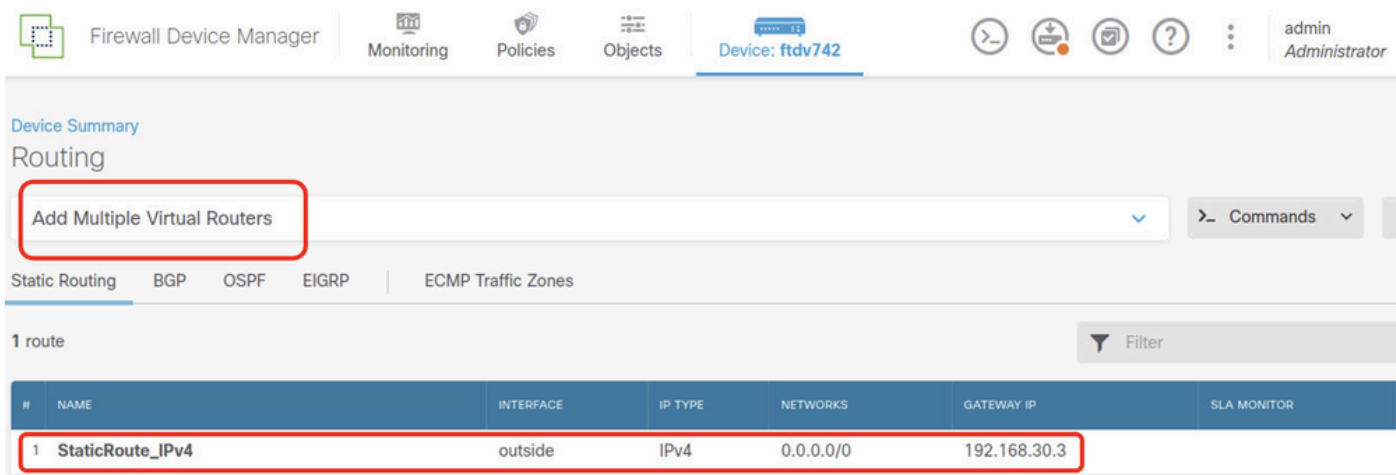
ليكشت ضرع ةق طقط . هيجوتلا > زاوجلإ لىل لقتنا . لوألا ڤره اظلا هجوملا ءاشنإ 4.3 ةوطخلا



FTD\_VIEW\_ROUTING\_Configuration

ةيره اظلال تاهجوم ال نم ديدع ال ةفاضل قوف رقنا 4.4 ةوطخل

كيدل نكت مل اذا FDM ةي ةيهت ءانثا ةيجراخل ةهجاو ال لال خ نم تباث راسم نيوكت مت :ةظحال م ايودي اهنيوكت يجر ي ف



