

راسملا ىلإ ڈنتسملا VPN ڈکبش نیوکت ڈسواوب ڈرادملا FTD ىلع VRF ڈنتسملا FDM

تاي وتحمل

[قىدقملا](#)

[قىس اس آلاتابل طتملا](#)

[تابل طتملا](#)

[قىدخت سملاتانوكملا](#)

[قىس اس آتامولع](#)

[نيوكتلا](#)

[ڈكبس للى طختلامسىلا](#)

[نيوكت FTD](#)

[نيوكت ASA](#)

[قىحصلانم قىحتللا](#)

[اچالص او عاطخآل افاش كتسا](#)

[عجممل](#)

قىدقملا

عقوم ىلإ عقوم نم راسملا ىلإ ڈنتسملا VPN ڈکبش نیوکت ڈي فيك ڈنتسملا اذه حضوي ڈسواوب ڈرادملا FTD ىلع VRF ڈنتسملا FDM.

قىس اس آلاتابل طتملا

تابل طتملا

ۋەيىلاتلا عيىض او ملاب ڈفرعم كىدل نوكت نأب Cisco يىصوت:

- (VPN) ڈيرهاظلا ڈصالخا ڈكبس للى يس اس آلماھفللا
- (VRF) ھيچوتلا ڈداع او ڈيرهاظلا ھيچوت للى يس اس آلماھفللا
- ڈرادا ڈبرجت fdm

قىدخت سملاتانوكملا

ۋەيىلاتلا ڈي داملا تانوكملا وجماربلا تارادصى ىلإ ڈنتسملا اذه يف ڈرادا ڈتامولع ڈنتسمللا دنتسست:

- Cisco FTDv، 7.4.2
- Cisco FDM، 7.4.2
- Cisco ASA v 9.20.3

ةـصـاخـ ةـيـلـمـعـ ةـيـيـبـ يـفـ ةـدـوـجـوـمـلـاـ ةـزـهـجـأـلـاـ نـمـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ ءـاعـشـنـاـ مـتـ تـنـاـكـ اـذـاـ .(ـيـضـارـتـفـاـ)ـ حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـمـدـخـتـسـمـلـاـ ةـزـهـجـأـلـاـ عـيـمـجـ تـأـدـبـ رـمـأـ يـأـلـ لـمـتـحـمـلـاـ رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ ،ـلـيـغـشـتـلـاـ دـيـقـ كـتـكـبـشـ.

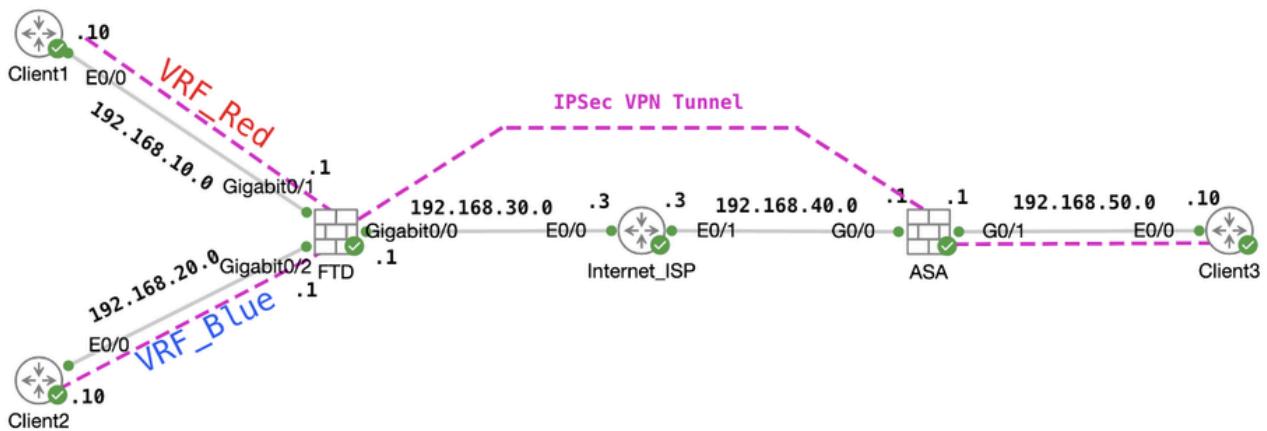
ةـيـسـاسـأـ تـامـوـلـعـمـ

ةـيـرـانـلـاـ ةـقـاطـلـاـ دـيـدـهـتـ نـعـ عـافـدـلـلـ دـحـاوـ زـاهـجـ لـعـ ةـلـوـزـعـمـلـاـ هـيـجـوـتـلـاـ تـالـيـثـمـ نـمـ دـيـدـعـلـاـ ءـاعـشـنـاـبـ لـوـدـجـبـ دـوـزـمـ لـصـفـنـمـ يـضـارـتـفـاـ هـجـوـمـكـ (ـVRFـ)ـ يـكـلـسـالـلـاـ دـدـرـتـلـاـ تـالـاـحـ نـمـ ةـلـاحـ لـكـ لـمـعـتـ .ـF~D~T~ رـفـوـيـوـ ةـكـبـشـلـاـ رـوـرـمـ ةـكـرـحـلـ يـقـطـنـمـلـاـ لـصـفـلـاـ ةـيـنـاـكـمـاـ حـيـتـيـ اـمـ ،ـبـ صـاخـلـاـ هـيـجـوـتـلـاـ تـاـنـاـيـبـلـاـ رـوـرـمـ ةـكـرـحـ ةـرـادـاـوـنـاـمـأـلـلـ ةـنـسـحـمـ تـاـنـاـكـمـاـ .ـ

