

ةجودزمل ةطشنل VPN ةكبش نيوكت
 عم عقوم لىل عقوم نم راسمل لىل ةدنتسمل
 FDM ةطساوب ةرادل FTD لىل PBR

تایوت حملہ

ةمدقملا

ةيساس ألاتابلطتملا

تابل طتملا

قمدخت سملاتانوكملا

قياس أساساً تامولعم

نى وكىتلا

عكې شىللى طىختىلا مىسىرلا

VPN ەكېشىلىغان ئىكەنلىكىنى تەكشۈرۈش

Site1 FTD VPN نیوكت

Site2 FTD VPN نیوكت

PBR ىلە تاننىۋىكتا

[Site1 FTD پ صا خ ل ا PBR ن ی و ک ت](#)

Site2 FTD ب ص ا خ ل ا PBR نی و ک ت

SLA ۋە شەرتلەر ئىشلىتىلىش

SLA ل SITE1 FTD ب قارم نى وكت

SITE2 FTD ل SLA ة بقارم نىوكت

تبادل اساسىلىق تاننىكتا

[SITE1 FTD ل تباثلا راسملا نىوكت](#)

[SITE2 FTD ل تباثلا راسملا نىوكت](#)

ةحصلا نم ققحتلا

دیجیٹل کتب خانہ کے لیے

VPN

قیرط

SLA ةشاش

غنی پ راپ ت خا

دیج وحن یل ل ISP2 لمع انا ثأ ة عطاق م ISP1 هجاوی

VPN

قیرط

SLA ةشاش

غنی پ رابت خا

دیجیٹل کتب خانہ ISP1 کے ساتھ علاقہ ISP2 کے ساتھ

VPN

قیرط

SLA ةشاش

غنی ب راب ت خا

اهـ حال صراو عاط خأل ا فاشك تسرا

مقدم

راسم الى دنتسملا ةجودزملا ةطشنل VPN ةكبش نيوكت ةيفيك دنتسملا اذه حضوي
FDM ةطساوب اهترادإ متت يتل FTD يلع PBR مادختساب عقوم يلع عقوم نم

ةيساسال تابلطتملا

تابلطتملا

ةيلالتل عيضاوملاب ةفرعم كيذل نوكت ناب Cisco ي صوت

- (VPN) ةيرهاظلا ةصاخلا ةكبشلل يساسال مهفل
- (PBR) ةسايسلا يلع مئاقلا هيچوتلل يساسال مهفل
- (IP SLA) تنرتنإلا لوكوتورب ةمدخ يوتسم ةيقافتال يساسال مهفل
- fdm ةرادإ ةبرجت

ةمدختسملا تانوكملا

ةيلالتل ةيداملا تانوكملا وجماربال تارادصل الى دنتسملا اذه يف ةدراول تامولعمل دنتست

- Cisco FTDv، رادصلإ 7.4.2
- Cisco FDM، رادصلإ 7.4.2

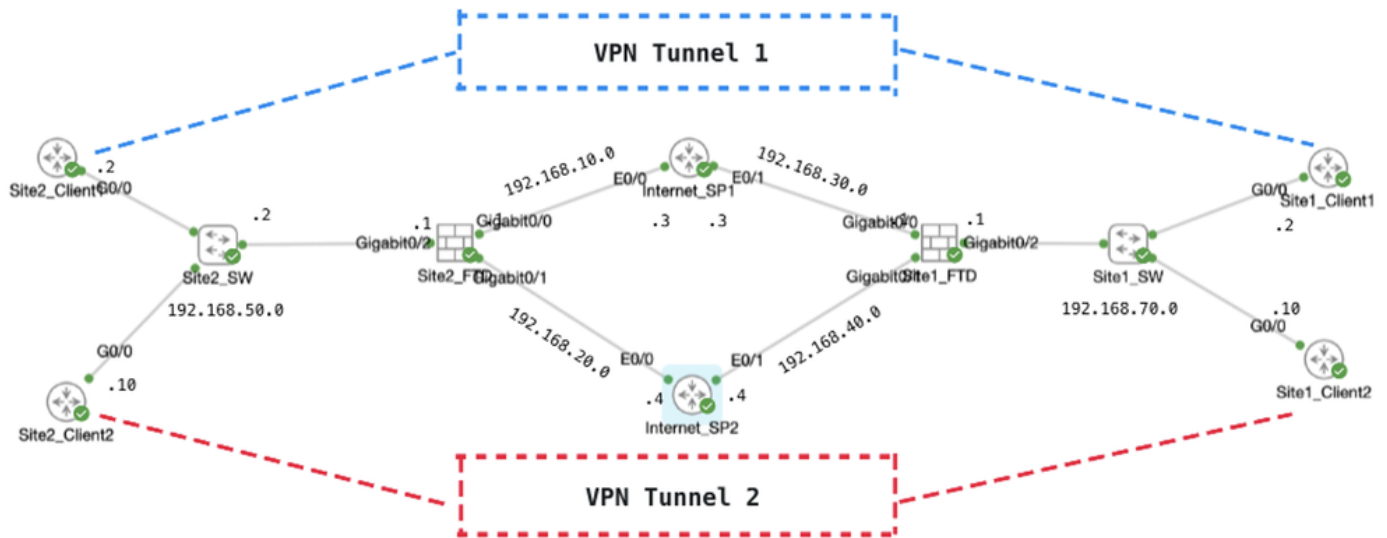
ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دنتسملا اذه يف ةدراول تامولعمل عاشنإ مت
تناك اذإ. (يضايرتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجال عيجمج تأدب
رمأ يأل لمحتحمل ريثأتلل كمهف نم دكأتف، ليغشتل ديقتك كبش

ةيساسا تامولعمل

عقوم نم راسم الى دنتسم ةجودزم ةطشن VPN ةكبش نيوكت ةيفيك دنتسملا اذه حرشي
تالاصتإ 2 عقوملاو 1 عقوملا نم لك يف FTDs نمضتت، لاثملا اذه يف FTD يلع عقوم الى
يوزم نم لك عم عقوم الى عقوم نم (VPN) ةيرهاظ ةصاخ ةكبش عاشنإل ةجودزم ةطشن ISP
ISP1 ربع 1 قفنل VPN رورم ةكرح ربعت، يضايرتفا لكشب. دحاو نأ يف (ISPs) تنرتنإلا ةمدخ
ISP2 ربع 2 قفنل ربع رورملا ةكرح رمت، نيددحمل نييفيضم لل ةبسنلاب. (قرزال طخلال)
ISP2 الى تانايبلا رورم ةكرح ليديتبت موقيسف، ةعطاقم نم ISP1 ىناع اذإ. (رمحال طخلال)
الى تانايبلا لقن كيلاعف، ةعطاقم ISP2 تهجاو اذإ، كلذ نم سكعلال يلعو. يطايرتفا خسنك
(PBR) ةسايسلا الى دنتسملا هيچوتلا مادختسا متي. يطايرتفا خسن ةيلمعك ISP1
هذهب عافولل لاثملا اذه يف (IP SLA) تنرتنإلا لوكوتورب ةمدخ يوتسم ةيقافتاو
تابلطتملا.