FTD\_ADD\_FIRST\_VIRTUAL\_ROUTER1

لوال صصخ م ال يره اظلال هجوم ال ءاشنل قوف رقنا 4.5 ةوطخل





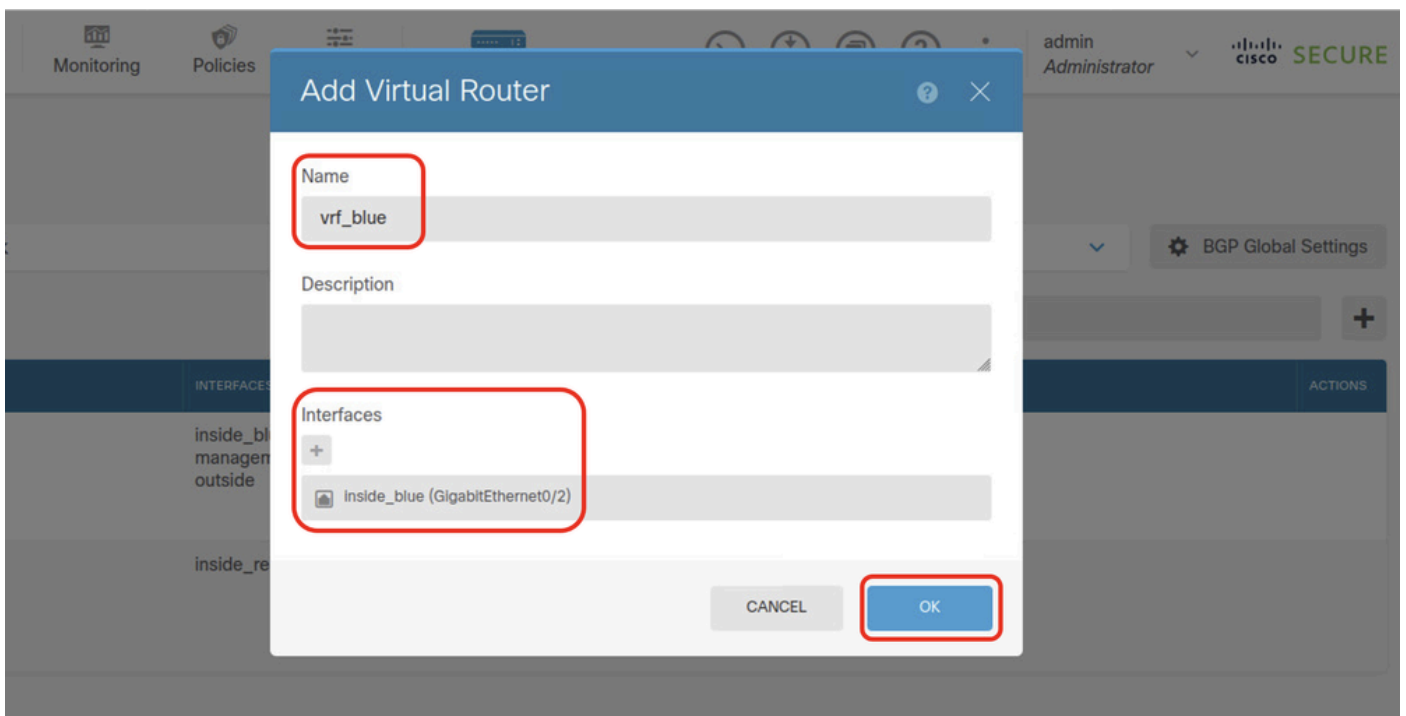
رز + قوف رقنا .



هجوم ل FTD\_Add\_Second\_Virtual\_Router

قف اوم قوف رقنا . ي ن ا ل ل ي ره ا ل ل ه ج و م ل ل م ز ل ل ل ا م و ل ع م ل ا ر ي ف و ت ب م ق . 4.8 ة و ط خ ل ا

- م س ا ل ا : vrf\_blue
- ا ت ا ه ج ا و ل ا : inside\_blue (GigabitEthernet0/2)



FTD\_ADD\_SECOND\_VIRTUAL\_ROUTER2

ة ي ا ه ن ل ل ط ا ق ن ل ر ا س م ل ا ا ذ ه ح ي ت ي . G l o b a l ل ي V R F \_ B l u e ن م ر ا س م ل ا ب ي ر س ت ئ ش ن ا . 5 ة و ط خ ل ا ل ي ل ع ق و م ن م V P N ق ف ن ز ا ي ت ج ا ا ه ن ا ش ن م ي ت ل ا ت ا ل ا ص ت ا ل ا ا د ب 192.168.20.0/24 ة ك ب ش ل ا ل ي ل ع 192.168.50.0/24 ة ك ب ش ة ي ا م ح ب ة د ي ع ب ل ا ة ي ا ه ن ل ل ا ة ط ق ن م و ق ت ، ل ا ث م ل ا ل ي ب س ل ي ل ع . ع ق و م

ة ي ل خ ي ف ض ر ع ل ا ز م ر ق و ف ر ق ن ا . ن ي و ك ت ل ا ض ر ع ق و ف ر ق ن ا . ه ي ج و ت ل ل > ز ا ه ج ل ا ل ي ل ل ق ت ن ا v r f \_ b l u e . ي ر ه ا ط ل ا ه ج و م ل ل ا ر ج ل ا