ةـكـبـشـ دـجـوـتـ .ـM~A~D~X~T~S~A~B~ V~T~I~ .ـV~R~F~ مـاـدـخـت~س~ا~ب~ V~R~F~ ل~ ة~ك~ر~د~م~ل~ا~ ة~ي~و~ك~ت~ ة~ي~ف~ي~ك~ د~ن~ت~س~م~ل~ا~ ا~ذ~ه~ ح~ر~ش~ي~ ـص~ا~خ~ل~ا~ ء~ا~ر~م~ح~ل~ا~ ة~ك~ب~ش~ل~ا~ ي~ف~1~L~I~M~U~L~A~ ل~ص~ت~ي~ د~ق~ .ـF~T~D~ ف~ل~خ~ ء~ا~ق~ر~ز~ل~ا~ V~R~F~ ة~ك~ب~ش~ و~ ء~ا~ر~م~ح~ل~ا~ ق~ف~ن~ ل~ال~خ~ ن~م~ A~S~A~ F~L~X~ 3~L~I~M~U~L~A~P~ V~R~F~ B~L~U~E~ ل~و~ك~و~ت~و~ر~ب~ ي~ف~2~L~I~M~U~L~A~O~ V~R~F~ B~L~U~E~ ل~و~ك~و~ت~و~ر~ب~ ـI~P~S~E~ V~P~N~ .ـ

نـيـوـكـتـلـاـ

ةـكـبـشـلـلـ يـطـيـطـخـتـلـاـ مـسـرـلـاـ



طـطـخـمـلـاـ

نـيـوـكـتـ F~T~D~

لـكـشـبـ دـقـعـلـاـ نـيـبـ I~P~ لـاـصـتـاـلـ يـلـوـأـلـاـ نـيـوـكـتـلـاـ لـاـمـتـكـاـ نـمـ دـكـأـتـلـاـ يـرـوـرـضـلـاـ نـمـ .ـ1~.ـQ~W~E~X~ ـL~X~A~D~ مـع~3~L~I~M~U~L~A~ نـوـكـي~ .ـQ~A~W~E~R~F~D~ مـع~3~L~I~M~U~L~A~ نـوـكـي~ .ـQ~A~W~E~R~F~D~ مـع~3~L~I~M~U~L~A~ نـوـكـي~ .ـQ~A~W~E~R~F~D~

ةـيـمـوـسـرـلـاـ مـدـخـت~س~م~ل~ا~ ة~ه~ج~ا~و~ ل~و~خ~د~ ل~ي~ج~س~ت~ب~ م~ق~ .ـQ~A~W~E~R~F~D~ م~ق~ .ـ2~.ـQ~W~E~X~ ـL~X~A~D~ مـع~3~L~I~M~U~L~A~ نـو~ك~ي~ .ـQ~A~W~E~R~F~D~ مـع~3~L~I~M~U~L~A~ نـو~ك~ي~ .ـQ~A~W~E~R~F~D~ مـع~3~L~I~M~U~L~A~ نـو~ك~ي~ .ـQ~A~W~E~R~F~D~

Firewall Device Manager

Monitoring Policies Objects Device: ftdv742

Model Cisco Firepower Threat Defense for KVM Software 7.4.2-172 VDB 376.0 Intrusion Rule Update 20231011-1536 Cloud Services Connected | fangni High Availability Not Configured CONFIGURE

Inside Network

Cisco Firepower Threat Defense for KVM 0/2

0/0 0/1 0/2 0/3 0/4 0/5 0/6 0/7 MGMT CONSOLE

ISP/WAN/Gateway Internet DNS Server NTP Server Smart Lic...

Interfaces Management: Merged Enabled 4 of 9 View All Interfaces > Routing 6 static routes View Configuration > Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration > System Settings Management Access Logging Settings DHCP Server / Relay DDNS Service DNS Server

وأهلاً وآهلاً FTD_VIEW_INTERFACES

رزاً + قوف رقنا. يرهاظلا قفنلا تاهجاً وبتلا ٰـمـالـعـ قـوـفـ رـقـنـاـ 2.1ـ ـوـطـخـلـاـ.

Firewall Device Manager

Monitoring Policies Objects Device: ftdv742

Device Summary

Interfaces

Cisco Firepower Threat Defense for KVM 0/0 0/1 0/2 0/3 0/4 0/5 0/6 0/7 MGMT CONSOLE

Interfaces Virtual Tunnel Interfaces > 2 tunnels Filter +

FTD_Create_VTI

رزاً ok تقطق طـ ـمـزـالـلـاـ تـامـوـلـعـمـلـاـ رـيـفـوـتـ 2-2ـ ـوـطـخـلـاـ.

- يتـفـوـمـيـدـ مـسـالـاـ
- 1: قـفـنـلـاـ فـرـعـمـ
- (GigabitEthernet0/0) جـرـاخـ: قـفـنـلـاـ رـدـصـمـ
- 169.254.10.1/24: يـعـرـفـلـاـ ةـكـبـشـلـاـ عـانـقـوـ IPـ نـاـونـعـ
- حـاتـمـلـاـ عـضـوـمـلـاـ يـلـعـ قـلـزـنـمـلـاـ رـقـنـاـ ةـلـاحـلـاـ

Name **Status**

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

Description

Tunnel ID **Tunnel Source**

0 - 10413

IP Address and Subnet Mask

/

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

CANCEL **OK**

لیصافت FTD_Create_VTI_Details

نیوکتل اضرع رزلا قوف رقنا . عقوم ایلا عقوم نم VPN ڈکبش > زاچ ایلا لقتنا 3. ڈوٹخلا

Firewall Device Manager **Device: FTDv742** SECURE

Model Cisco Firepower Threat Defense for KVM Software 7.4.2-172 VDB 376.0 Intrusion Rule Update 20231011-1536 Cloud Services ⚠ Issues | Unknown High Availability Not Configured CONFIGURE

Interfaces Management: Merged Enabled 4 of 9 View All Interfaces

Smart License Registered Tier: FTDv50 - 10 Gbps View Configuration

Site-to-Site VPN There are no connections yet View Configuration

Routing 1 static route View Configuration

Backup and Restore View Configuration

Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration

Troubleshoot No files created yet REQUEST FILE TO BE CREATED

System Settings Management Access Logging Settings DHCP Server / Relay DDNS Service DNS Server Hostname Time Services SSL Settings See more

Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration

Device Administration Audit Events, Deployment History, Download Configuration View Configuration

FTD_SITE-to-SITE_VPN_VIEW_CONFIGURATION

نم لاصتا عاشنا رز لىع رقنا .عقوم ىلا عقوم نم ةديج VPN ةكبش عاشنا عدب .3.1. رز + قوف رقنا وأ .عقوم ىلا عقوم

The screenshot shows the 'Device Summary' section for a 'Site-to-Site VPN'. At the top, there are tabs for 'Monitoring', 'Policies', 'Objects', and 'Device: ftdv742'. The 'Device' tab is selected. On the right, there are icons for device status, logs, and help, along with the user 'admin' and role 'Administrator'. A green 'SECURE' badge is visible. Below the tabs, a message says 'There are no Site-to-Site connections yet.' followed by 'Start by creating the first Site-to-Site connection.' A prominent blue 'CREATE SITE-TO-SITE CONNECTION' button is centered, surrounded by a red box.