نيوكتلا

ةكبشلل يطيختل مسرلا



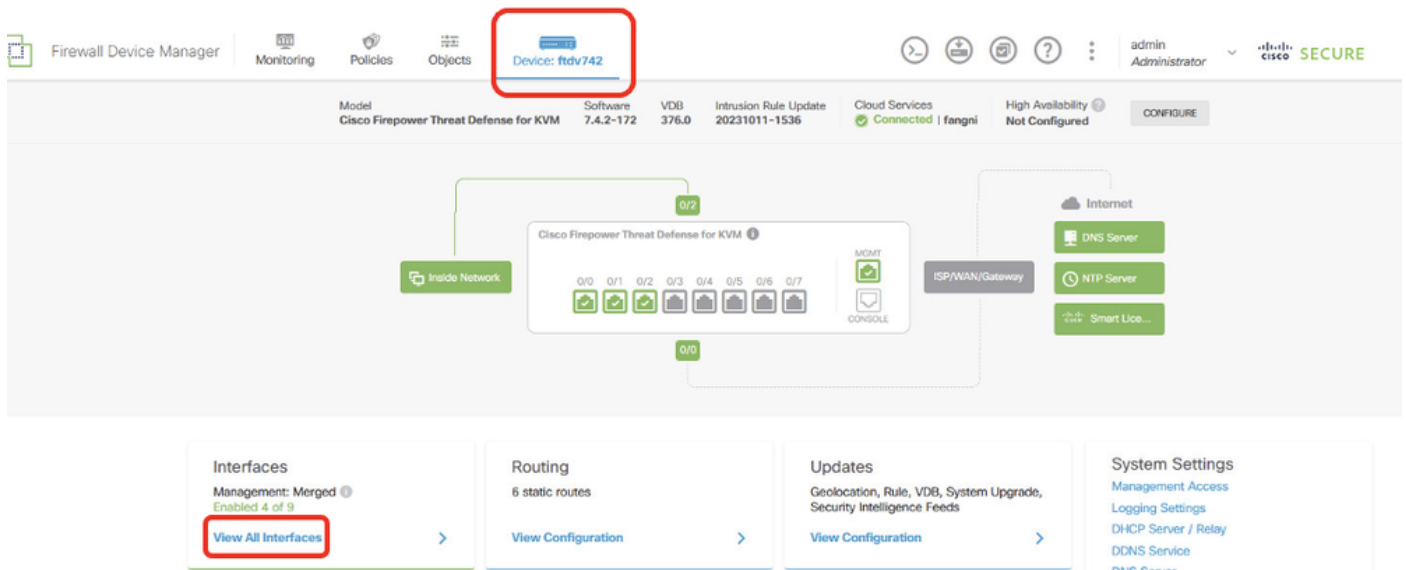
ططخم ل

VPN ةكبش ىل ع تانيوكت ل

ل كشب دق ع ل نيب ينيب ل IP لاصتال يلوأ ل نيوكت ل لامتكا نم دكأت ل يرورض ل نم قئاف ل اسر ل اجمانرب" ي ف دوچوم ل IP ناو ن ع م Site1 و Site2 نم لك ي ف االم ع ل نوكي .حي حص ةب اوبك " (FTD) ة ع ر س ل ل

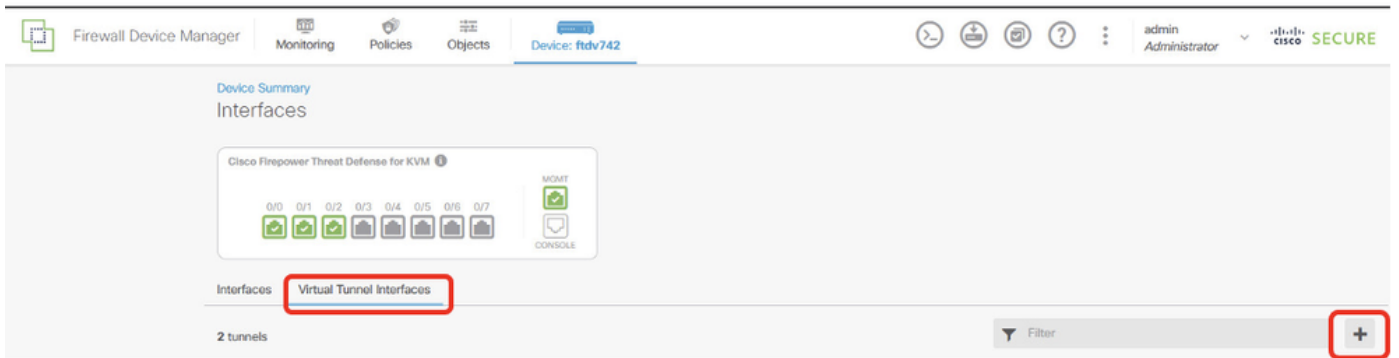
Site1 FTD VPN نيوكت

ةه ا و ل ل لوخ د ل ليج س ت ب مق . ISP1 و ISP2 ل ةيره اظ ل ق ف ن ل تاه ا و اءاش ن اب مق 1. ةوطخ ل ضر ع ق و ف ر ق ن ا . تاه ا و ا و ل > زاه ا ل ل ل ق ت ن ا . Site1 FTD ل FDM ل (GUI) ةي م و س ر ل م د خ ت س م ل تاه ا و ا و ل ع ي م ج



Site1FTD_VIEW_ALL_Interfaces

+ ر ز ل ق و ف م ث يره اظ ل ق ف ن ل تاه ا و ا ب ي و ب ت ل ة م ا ل ع ق و ف ر ق ن ا 2. ةوطخ ل



Site1FTD_Create_VTI

رر. ok تقطوط. VTI لي صافات لوح ةروررضلا تامولعمل ري فوتب مق. 3 ةوطخل

- يتفوميد: مسالا
- ققننل فرعم: 1
- جراخ: ققننل ردصم (GigabitEthernet0/0)
- ةيعرفلل ةكبشلل عانقو IP ناونع: 169.254.10.1/24
- حاتمالم عوضومال لعل ققننل رقنا: ةلحال

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

site1FTD_VTI_Details_Tunnel1_ISP1

- مسالا: demovti_sp2
- ققننل فرعم: 2

- حارة الة عؤوم الة ع قلع قلع زنع الة رقنا :ةالال
- ةعرف الة ةكبش الة عانق و IP ناونع : 169.254.20.11/24
- حارة الة عؤوم الة ع قلع قلع زنع الة رقنا :ةالال

Name

demovti_sp2

Status

☒

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

Description

Tunnel ID ⓘ

2

Tunnel Source ⓘ

outside2 (GigabitEthernet0/1) ▼

0 - 10413

IP Address and Subnet Mask

169.254.20.11 / 24

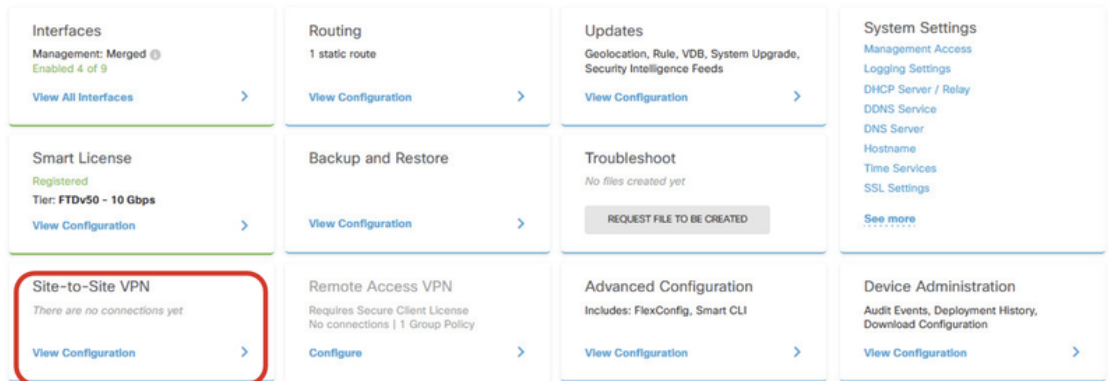
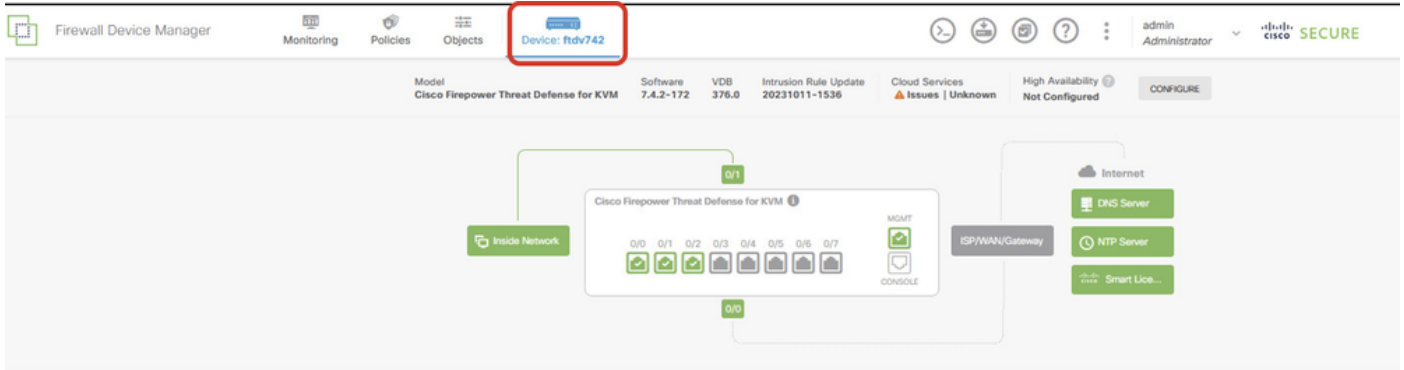
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