Device Summary  
Virtual Routers

How Multiple Virtual Routers Work

3 virtual routers

#	NAME	INTERFACES	SHOW/TROUBLESHOOT	ACTIONS
1	Global	management outside	> Routes > IPv6 routes > BGP > OSPF	
2	vrf_blue	inside_blue	> Routes > IPv6 routes > BGP > OSPF	View
3	vrf_red	inside_red	> Routes > IPv6 routes > BGP > OSPF	

FTD\_VIEW\_VRF\_BLUE

رز + قوف رقنا . تباث هي جوت بيوبتلا ةمالع قوف رقنا . 5.1 ةوطخلا

Device Summary / Virtual Routers  
vrf\_blue

How Multiple Virtual Routers Work

Virtual Router Properties | **Static Routing** | BGP | OSPF | ECMP Traffic Zones

Commands

Filter

FTD\_Create\_STATIC\_ROUTE\_VRF\_BLUE

رز ok ةق طقط . ةمزاللا تامولعمل ريفوتب مق . 5.2 ةوطخلا

- مسالا : Blue\_to\_ASA
- ةهجاوولا : Demovti (1 قفنلا)
- تاكبشلا : remote\_192.168.50.0
- اغراف رصنعللا اذه كرتأ : ةباوبلا .

**Name**  
Blue\_to\_ASA

**Description**

**Interface**  
demovti (Tunnel1) Belongs to current Router  
N/A

**Protocol**  
 IPv4  IPv6

**Networks**  
+  
remote\_192.168.50.0

**Gateway**  
Please select a gateway Metric  
1

**SLA Monitor** *Applicable only for IPv4 Protocol type*  
Please select an SLA Monitor

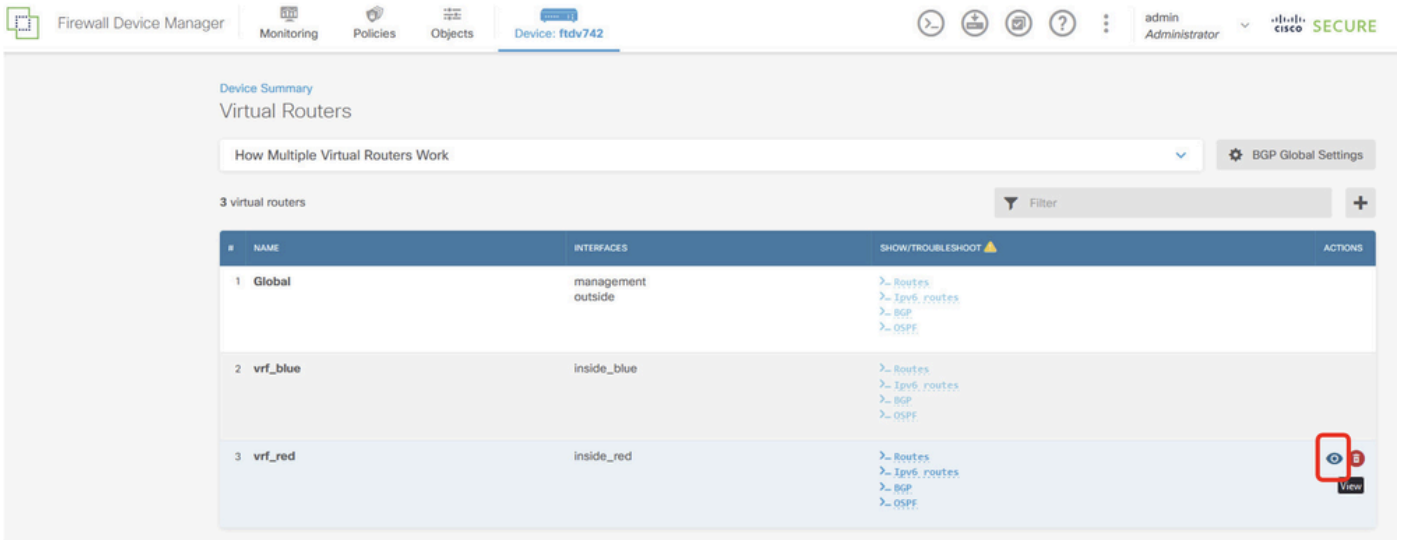
CANCEL OK

FTD\_Create\_STATIC\_ROUTE\_VRF\_BLUE\_Details لي صافات