FTD_CREATE_SITE2SITE_CONNECTION

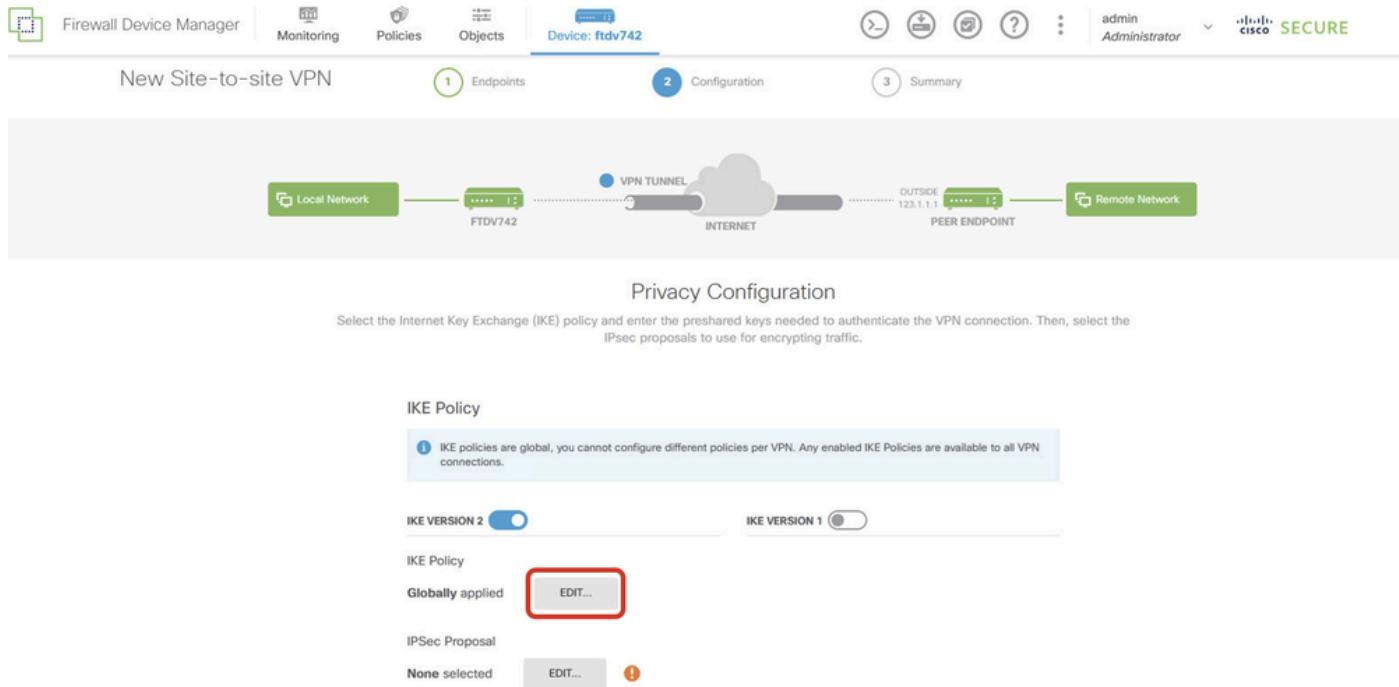
رز كلذ دعب تقطق ط .ةيرورضلا تامولعملاء ريفوت .3.2.

- يحييضوتلا ضرعلا :لاصتا فيرعت فلم مسا_S2S
- (VTI) راسملاء ىلا دنتسم :عونلما
- 2 ةوطخلاء يف اهؤاشناء مت) Demovti :ةيلحملاء VPN ةكبش ىلا لوصولا ٰهجا و
- ناونع جراخ ريظنلاء ASA واه) ديعبلا IP ناونع

The screenshot shows the 'New Site-to-site VPN' wizard at step 1, 'Endpoints'. The diagram illustrates a 'Local Network' connected via 'FTDV742' to a 'VPN TUNNEL' through the 'INTERNET', which connects to a 'PEER ENDPOINT' and a 'Remote Network'. Below the diagram, the 'Define Endpoints' section is shown. It includes fields for 'Connection Profile Name' (Demo_S2S), 'Type' (Route Based (VTI)), and 'Sites Configuration' for both 'LOCAL SITE' and 'REMOTE SITE'. The 'NEXT' button is highlighted with a red box at the bottom right.

FTD_SITE-to-SITE_VPN_ENDPOINTS

رز رحي تقطق ط IKE ءاسايسلإا لقتنا .3.3.



FTD_Edit_IKE_Policy

رقنلاب ديدج جهن عاشن! كنكمي وا اقبسم فرعم مادختس! كنكمي، IKE جهنل 3.4. ووطخل ا IKE جهن عاشن! قوف .

ظفحلل قفاصوم رزل ا قوف رقنا . IKE دوجوم AES-SHA ايس مسا ليدبت ، لاثمل ا اذه يف.