CANCEL

OK

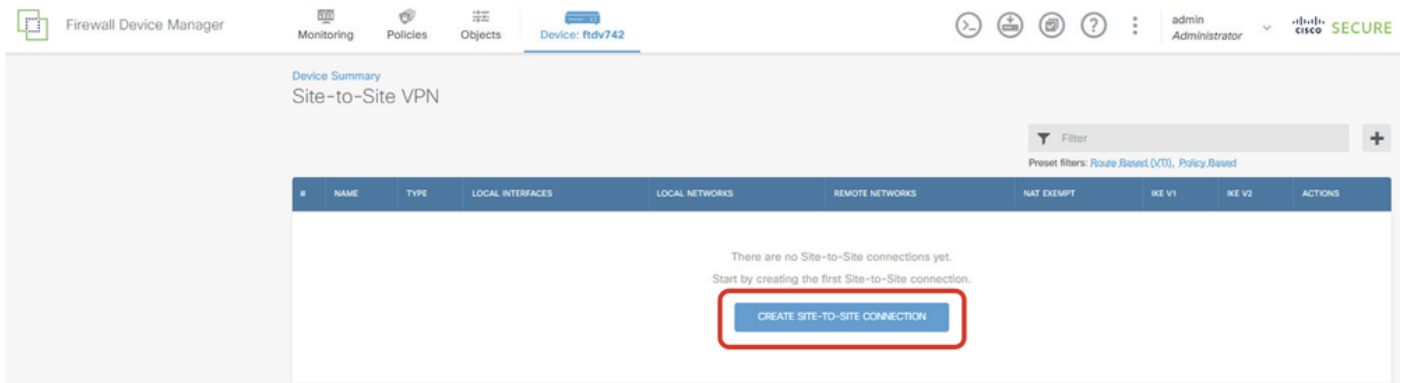
site1FTD_VTI_Details_Tunnel2_ISP2

رز لة كشت ضرع ةق طقط . ع قوم الة ع قوم نم VPN ةكبش > زاهج الة لقتنا . 4 ةوطخال



Site1FTD_VIEW_SITE2Site_VPN

قوف رقنا 1. ISP لال خ نم عقوم ىلإ عقوم نم ةديج VPN ةكبش عاشنإ يف أدبا 5. ةوطخل رزلا قوف رقنا وأ ،عقوم ىلإ عقوم نم لاصتا عاشنإ +.



Site1FTD_Create_site-to-site_Connection

رز كلذ دعب تقطقط .ةياهنلا طاقن نع ةمزاللا تامولعمل ريفوت - 5-1 ةوطخل

- S2S_يحيضوتلا ضرعلا :لاصتالا فيرعت فلم مسا
- (VTI) راسملا ىلإ دنتسم :عونلا
- (3. ةوطخلال يف اهؤاشنإ مت) demovti :ةيحمل VPN ةكبش ىلإ لوصولا ةهجاو
- (1. ISP Site2 FTD ل IP ناونع وه اذه) 192.168.10.1 :ديعبلا IP ناونع

New Site-to-site VPN

1 Endpoints

2 Configuration

3 Summary



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: **Demo_S2S** Type: **Route Based (VTI)** Policy Based

Sites Configuration

LOCAL SITE

Local VPN Access Interface: **demovti (Tunnel1)**

REMOTE SITE

Remote IP Address: **192.168.10.1**

CANCEL NEXT

site1FTD_ISP1_site-to-site_VPN_Define_Endpoints

رز ررحي ةق طوط IKE ةسايس ل لقتنا 5.2 ةوطخل

Firewall Device Manager Monitoring Policies Objects Device: ftdv742

New Site-to-site VPN 1 Endpoints 2 Configuration 3 Summary

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

EDIT...

IPSec Proposal

None selected

EDIT...

Site1FTD_Edit_IKE_Policy

رقن لاب دي دج چن عاشن كن كمى و اق بسم فرعم مادختس كن كمى، IKE چنل 5.3 ةوطخل
دي دج IKE چن عاشن قوف

عاشن اب اضي مقو AES-SHA ةي لالحل IKE ةسايس ني ب لي دب تلاب مق، لاثملا اذه ي
تذقن in order to رز ok ةق طوط .يحيضوتل ضرعل ضرغب ةدي دج ةسايس

- اسم السال: AES256_DH14_SHA256_SHA256
- AES256 راي عم، روطت السال راي عم: ريفش السال
- DH: 14 ةومجم
- 256 م.أ: لملكت السال ةئجت
- 256 م.أ: PRF ةئجت
- 86400 رملع السال (الضارثال)

The image shows the 'Add IKE v2 Policy' configuration window. On the left, a list of policies is shown with 'AES-SHA-SHA' selected. A red box highlights this selection. A red arrow points from this selection to the 'Add IKE v2 Policy' window on the right. The right window shows the configuration for the selected policy. Red boxes highlight the following fields: Priority (1), Name (AES256_DH14_SHA256_SHA256), State (enabled), Encryption (AES, AES256), Diffie-Hellman Group (14), Integrity Hash (SHA, SHA256), Pseudo Random Function (PRF) Hash (SHA, SHA256), and Lifetime (86400 seconds). The 'Create New IKE Policy' button is also highlighted with a red box.

Site1FTD_Add_New_IKE_Policy

Filter

AES-GCM-NULL-SHA

i

AES-SHA-SHA

i

DES-SHA-SHA

i

AES256_DH14_SHA256_SHA256

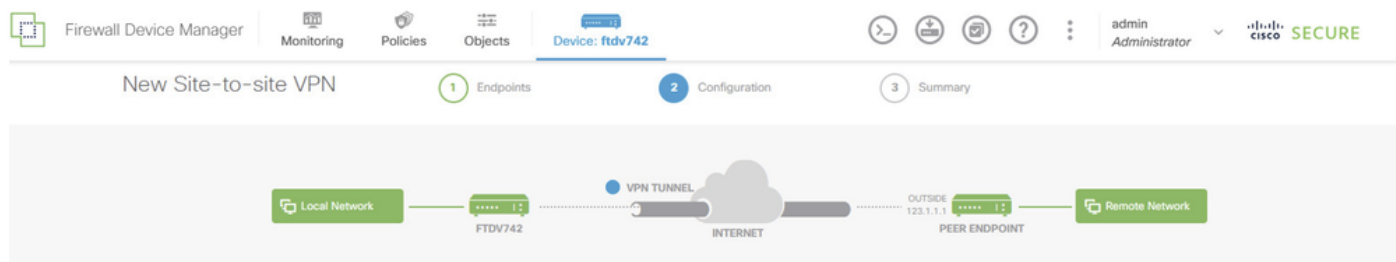
i

Create New IKE Policy

OK

site1FTD_ENABLE_NEW_IKE_POLICY

رز ررحې ةق طقط IPSec حارتقا ىلإ لقتنا 5.4 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

EDIT...

IPSec Proposal

None selected

EDIT...