ةي اهنلا طاقنل راسملا اذه حيتي. Global لي VRF\_RED نم راسملا بيرست ئشنأ. 6 ةوطخلا  
لي عقوم نم VPN قفن زاي تجا اهنأش نم يتلا تالاصتالا ادب 192.168.10.0/24 ةكبشلا لي ع

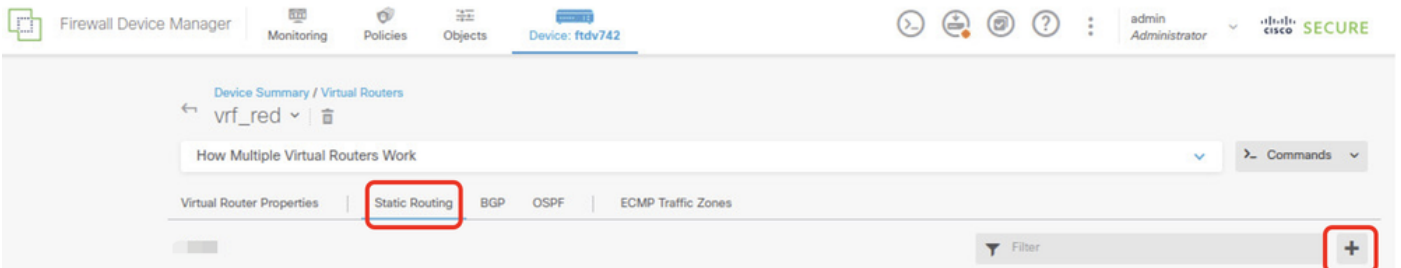
192.168.50.0/24. ةكبش ةيماحب ةديعبل ةياهنل ةطقن موقت ،لاثلما ليلبس لىل ع. قوم

ةيلخ يف ضرعل زمر قوف رقنا . نيوكتل ضرع قوف رقنا . هيجوتلا > زاوجل لىل لقتنا  
vrf\_red. يرهاظلا هجوملل تاءارجل



FTD\_VIEW\_VRF\_RED

رز + قوف رقنا . تباث هيجوت بيوبتل ةمالع قوف رقنا . 6.1 ةوطخلا



FTD\_Create\_STATIC\_ROUTE\_VRF\_RED

رز. ةقطط . ةمزاللا تامولعمل ريفوت . 6-2 ةوطخلا

- مرسال: Red\_to\_ASA
- ةهجاول: Demovti (1 قفنل) : ةهجاول
- تاكلشل: remote\_192.168.50.0
- اغراف رصنعل اذه كرتأ : ةباوجل

vrf\_red

## Add Static Route



Name

Red\_to\_ASA

Description

Interface

demovti (Tunnel1)

Belongs to current Router

N/A

Protocol



IPv4



IPv6

Networks



remote\_192.168.50.0

Gateway

Please select a gateway

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

FTD\_Create\_STATIC\_ROUTE\_VRF\_RED\_Details لى صرافات

تاراسم لحمستو. ةضارت فالال ال الءءوم ال نم راسم ال بىرست ءاشن ال 7 ةوطء ال ءقوم ال ال ءقوم ال نم VPN ءءبش نم ءىءب ال فرط ال ءطساوب ءىءءم ال ءىءه ال طاقن ل

192.168.20.0/24 ةكبش و VRF\_RED يره اظلال هجوم ل ا ف 192.168.10.0/24 ةكبش ل ا لوصول اب ف VRF\_BLUE يره اظلال هجوم ل ا ف .