 Filter

AES-GCM-NUL-SHA



AES-SHA-SHA



DES-SHA-SHA

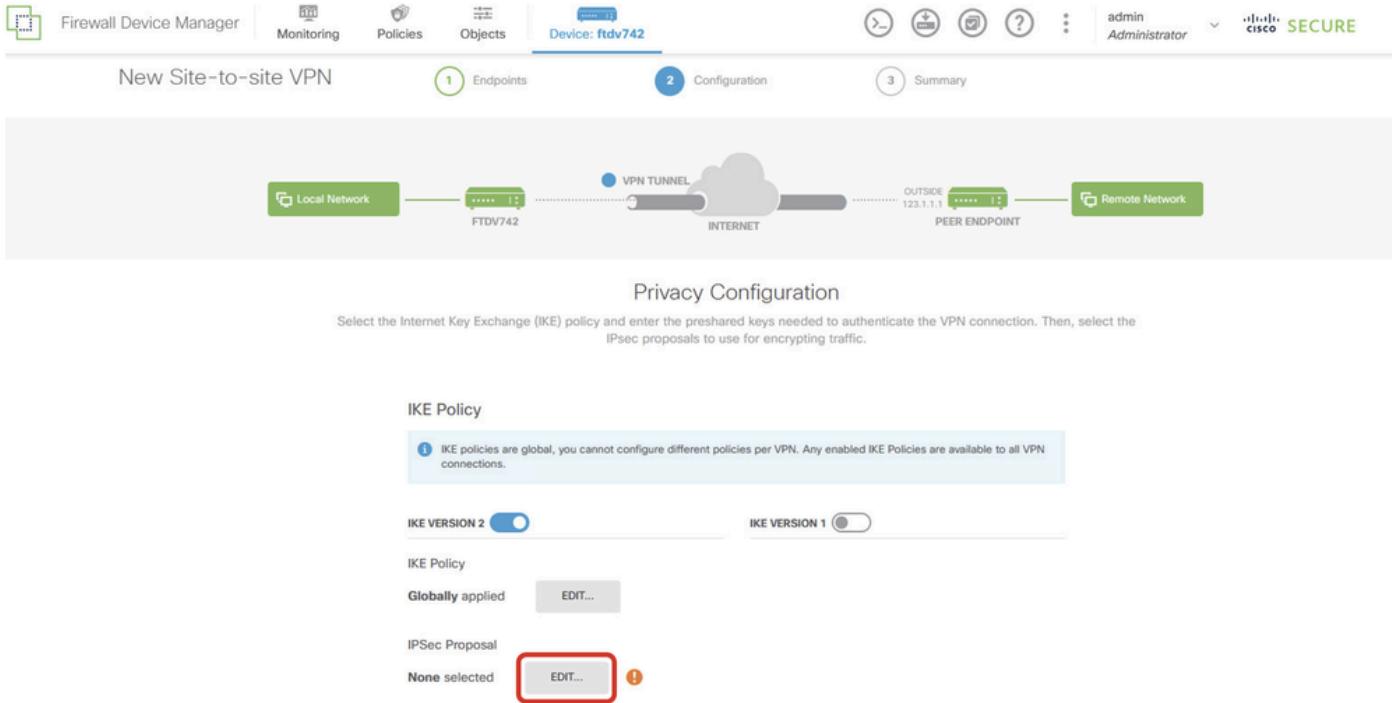


Create New IKE Policy

OK

FTD_ENABLE_IKE_POLICY

رژ رەھى ۋەقەطقەت حارتقا ئىلار قىتىندا 3.5. ۋەوطخلار.



FTD_Edit_IPSec_Proposal

حارتقا عاشن! كنكمي وأ اقبسم فرع مادختس! كنكمي IPSec حارتقال ئېسەنلاب 3.6. ۋوطخلا دىدج IPSec حرتقىم عاشن! قوف رقنىلا لالخ نم دىدج

ظفحلى رز قفاوم رقنا . IPSec دوجوملا حارتقا مسا لدب ، لاثملار اذىيە.

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

تقطقط . اقبسم كرتشملا حاتفملا نيوكتو وحفصلال فسل ريرم تلاب مق 3.7. ووطخلا رز كلذ دعب.

اقحال ASA ىلع هنيوكتو اقبسم كرتشملا حاتفملا اذه ظحالم عاجرلا.

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftv742 | FTDV742 | INTERNET | PEER ENDPOINT | admin Administrator | Cisco SECUR|

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

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 EDIT...

IPSec Proposal
Custom set selected EDIT...

Authentication Type
 Pre-shared Manual Key Certificate

Local Pre-shared Key

Remote Peer Pre-shared Key
*****@

BACK NEXT

FTD_CONFIGURE_PRE_SHARED_KEY

رزلـا قوف رقـنـا ،ليـدعـتـلـا إـلـا ـقـجـاحـبـ عـيـشـ يـأـ كـانـهـ نـاـكـ اـذـاـ VPNـ ـةـ كـبـشـ نـيـوـكـتـ عـجـارـ 3.8ـ ـةـ وـطـخـلـاـ رـزـلـاـ عـاهـنـاـ قـوـفـ رـقـنـاـ ،ـادـيـجـ عـيـشـ لـكـ نـاـكـ اـذـاـ .ـقـبـاسـلـاـ

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 Group: Null (not selected)

BACK **FINISH**

FTD REVIEW VPN CONFIGURATION

اذه يف FTD رب ع رورملا ةكرحل حامسلل لوصولاي ف مكحتلا ةدعاق ءاشناب مق. 3.9. 3 ووطخلما كب صاخلا جهنلا ليديعت عاجرلا. يحييضوتلا ضرعلا فدهب عيمجلل حامسلاب مق، لاثملما ئيلعفلما كتاجايتحا ىلا ادانتسا.

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

Default Action: Access Control Block

FTD_ACP_Example

نالك اذا FTD ئيلع ليعمل رورم ةكرحل NAT ءانثتسا ةدعاق نيوكتب مق (يرايتحا). 3.10. 3 ووطخلما

دجوت ال ، لاثمل ا اذه يف . تنرتن إلإ ىلإ لوصولل ليجعلل هنيوكت مث يكيمانيد NAT كانه
دجوت ال ، لاثمل ا اذه يف . تنرتن إلإ ىلإ لوصولل ليجعلل هنيوكت مث يكيمانيد NAT كانه
دجوت ال ، لاثمل ا اذه يف . تنرتن إلإ ىلإ لوصولل ليجعلل هنيوكت مث يكيمانيد NAT كانه

نيوكتلا تارييغت رشن . 3.11. ٤. ٥. ٦. ٧. ٨. ٩. ١٠. ١١.