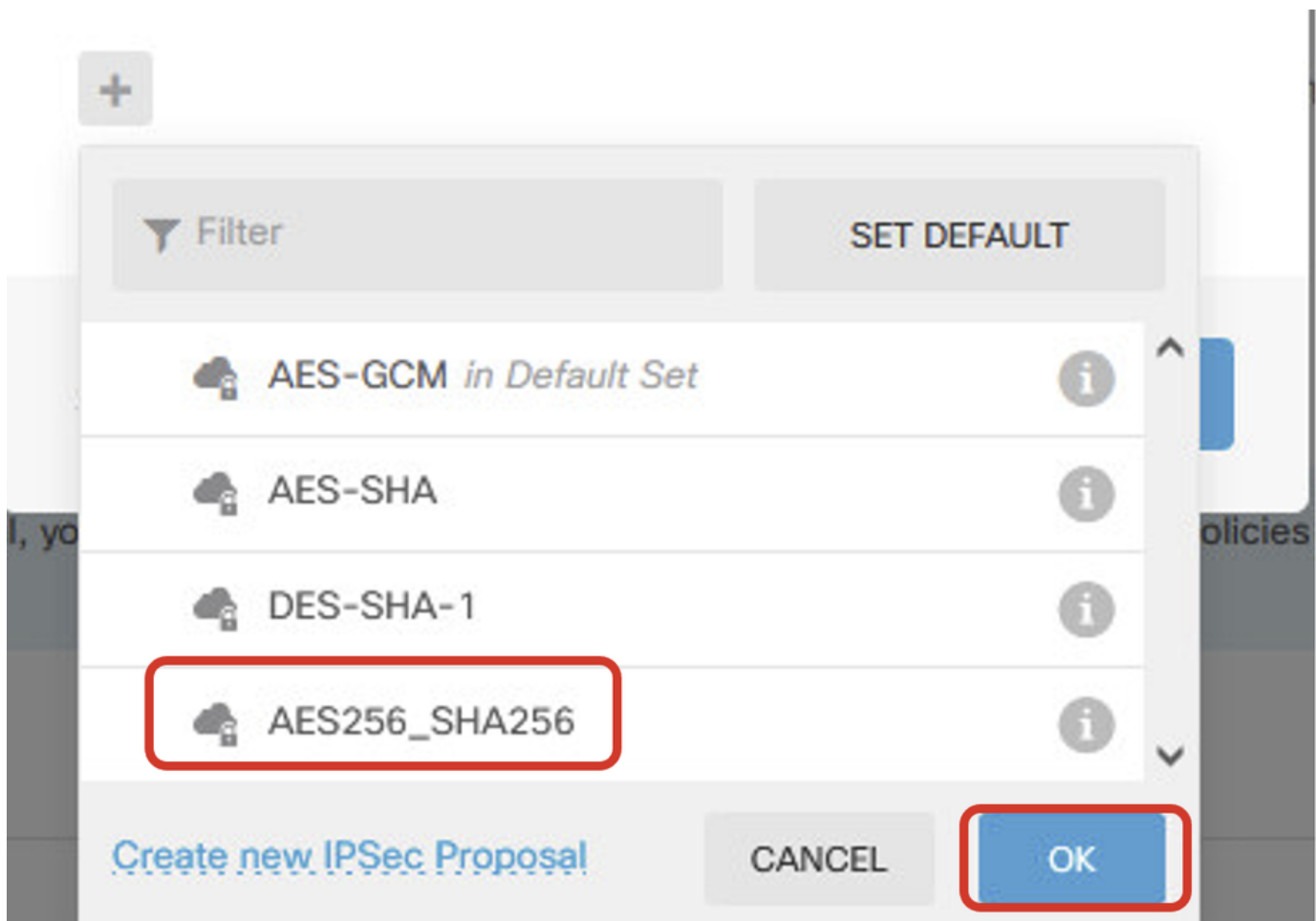


Site1FTD_Edit_IKE_Proposal

حارث قا عاشن إ كنكمي وأ اق بسم فرعم مادختس إ كنكمي، IPsec حارث قال ةبسنن لآب 5.5 ةوطخل دي دج لآثم عاشن إ ب مق، لآثمل اذه ي. دي دج IPsec حارث قم عاشن إ قوف رقنن لآلخ نم دي دج تذنقنأ in order to رز ok ةق طقط. يحيضوتل ضرعل ضرغل

- م سالا: AES256_SHA256
- AES256 راي عم، روطتمل ريفشتل راي عم: ريفشتل
- SHA1، SHA256 لملكتل ةئجت

Site1FTD_Add_New_IKE_Proposal



Site1FTD_ENABLE_NEW_IKE_Proposal

رزل قوف رونا .اقبس م كرتشم الحاتفم لنيوكتب مقو ءحفصل الى قلزنا .5.6 ءوطخل اللات.

اقحال Site2 FTD الى ع هنيوكتب مقو اقبس م كرتشم الحاتفم اذ طحال

Firewall Device Manager

Monitoring Policies Objects **Device: ftdv742**

FTDV742 INTERNET PEER ENDPOINT

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

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 **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**

Site1FTD_CONFIGURE_PRE_SHARED_Key

رز قوف رقنا ،ليدعتلل جاتحي عيش ي ا كانه ناك اذ . VPN ةكبش نيوكت عجار . 5.7 ةوطخل
 "ءاهن رزلا قوف رقنا ،ادي ج عيش لك ناك اذ . فلخل

Demo_S2S Connection Profile

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

VPN Access
Interface

 demovti (169.254.10.1)



Peer IP Address

192.168.10.1

IKE V2

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

IPSec Proposal aes,aes-256-sha-1,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 Null (not selected)

i 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

site1FTD_ISP1_REVIEW_VPN_Config_Summary

ISP2. لالځ نم عقوم ىلا عقوم نم ةديج VPN ةكبش عاشنإ لجأ نم 5. ةوطخلا ررك 6. ةوطخلا

Demo_S2S_SP2 Connection Profile

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

VPN Access
Interface

demovti_sp2 (169.254.20.11)



Peer IP Address

192.168.20.1

IKE V2

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

IPSec Proposal aes,aes-256-sha-1,sha-256

Authentication Type Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration 28800 seconds

Lifetime Size 4608000 kilobytes

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)

BACK

FINISH

site1FTD_ISP2_REVIEW_VPN_Config_Summary

اذا في FTD ربع رورم الة كرحل حامس لل لوصولو في مكحت الة دعاق عاشن اب مق 7. ووطخل ك صاخل جهنن ل ليدعتب مق .يحيضوت ال ضرع ال فدهب عي مجلل حامس ل اب مق ،ل اثل م الة لعل ف ال ك انا ايتح اى ال انا تس ا.

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

Security Policies

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

Default Action Access Control Block

Site1FTD_ALLOW_ACCESS_CONTROL_RULE_EXAMPLE

ناك اذا FTD لى لى م عمل رورم الة كرحل NAT انا تس ا دعاق ني وكتب مق (ي رايتخا). 8. ووطخل

ت.نرتنإلا ىلإ لوصولا لجأ نم ليعملل هنيوكت مت يكيمايدي NAT كانه

ىلإ لوصولا لجأ نم عالعملل يكيمايدي NAT هنيوكت متي ،يحيضوتال ضرعلا فدهل NAT. انثتسا ةدعاق دوجو مزلي كلذل .لاثمال اذه ي ف ت نرتنإلا

ق.فاوم قوف رقاو ليصافتلا ريفوتب مق .رز + قوف رقا . NAT > تاسايسلا ىلإ لقنتا

- NAT ءافعإ :ناونعلا
- ةيئاقلتلا NAT دعاقو لبق :عضولا
- تباث :عونلا
- لخاد :ردصملا ةهجاو
- يا :ةهجولا
- 192.168.70.0/24 :يلصلأال ردصملا ناونع
- 192.168.70.0/24 :مچرتملا ردصملا ناونع
- 192.168.50.0/24 :ةيلصلأال ةهجولا ناونع
- 192.168.50.0/24 :ناونع ةياغ ةمچرت
- راسملا نع ثحبلل نيكمتم عم