ةيلخ ف ضرع ل ا زمر قوف رونا . نيوكت ل ا ضرع قوف رونا . هي جوت ل ا > زا ج ل ا ل ا لقتن ا ماع ل ا يره اظلال هجوم ل ا ل ا ل ا ل ا ل ا ل ا ل ا ل ا ل ا ل ا ل ا ل a

Device Summary  
Virtual Routers

How Multiple Virtual Routers Work

3 virtual routers

#	NAME	INTERFACES	SHOW/TROUBLESHOOT	ACTIONS
1	Global	management outside	> Routes > Ipv6 routes > BGP > OSPF	View
2	vrf_blue	inside_blue	> Routes > Ipv6 routes > BGP > OSPF	
3	vrf_red	inside_red	> Routes > Ipv6 routes > BGP > OSPF	

FTD\_VIEW\_VRF\_Global

رز + قوف رونا . تباث هي جوت بيوت ل ا ةمالع قوف رونا . 7.1 ةوطخل ا

Device Summary / Virtual Routers  
Global

How Multiple Virtual Routers Work

Virtual Router Properties | Static Routing | BGP | OSPF | EIGRP | ECMP Traffic Zones

3 routes

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	StaticRoute_IPv4	outside	IPv4	0.0.0.0/0	192.168.30.3		1	

FTD\_Create\_STATIC\_ROUTE\_VRF\_GLOBAL

رز ok ةق طقط . ةمزال ل ا تامولعمل ا ريفوت . 7-2 ةوطخل ا

- م س ل ا : S2S\_leaks\_blue
- ةه ج اول ا : inside\_blue (GigabitEthernet0/2)
- ت اكبش ل ا : local\_blue\_192.168.20.0
- اغراف رصنعل ا اذه كرت ا : ةب اول ا

# Global Add Static Route



Name

S25\_leak\_blue

Description



The selected interface belongs to a different virtual router. If you create this static route, the route will cross virtual router boundaries, with the risk that traffic from this virtual router will leak into another virtual router. Proceed with caution.

Interface

inside\_blue (GigabitEthernet0/2)

Belongs to different Router

vt\_blue

Protocol



IPv4



IPv6

Networks



local\_blue\_192.168.20.0

Gateway

Please select a gateway

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK



```
encryption aes-256 aes-192 aes
integrity sha512 sha384 sha256 sha
group 21 20 16 15 14
prf sha512 sha384 sha256 sha
lifetime seconds 86400
```

يُجرى اختبار التكوين في FTD. يتم إجراء اختبار التكوين في FTD. يتم إجراء اختبار التكوين في FTD.

<#root>

```
crypto ipsec ikev2 ipsec-proposal
```

**AES-SHA**

```
protocol esp encryption aes-256 aes-192 aes
protocol esp integrity sha-512 sha-384 sha-256 sha-1
```

10. إجراء اختبار التكوين في IPsec، إجراء اختبار التكوين في IPsec، إجراء اختبار التكوين في IPsec.

<#root>

```
crypto ipsec profile
```

```
demo_ipsec_profile
```

```
set ikev2 ipsec-proposal
```

**AES-SHA**

```
set security-association lifetime kilobytes 4608000
set security-association lifetime seconds 28800
```

2. إجراء اختبار التكوين في IKEv2، إجراء اختبار التكوين في IKEv2، إجراء اختبار التكوين في IKEv2.

<#root>

```
group-policy
```

```
demo_gp_192.168.30.1
```

```
internal
group-policy demo_gp_192.168.30.1 attributes
vpn-tunnel-protocol ikev2
```

3. إجراء اختبار التكوين في FTD، إجراء اختبار التكوين في FTD، إجراء اختبار التكوين في FTD.