ةيرهاظلا تاهجوملا نيوكت . 4. ٤. ٥. ٦. ٧. ٨. ٩. ١٠. ١١.

قفوف رقنا ، تاكبش < تانئاک ىلإ لقتنا . تباثلا راسملل ةكبش تانئاک عاشنإ . 4. ٤. ٥. ٦. ٧. ٨. ٩. ١٠. ١١.



FTD_Create_NetObjects

رجز ok تقطق ط . ةكبش نئاک لکل ةمزاللا تامولعملاريفوت . 4. ٤. ٥. ٦. ٧. ٨. ٩. ١٠. ١١.

- 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

- مسالا: 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::CD30::/60

CANCEL

OK

FTD_VRF_RED_Network

- مسالا: remote_192.168.50.0
- ةكبشلا: عونلا
- ةكبشلا: 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

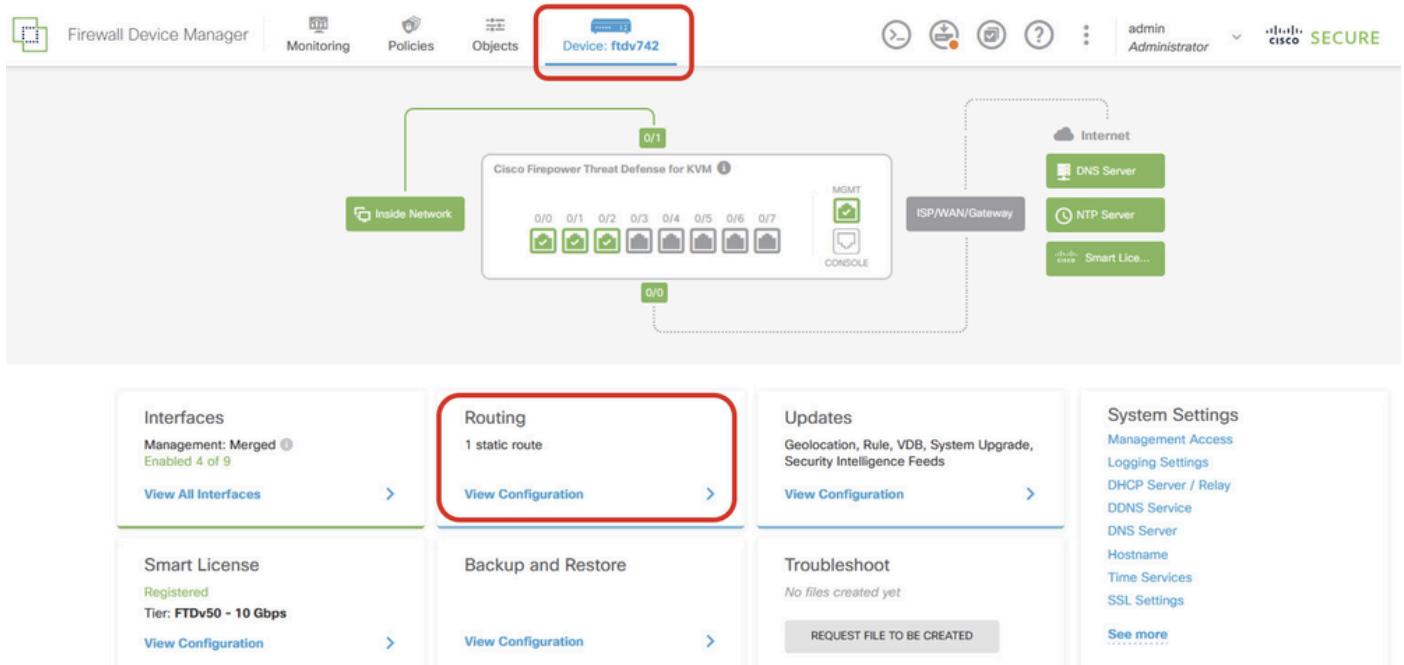
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

FTD_REMOTE_NETWORK

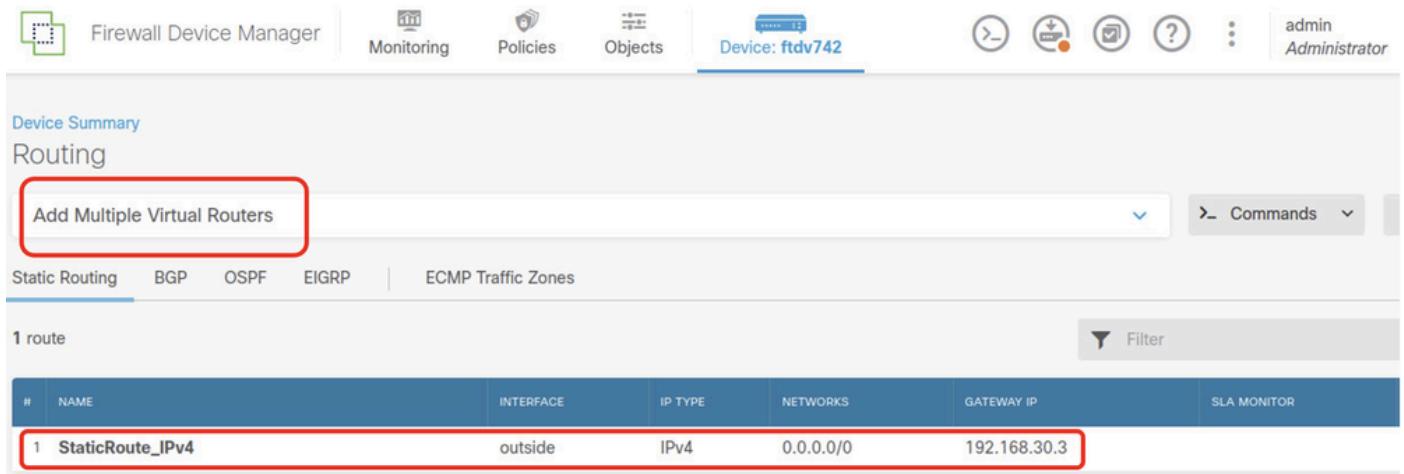
لیکشت ضرع ۋە قىطۇق طە . ھېجوتلى > زاھىجلا ئىلإ لىقتىنە . لە ولۇغا يەرھا ئۆزىلە جۇمۇلە ئاشنە 4.3. ۋە ئۆزىلە



FTD_VIEW_ROUTING_Configuration

ةيرهاظللا تاهجوملا نم ديدعل ا ةفاضا قوف رقنا . 4.4. ٥وطخل .