The screenshot shows the 'Add NAT Rule' dialog box in the Cisco Firewall Device Manager. The dialog is titled 'Add NAT Rule' and has a close button (X) in the top right corner. It contains several sections and fields:

- Title:** 'NAT Exempt' (highlighted with a red box).
- Create Rule for:** 'Manual NAT' (dropdown menu).
- Status:** A toggle switch that is turned on (highlighted with a red box).
- Placement:** 'Before Auto NAT Rules' (dropdown menu, highlighted with a red box).
- Type:** 'Static' (dropdown menu, highlighted with a red box).
- Packet Translation:** This section is divided into 'ORIGINAL PACKET' and 'TRANSLATED PACKET'.
 - ORIGINAL PACKET:**
 - Source Interface:** 'inside' (dropdown menu, highlighted with a red box).
 - Source Address:** 'inside_192.168.70' (dropdown menu, highlighted with a red box).
 - Source Port:** 'Any' (dropdown menu).
 - Destination Address:** 'peer_192.168.50.0' (dropdown menu, highlighted with a red box).
 - Destination Port:** 'Any' (dropdown menu).
 - TRANSLATED PACKET:**
 - Destination Interface:** 'Any' (dropdown menu, highlighted with a red box).
 - Source Address:** 'inside_192.168.70' (dropdown menu, highlighted with a red box).
 - Source Port:** 'Any' (dropdown menu).
 - Destination Address:** 'peer_192.168.50.0' (dropdown menu, highlighted with a red box).
 - Destination Port:** 'Any' (dropdown menu).
- Show Diagram:** A toggle switch that is turned off.
- Buttons:** 'CANCEL' and 'OK' (highlighted with a red box).

Site1FTD_NAT_EXEMPT_RULE

Add NAT Rule
? ×

Title
NAT Exempt

Create Rule for
Manual NAT

Status
☒

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement
Before Auto NAT Rules

Type
Static

Packet Translation
Advanced Options

☐ Translate DNS replies that match this rule
☐ Fallthrough to Interface PAT (Destination Interface)
☒ Perform route lookup for Destination interface
☐ Do not proxy ARP on Destination Interface

Show Diagram
☐
CANCEL
OK

site1FTD_nat_EXEMPT_RULE_2

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

Security Policies
SSL Decryption
Identity
Security Intelligence
NAT
Access Control
Intrusion

3 rules
Filter

#	NAME	TYPE	INTERFACES	ORIGINAL PACKET				TRANSLATED PACKET				ACTIONS
				SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	
Manual NAT Rules												
> 1	NAT Exempt	STATIC	Inside Any	inside_192.1...	peer_192.16...	ANY	ANY	inside_192.1...	peer_192.16...	ANY	ANY	
Manual NAT Rules (After)												
> 1	ISP1NatRule	DYNAMIC	Inside outside	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY	
> 3	ISP2NatRule	DYNAMIC	Inside outside2	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY	

Site1FTD_NAT_RULE_OVERVIEW

نيوكتالت تاريخي غت رشن 9. ةوطخل

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

site1FTD_DEPLOYMENT_CHANGES

Site2 FTD VPN نيوكت

Site2 FTD لة لباقم ل تامل عمل مادختساب 9 ةوطخل الى 1 ةوطخل ررك 10. ةوطخل

DemoS2S Connection Profile

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

VPN Access Interface

demovti25 (169.254.10.2)

Peer IP Address

192.168.30.1

IKE V2

IKE Policy

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

IPSec Proposal

aes,aes-256-sha-1,sha-256

Authentication Type

Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration

28800 seconds

Lifetime Size

4608000 kilobytes

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

site2FTD_ISP1_review_vpn_config_summary

Demo_S2S_SP2 Connection Profile

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

VPN Access Interface demovti_sp2 (169.254.20.12)



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, aes,aes-256-sha,sha256-sha,sha256-14
IPSec Proposal aes,aes-256-sha-1,sha-256
Authentication Type Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

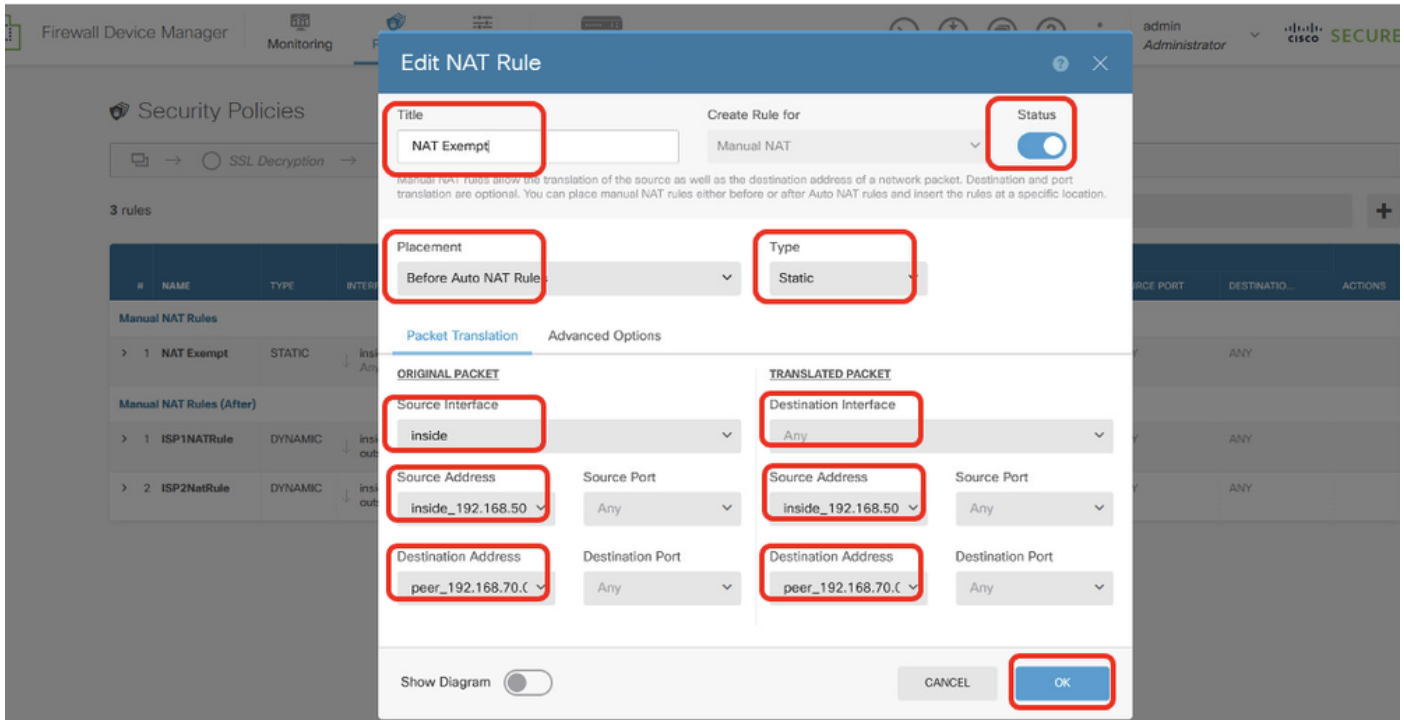
Lifetime Duration 28800 seconds
Lifetime Size 4608000 kilobytes