عم هسفن اقبس م كرتشم لاحتفم لانيوكت و 12 ةوطخلال يه اءاشنإ مت يتللة ةومم لال FTD(3.7) ةوطخلال يه هءاشنإ مت يذلل).

```
<#root>
```

```
tunnel-group 192.168.30.1 type ipsec-l2l  
tunnel-group 192.168.30.1 general-attributes  
  default-group-policy  
  
demo_gp_192.168.30.1
```

```
tunnel-group 192.168.30.1 ipsec-attributes  
  ikev2 remote-authentication pre-shared-key *****  
  ikev2 local-authentication pre-shared-key *****
```

ةءءراخللة ةهءاولا ىلع IKEv2 نيكمتب مق 14 ةوطخلال

```
crypto ikev2 enable outside
```

يرهاظ قفن ءاشنإ 15 ةوطخلال

```
<#root>
```

```
interface Tunnel1  
  nameif demovti_asa  
  ip address 169.254.10.2 255.255.255.0  
  tunnel source interface outside  
  tunnel destination 192.168.30.1  
  tunnel mode ipsec ipv4  
  tunnel protection ipsec profile  
  
demo_ipsec_profile
```

تبات راسم ءاشنإ 16 ةوطخلال

```
route demovti_asa 192.168.10.0 255.255.255.0 169.254.10.1 1  
route demovti_asa 192.168.20.0 255.255.255.0 169.254.10.1 1  
route outside 0.0.0.0 0.0.0.0 192.168.40.3 1
```

## ةءاصلال نم ققءءال

ءءءء لءءءب نانيوكتللا لمء ءءكأءل مسقللا اءه مءءءءسا

SSH وأمكنحتللا ةدحو ربع ASA و FTD بة صاخلا (CLI) رم أوألا رطس ةهجاو يلى لقتنا 1. ةوطخللا  
show crypto ikev2 sa لال خ نم 2 ةلحررمل او 1 ةلحررمل لل VPN ةكبش ةلاح نم ققحتلل  
gshow crypto ipSec .

FTD: جم انرب

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
ftdv742#
ftdv742# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
32157565 192.168.30.1/500 192.168.40.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/67986 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: 0x4cf55637/0xa493cc83
```

```
ftdv742# show crypto ipsec sa
interface: demovti
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.1
```

```
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: 192.168.40.1
```

```
#pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
#pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 30, #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
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 192.168.30.1/500, remote crypto endpt.: 192.168.40.1/500
path mtu 1500, ipsec overhead 94(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: A493CC83
current inbound spi : 4CF55637
```

```
inbound esp sas:
spi: 0x4CF55637 (1291146807)
SA State: active
transform: esp-aes-256 esp-sha-512-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, VTI, }
slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4055040/16867)
```

```
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
outbound esp sas:
spi: 0xA493CC83 (2761149571)
SA State: active
transform: esp-aes-256 esp-sha-512-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, VTI, }
slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4285440/16867)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

## ASA:

```
ASA9203# show crypto ikev2 sa
```

```
IKEv2 SAs:
```

```
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote
26025779 192.168.40.1/500 192.168.30.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/68112 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: 0xa493cc83/0x4cf55637
```

```
ASA9203#
```

```
ASA9203# show cry
```

```
ASA9203# show crypto ipsec sa
```

```
interface: demovti_asa
```

```
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.40.1
```

```
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: 192.168.30.1
```

```
#pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
#pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 30, #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
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 192.168.40.1/500, remote crypto endpt.: 192.168.30.1/500
path mtu 1500, ipsec overhead 94(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 4CF55637
```

current inbound spi : A493CC83

inbound esp sas:

spi: 0xA493CC83 (2761149571)

SA State: active

transform: esp-aes-256 esp-sha-512-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 (kB/sec): (4101120/16804)

IV size: 16 bytes

replay detection support: Y

Anti replay bitmap:

0x00000000 0x00000001

outbound esp sas:

spi: 0x4CF55637 (1291146807)