كيدل نكت مل اذا FDM. ٤.٥. ةيجهنلا ةانثأ ةيجراخلا ةهجاوللا لالخ نم تباث راسم نيكوت مت : ظحالم ايودي انهنيوكت ئجريف .



FTD_ADD_FIRST_VIRTUAL_ROUTER1

لواًلا صصخمللا يرهاظللا هجوملا عاشنإ قوف رقنا . 4.5. ٥وطخل .

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftv742 | admin Administrator

Device Summary

Routing

Virtual Route Forwarding (Virtual Routing) Description

You can create multiple virtual routing and forwarding instances, called virtual routers, to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device. Thus, you can provide support to two or more distinct customers over a common set of networking equipment. You can also use virtual routers to provide more separation for elements of your own network, for example, by isolating a development network from your general-purpose corporate network.

How Multiple Virtual Routers Work

Multiple Virtual Router mode is enabled automatically if there is at least one custom Virtual Router.

CREATE FIRST CUSTOM VIRTUAL ROUTER

FTD_ADD_FIRST_VIRTUAL_ROUTER2

جوملا عاشن دعب رز ok ۋە قىقىطى لە جوملە تامولۇملا رىفوت. 4.6. ۋە قىقىطى اىيئاقلت VRF لە ماسا ضرع مىتىس، لە ئەرەاظى.

- ماسالا: vrf_red
- تاهاجىدا: inside_red (GigabitEthernet0/1)

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftv742 | admin Administrator

Device Summary

Routing

Virtual Route Forwarding (Virtual Routing)

You can create multiple virtual routing and forwarding instances, called virtual routers, to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device. Thus, you can provide support to two or more distinct customers over a common set of networking equipment. You can also use virtual routers to provide more separation for elements of your own network, for example, by isolating a development network from your general-purpose corporate network.

How Multiple Virtual Routers Work

Multiple Virtual Router mode is enabled automatically if there is at least one custom Virtual Router.

CREATE FIRST CUSTOM VIRTUAL ROUTER

Add Virtual Router

Name: **vrf_red**

Description:

Interfaces:

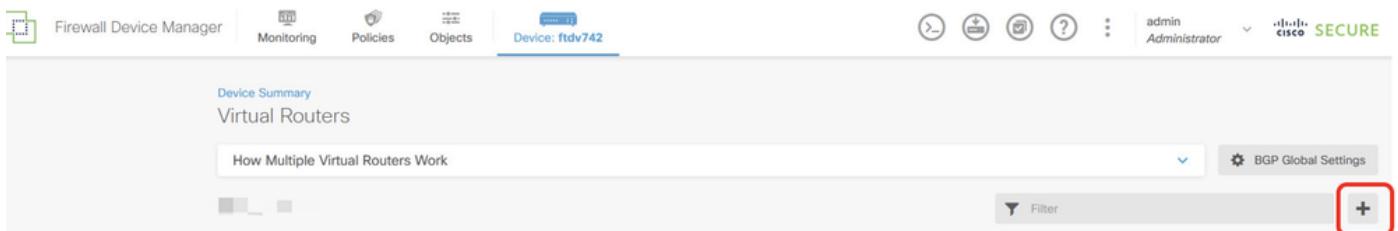
- + **inside_red (GigabitEthernet0/1)**

OK

FTD_ADD_FIRST_VIRTUAL_ROUTER3

لىكش ضرع ۋە قىقىطى . ھېجوتلىا > زاھىلە ئىلە لىقتىنە . نات يەرەاظە جوملا عاشناب مىق. 4.7. ۋە قىقىطى

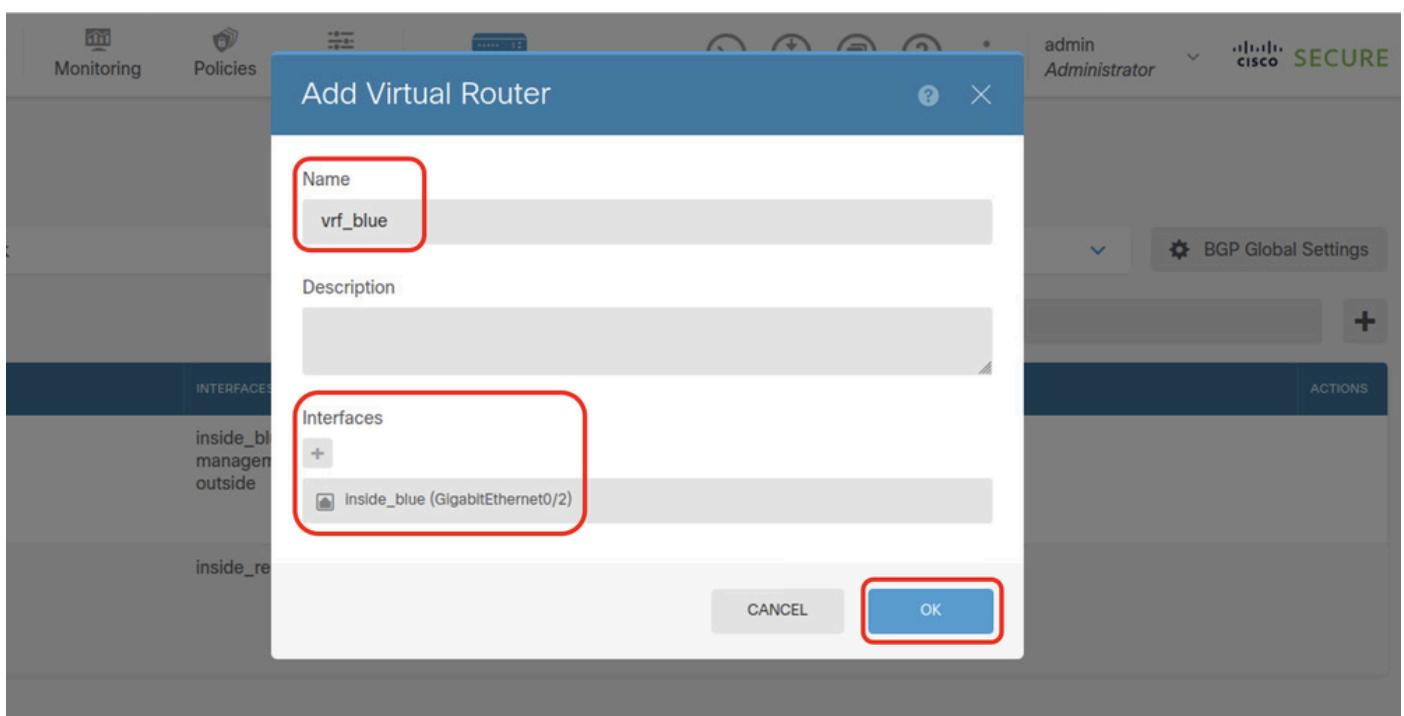
. رز + قوف رقنا.