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

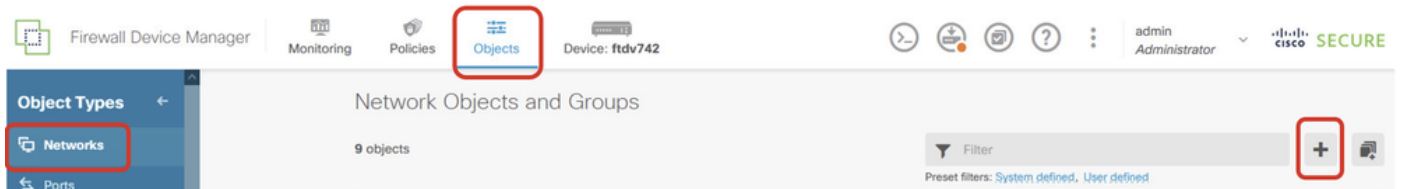


Site2FTD_nat_EXEMPT_RULE

PBR تانيوكتال

Site1 FTD ب صاخال PBR نيوكت

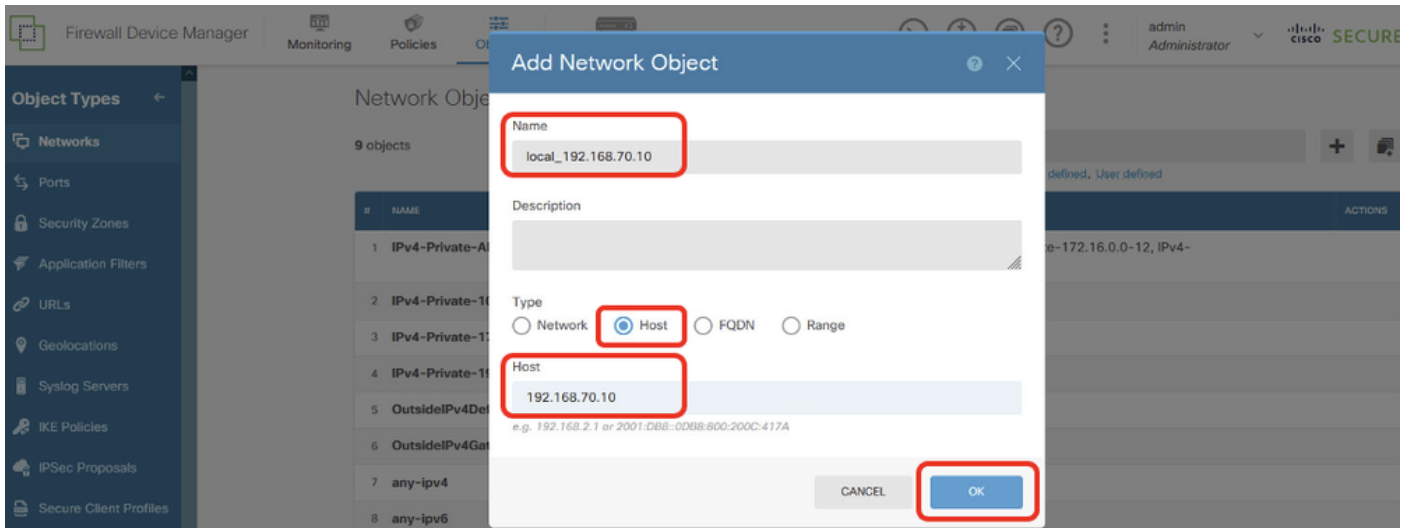
PBR ل لوصول اعمئاق لبق نم اهم ادخستل متيل ةديج ةكبش تانيك عاشناب مق 11. ةوطخال رز + رقناو تاكبشل > تانيكال ال لقتنا. 1 FTD عقوملل



site1FTD_CREATE_NETWORK_OBJECT

تامولعمل ري فوتب مق 2. Client1 Site1 ب صاخال IP ناو نعل نئاك عاشناب مق 11.1. ةوطخال قفاوم رزلا قوف رقنا. ةرورضال

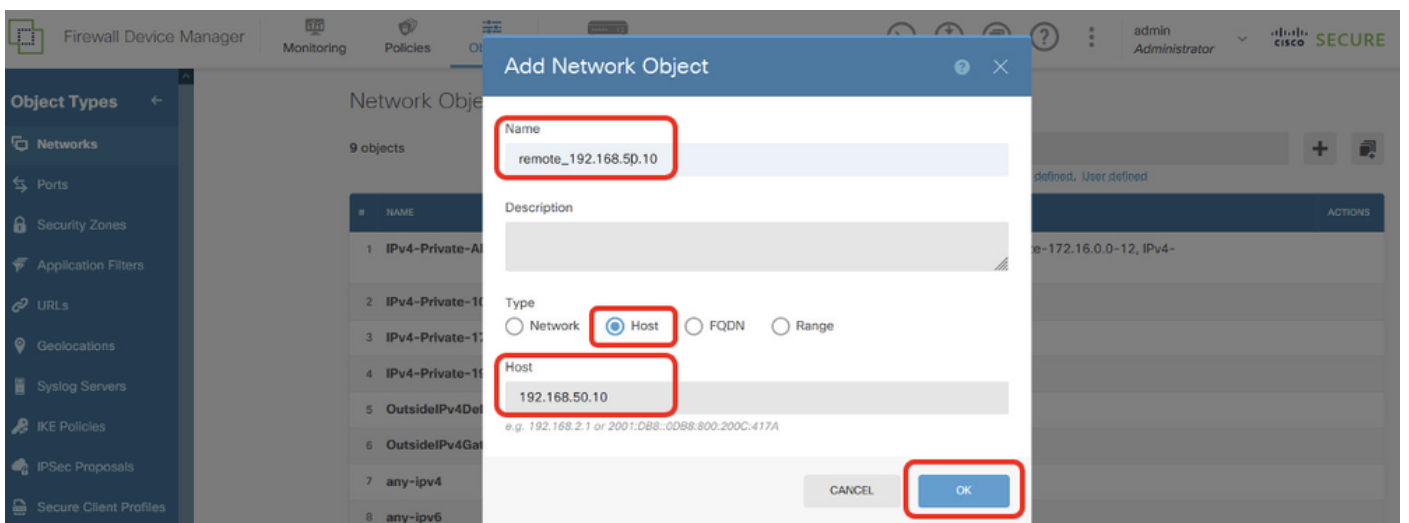
- مرسال: local_192.168.70.10
- فيضم: عونل
- فيضمال: 192.168.70.10



Site1FTD_Site1FTD_PBR_LocalObject

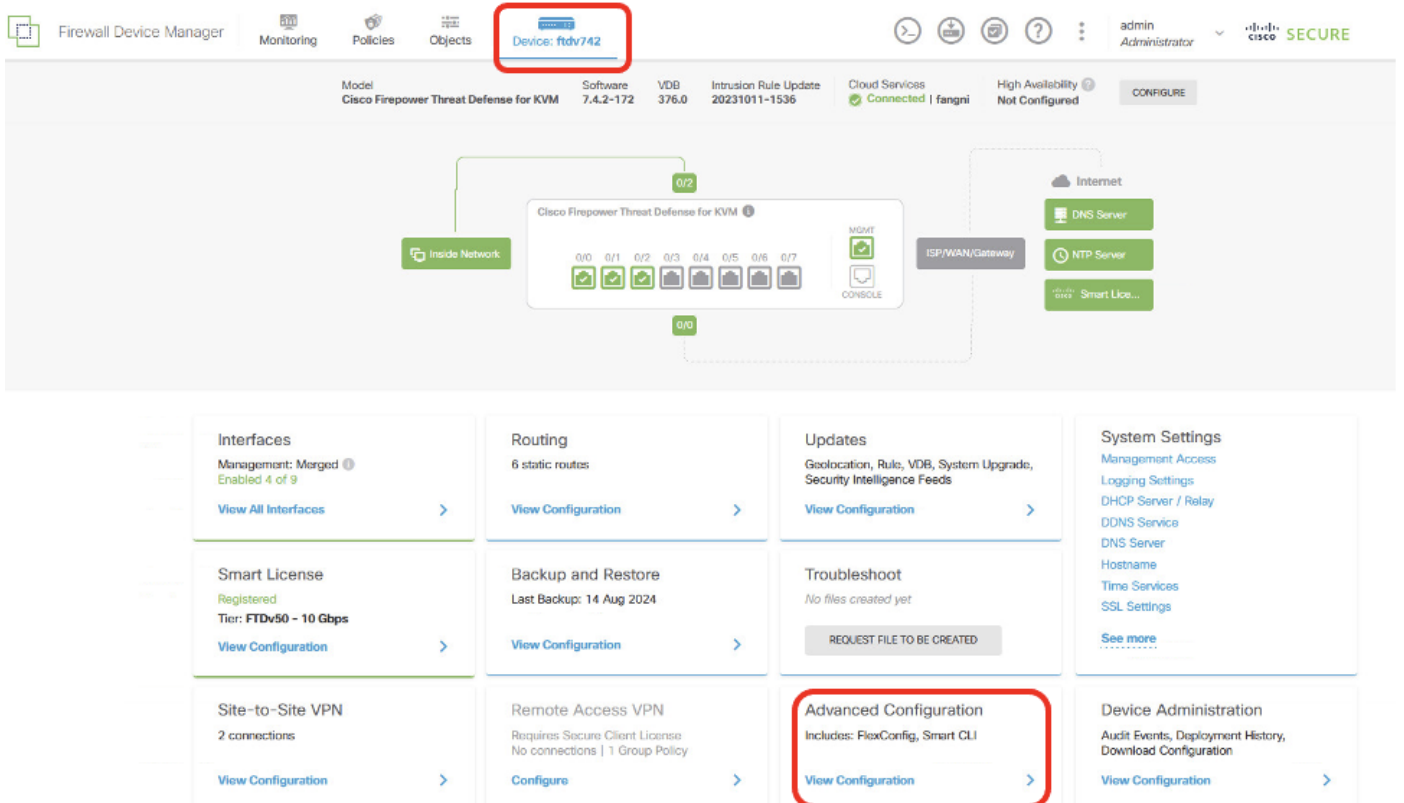
مزالل تامولعمل ري فوت. Site2 Client2 ب صا ال IP ناون عل نئاك ءاشنإ 11.2 ةوطخلا رز ok تق طوط.