SA State: active

transform: esp-aes-256 esp-sha-512-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 (kB/sec): (4055040/16804)

IV size: 16 bytes

replay detection support: Y

Anti replay bitmap:

0x00000000 0x00000001

FTD على Global و VRF راسم نم ققحت 2. ةوطخا

ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN  
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, \* - candidate default, U - per-user static route  
o - ODR, P - periodic downloaded static route, + - replicated route  
SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is 192.168.30.3 to network 0.0.0.0

```
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C 169.254.10.0 255.255.255.0 is directly connected, demovti
L 169.254.10.1 255.255.255.255 is directly connected, demovti
SI 192.168.10.0 255.255.255.0 [1/0] is directly connected, inside_red
SI 192.168.20.0 255.255.255.0 [1/0] is directly connected, inside_blue
C 192.168.30.0 255.255.255.0 is directly connected, outside
L 192.168.30.1 255.255.255.255 is directly connected, outside
```

ftdv742# show route vrf vrf\_blue

Routing Table: vrf\_blue

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN  
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, \* - candidate default, U - per-user static route

```
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set
```

```
C      192.168.20.0 255.255.255.0 is directly connected, inside_blue
L      192.168.20.1 255.255.255.255 is directly connected, inside_blue
SI     192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti
```

```
ftdv742# show route vrf vrf_red
```

```
Routing Table: vrf_red
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set
```

```
C      192.168.10.0 255.255.255.0 is directly connected, inside_red
L      192.168.10.1 255.255.255.255 is directly connected, inside_red
SI     192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti
```

3. قوقحتال را بتخال لاصتال.

FTD. لى لى |encap|decap inc:هجاو | show crypto ipSec sa تادادع نم قوقحت، لاصتال را بتخال لبق

لزل او نيمضتال نم لكل ةمزح 30 ققفنال ضرعي، لاثمال اذ ي

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
    #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
ftdv742#
```

حاجن ب 3 Client1 لاصتال را بتخال ليمع

```
Client1#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/299/620 ms
```

حاجن ب 3 Client2 لاصتال را بتخال ليمع

```
Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/297/576 ms
```

لاصتال را بتخ | دع ب FTD ي ف inc:|encap|decap | show crypto ipsec sa | تاداع نم قحت حاجن ب.

حجان لاصتا را بتخ | دع ب لزعل او ني مضتال نم لكل ة مزح Tunnel1 40 ضرعي، لاثملا اذه ي ف لاصتال را بتخ | دص تا بل ط ق باطي امم، مزح 10 رادق م ب ني ددعلا الك داز، كلذى ل ة فاضال ابو IPSec. ق فن ربع حاجن ب ترم دق ping رورم ة كرح نأ ل ريشي امم، ة رشحعلا

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 40, #pkts encrypt: 40, #pkts digest: 40
    #pkts decaps: 40, #pkts decrypt: 40, #pkts verify: 40
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

## اه حالص او ااطخال ا فاشك تسا

اه حالص او ني وكتل ااطخال ا فاشك تسال اهم ادختسا | كنكمي تامولعم مسقلا اذه رفوي

م مسق VPN ل ا رحتي نأ رمأ طبضي نأ تلمعتسا عي طتسي تنأ

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug vti 255
```

اه حالص او راسملا مسق ااطخال ا فاشك تسال هذه ااطخال ا حي حصت رم او ا ادختسا | كنكمي

```
debug ip routing
```

## عجرملا

[7.4 رادصال، Cisco نم نم آل ا ة ي امحلا رادج زا هج ري دم ني وك ت ل ي ل د](#)

[Cisco Secure Firewall ASA VPN، 9.20 رم او آل ا رطس ة هج او ني وك ت ل ي ل د](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت  
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو  
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئى. ةصاغل مهتغب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىلإ أمئاد عوچرلاب يصوت وتامچرتل هذه ةقदन ةتيلوئسم Cisco  
Systems (رفوتم طبارلا) يلصلأل يزلچنلإل دن تسمل