جوجوملا FTD_Add_Second_Virtual_Router

قف اوم قوف رقنا . يناثلا يرهاظلا هجوملل ئامولعملاريفوتب مق 4.8. ۋەطخلا

- مسالا: vrf_blue
- تاهجولا: inside_blue (GigabitEthernet0/2)



FTD_ADD_SECOND_VIRTUAL_ROUTER2

ئياهنلا طاقنل راسملاده حيتى Global نم راسملابيرست ئىشنأ 5. ۋەطخلا ىلإ عقوم نم VPN قفن زايتج اهنأش نم يتلا تالاصتالا عدب 192.168.20.0/24 ۋە كېشلە ىلۇع 192.168.50.0/24. ۋە كېش ئيامحبا دىعبلالا ئياهنلا ئەطقن موقت، لاتىملا ليبس ىلۇع عقوم

ئيلخ يف ضرعلا زمر قوف رقنا . نيوكتلا ضرع قوف رقنا . هيچوتلا > زاهجلا ىلإ لقتنا vrf_blue يرهاظلا هجوملل ئارجىلا.

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	Edit View
3 vrf_red	inside_red	> Routes > IPv6 routes > BGP > OSPF	

FTD_VIEW_VRF_BLUE

رژ + قوف رقنا. تباث هیجوت بیوبتل ا ئممالع قوف رقنا. 5.1. ۋوطخل.

Device Summary / Virtual Routers
vrf_blue

How Multiple Virtual Routers Work

Virtual Router Properties | Static Routing BGP OSPF ECMP Traffic Zones

+

FTD_Create_STATIC_ROUTE_VRF_BLUE

رژ ok ۋقىطقىط. ئامولۇغا رىفوتب مق. 5.2. ۋوطخل.

- مسالا: Blue_toASA
- 1 قىفنلە: Demovti
- remote_192.168.50.0
- اغراف رىصنىعلا اذە كرتا: ئاباپلە.

Form fields highlighted with red boxes:

- Name: Blue_to ASA
- Interface: demovt1 (Tunnel1)
- Networks: remote_192.168.50.0
- OK button

Other form fields and labels:

- Description: (empty)
- Belongs to current Router: N/A
- Protocol: IPv4 (selected), IPv6
- Gateway: Please select a gateway
- Metric: 1
- SLA Monitor: Applicable only for IPv4 Protocol type
Please select an SLA Monitor
- CANCEL button

لیصافت FTD_Create_STATIC_ROUTE_VRF_BLUE_Details

قیاھنلا طاقنل راسمل اذھ حیتی. Global نم راسمل بیرسن یشنا 6. ۋوطخلى یللا عقوم نم VPN قفن زایتچا اهنأش نم یتللا تالاھىتالا عدب 192.168.10.0/24 ۋېبىشلا یللا

192.168.50.0/24. ئەكپش ئىامح ب ئەدىع بلا ئەياهنلا ئەطقن موقۇت ، لاثمەلە لىبىسلىع . عقۇم

ئەيلخ يىف ضرۇلۇ زىمر قوف رقنى . نىيوكىتلار ضرۇ قوف رقنى . ھىجوتلا > زاھىجلا لىلە لىقتىنالا vrf_red يىرەاظلە جۆمەللى تاءارجىلە.

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

FTD_VIEW_VRF_RED

رەز + قوف رقنى . تېباڭ ھىجوت بىيوبتىلا ئەم الاع قوف رقنى . 6.1. 6.2 ووطخلە.

Device Summary / Virtual Routers
vrf_red

How Multiple Virtual Routers Work

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

+ Filter

FTD_Create_STATIC_ROUTE_VRF_RED

رەز ok ۋە قەققەط . ۋە مزاىىلا تامولىع ملا رىفوت . 6-2 ووطخلە.

- مىسىلا: Red_to_ASA
- 1 قىفۇنلار: Demovti (1)
- remote_192.168.50.0
- اغراف رصىنۇلۇ اذە كرتا: ئەباوبىلا

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

ليصافت FTD_Create_STATIC_ROUTE_VRF_RED_Details

تاراسملـا حـمسـتو .ـيـضـارتـفـالـا ـلـا ـيـمـلـاعـلـا تـاهـجـوـمـلـا نـم رـاسـمـلـا بـيـرسـتـ عـاشـنـا 7ـ وـطـخـلـا عـقـومـلـا ـلـا عـقـومـلـا نـم VPNـ كـبـشـ نـم دـيـعـبـلـا فـرـطـلـا ـطـسـاوـبـ ـيـمـحـمـلـا ـيـاهـنـلـا طـاقـنـلـا

ئەگبىش ىلى لوصولاب VRF_RED يرەاظلا ھجوملا يف 192.168.10.0/24 و 192.168.20.0/24 يرەاظلا ھجوملا يف VRF_BLUE.