- مسالال: remote_192.168.50.10
- فيضم: عونل
- فيضمال: 192.168.50.10



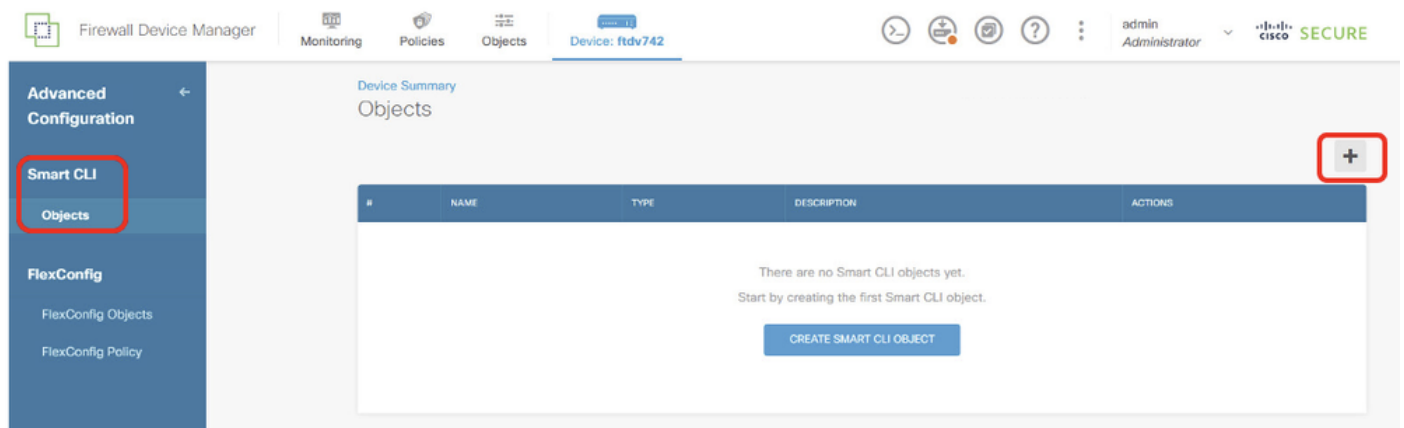
Site1FTD_PBR_RemoteObject

مدقتمل نيوكتل > زاهال إلقنا PBR ل ةسوم لوصو ةمئاق ءاشنإ 12 ةوطخلا ليكشت ضرع ةق طوط.



site1FTD_VIEW_ADVANCED_CONFIGURATION

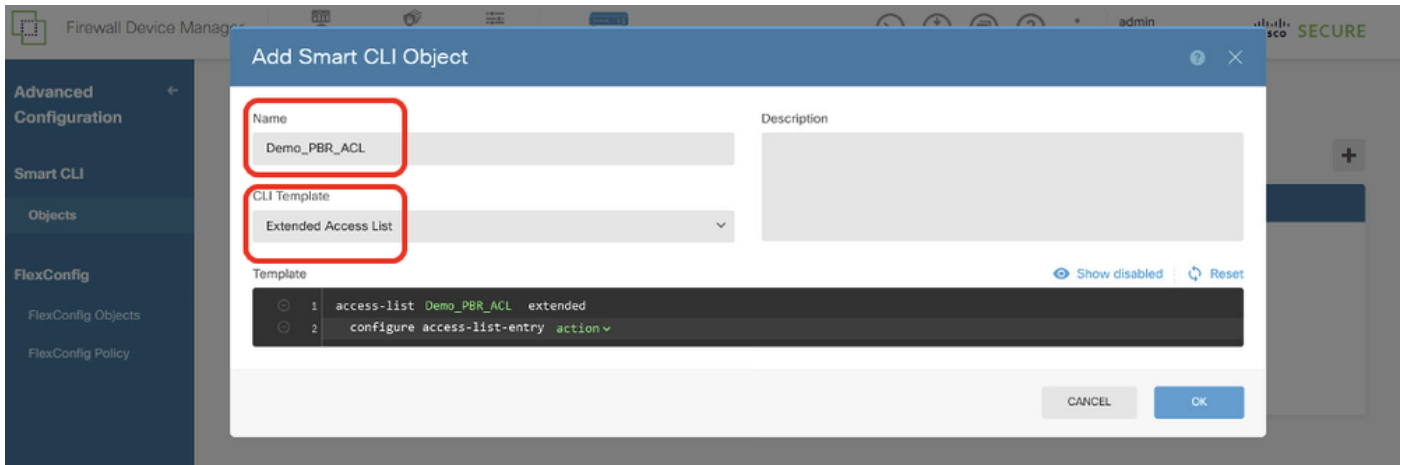
رز + قوف رقنا . تانئالك > ةيكدال (رماولا رطس ةهجاو) CLI ىلإ لقتنا 12.1 ةوطخلا



Site1FTD_Add_SmartCLI_Object

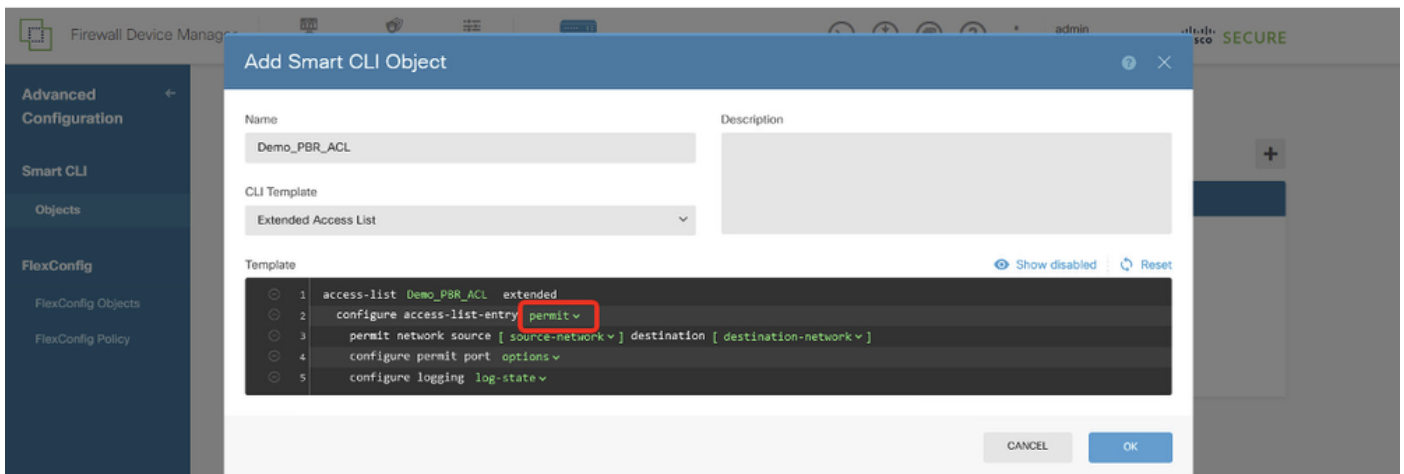
رماولا رطس ةهجاو بلاق رتخاو نئالك ل امسا لخدأ 12.2 ةوطخلا