ةيلخ يف ضرعلا زمر قوف رقنا . نىيوكىلما ضرع قوف رقنا . هيچوتلا > زاھجلا ىلى لقتنا ماعلما يرەاظلا ھجوملل تاءارجىلما.

#	NAME	INTERFACES	SHOW/TROUBLESHOOT	ACTIONS
1	Global	management outside	>- Routes >- IPv6 routes >- BGP >- OSPF	
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 رقنا . تباڭ ھيچوت بىوبتلا ۋەممالۇ قوف رقنا . 7.1. ۋەطخىلما.

#	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 ۋەققىط . ۋەمزاڭلا تاموւىمىلا رىفوت 7-2. ۋەطخىلما.

- مسالا: S2S_leaks_blue
- ھەجىلما: inside_blue (GigabitEthernet0/2)
- local_blue_192.168.20.0
- اغراف رصىنۇلا اذه كرتا: ۋېاپلا

Global

Add Static Route



Name

S2S_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 traffic from this virtual router will leak into another virtual router. Proceed with caution.

Interface

inside_blue (GigabitEthernet0/2)

Belongs to different Router



vti_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
```

ىلع اهن يوكت مت يتلا تامىع ملسا فن ددھي يذلا IKEv2 IPsec حرتقم عاشناب مق. 10 ۋوطخلا 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 ۋوطخلا يف IPSec حرتقم عاشنامت عجرملا، فيرعت فلم عاشناء. 11 ۋوطخلا.

```
<#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
```

12 ۋوطخلا IKEv2 لوكوتوربب حمسەت ئەسايىس عاشناب مق.

```
<#root>

group-policy
demo_gp_192.168.30.1

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

13 ۋوطخلا FTD، رىظنلىلىخالا IP ناونىل قافنأ ئەسايىس عاشناب مق.

ع م هـ سـ فـ نـ اـ قـ بـ سـ مـ كـ رـ تـ شـ مـ لـ اـ حـ اـ تـ فـ مـ لـ اـ نـ يـ وـ كـ تـ وـ 12ـ ةـ وـ طـ خـ لـ اـ يـ فـ اـ هـ ؤـ اـ شـ نـ اـ مـ تـ يـ تـ لـ اـ ةـ عـ وـ مـ جـ مـ لـ اـ FTDـ (ـ 3.7ـ)ـ .

<#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 *****
```

ةـ يـ جـ رـ اـ خـ لـ اـ ةـ جـ اـ وـ لـ اـ اـ لـ عـ IKev2ـ نـ يـ كـ مـ تـ بـ مـ قـ .ـ 14ـ ةـ وـ طـ خـ لـ اـ .

```
crypto ikev2 enable outside
```

يـ رـ هـ اـ ظـ قـ فـ نـ عـ اـ شـ نـ اـ .ـ 15ـ ةـ وـ طـ خـ لـ اـ .

<#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
```

تـ بـ اـ ثـ رـ اـ سـ مـ عـ اـ شـ نـ اـ .ـ 16ـ ةـ وـ طـ خـ لـ اـ .

```
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
```

ةـ حـ صـ لـ اـ نـ مـ قـ قـ حـ تـ لـ اـ

حـ يـ حـ صـ لـ كـ شـ بـ نـ يـ وـ كـ تـ لـ اـ لـ مـ عـ دـ يـ كـ أـ تـ لـ مـ سـ قـ لـ اـ اـ ذـ هـ مـ دـ خـ تـ سـ اـ .

وأـ SSH مـ كـ حـ تـ لـ اـ ةـ دـ حـ وـ رـ بـ عـ وـ FTD بـ ظـ اـ خـ لـ اـ (CLI) رـ مـ اوـ الـ اـ رـ طـ سـ ةـ جـ اوـ الـ اـ لـ قـ تـ نـ اـ 1ـ ةـ وـ طـ خـ لـ اـ

show crypto ikev2 sa
show crypto ipsec

جـ اـ نـ ربـ FTD:

```
> 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

```

٢. وظائف FTD. و Global عجلات VRF و راسم نم قيقحت.

```

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
```

لاصتالا رابتخا نم ققحتلا 3. ۋوطخلما.

تادادع نم ققحت، لاصتالا رابتخا لبقل جاو | show crypto ipsec sa | inc:|encap|decap ىلع FTD.

لزعلاو نيمضتلا نم لكل 30 ىقفنلار ضرعى، لاثملما اذه يف.

```
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#
```

حاجنب لاصتالا رابتخا Client1 3 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
```

حاجنب لاصتالا رابتخا Client2 3 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

```

لاصتالا رابتخا دعب FTD يف تادادع نم ققحت حاجنب show crypto ipsec sa | inc:|encap|decap

حجان لاصتا رابتخا دعب لزعلاو نيمضتلا نم لك كل ٤٠ ضرعى، لاثمل اذه يف
لاصتالا رابتخا يدىص تابلط قباطي امم، مزح ١٠ رادقمب نيددعلا الک داز، كلذ لىا ٤٠ فاضالاب و
قفن رب ع حاجنب ترم دق ping رورم ٤٠ كرخ نأ لىا ريشي امم، ٤٠ رشع علما IPSec.

```

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

```

اهالص او عاطخآل ا فاشكتسال

اهالص او نيوكتل ا عاطخاؤ فاشكتسال اهم ادختسال كنكمي تامولعم مسقل اذه رفوي

مسق VPN لايحتي نأ رمأ طبضي نأ تلمعتسا عيطة سى تنا

```

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

```

اهالص او راسمل ا مسق عاطخاؤ فاشكتسال هذه عاطخآل ا حيحصت رم اوأ مادختسال كنكمي

```
debug ip routing
```

عجملا

[7.4 رادصالا Cisco نم نمآل اقيام حلارادج زاهج ريدم نيوكت ليلىد](#)

[Cisco Secure Firewall ASA VPN, 9.20 رم اوأ لارطس ٤٥٥ جاو نيوكت ليلىد](#)

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).