- PBR_ACL_يحيضوتلا ضرعلا :مسالا
- ةعسوملا لوصولا ةمئاق :رماولا رطس ةهجاو بلاق



Site1FTD_Create_PBR_ACL_1

تذقنأ in order to رز ok لآ تقطقط .نپوكتلاو بلالقا لىل لقتنا 12.3 ةوطخلا
حامس رتخأ .عارجا قوف رقنا 2 رطسل

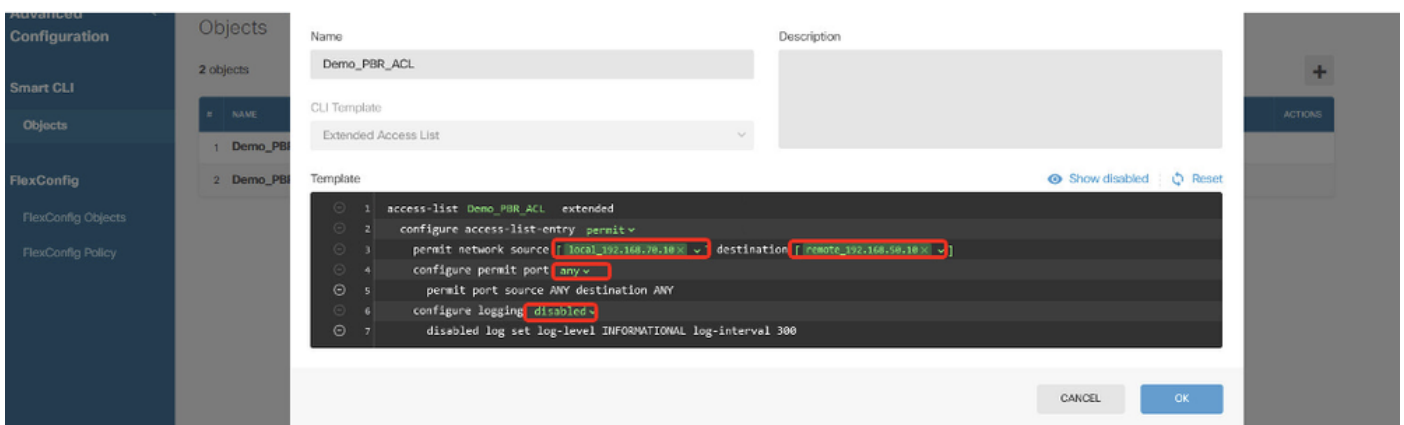


Site1FTD_Create_PBR_ACL_2

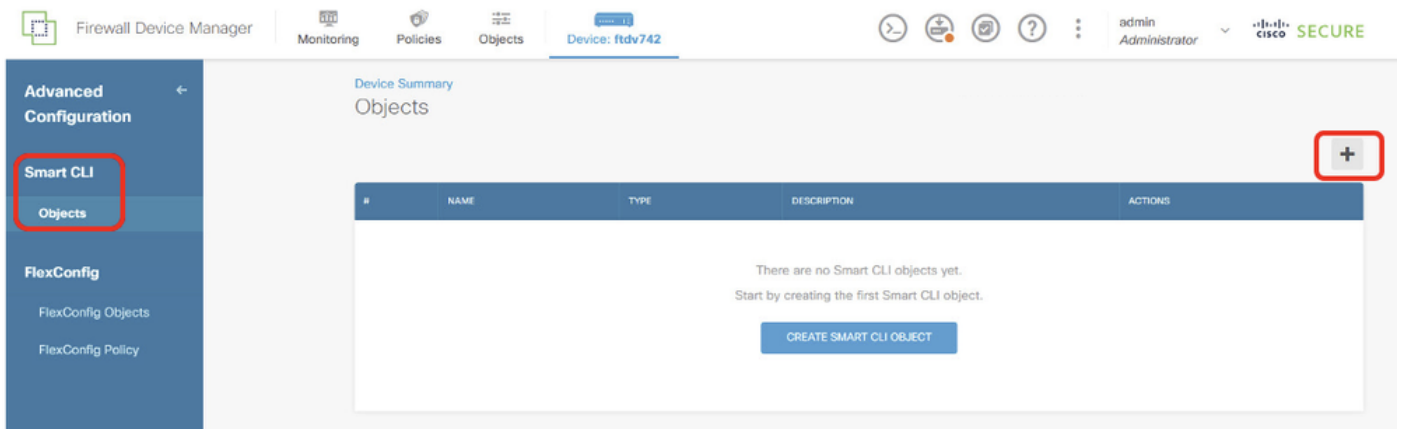
رتخأ .ةكبش-ةياغ تقطقط 192.168.70.10_يلحم تترتخأ .ردصملا ةكبش قوف رقنا 3 رطسل
remote_192.168.50.10.

يأ رتخاو تارايل رقنا 4 رطسل

ل.لطعم رتخاو لجسللا ةلاح قوف رقنا 6 رطسل

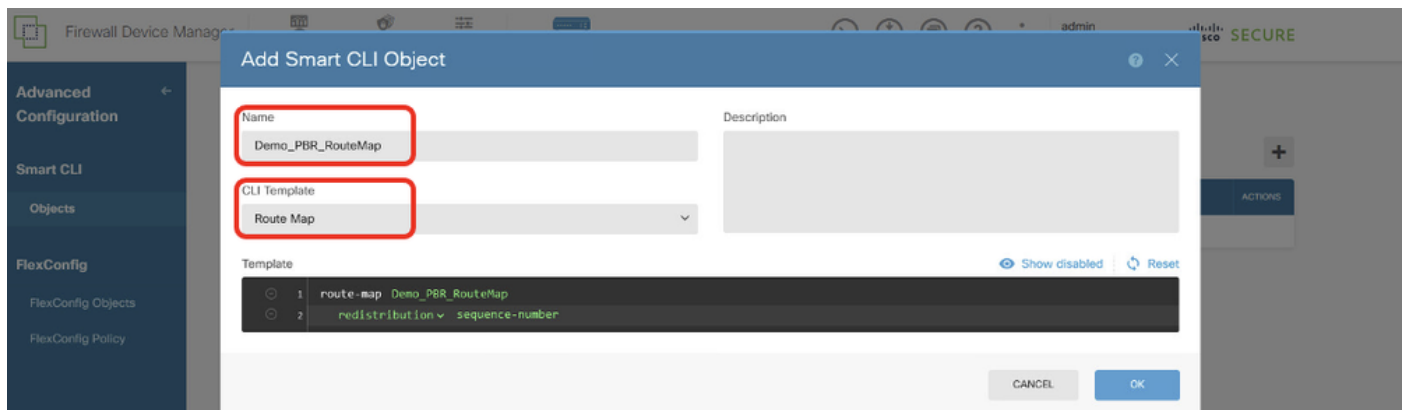


> يـكـذلـا CLI > مـدقـتـم نـيـو كـت > زـا هـجـالـى إـلـى لـقـتـنا PBR. لـ رـاسـم ةـطـيـر خـا شـنـا 13. ةـوـطـخـالـ رز + قـوـف رـقـنـا .تـانـئـالـا



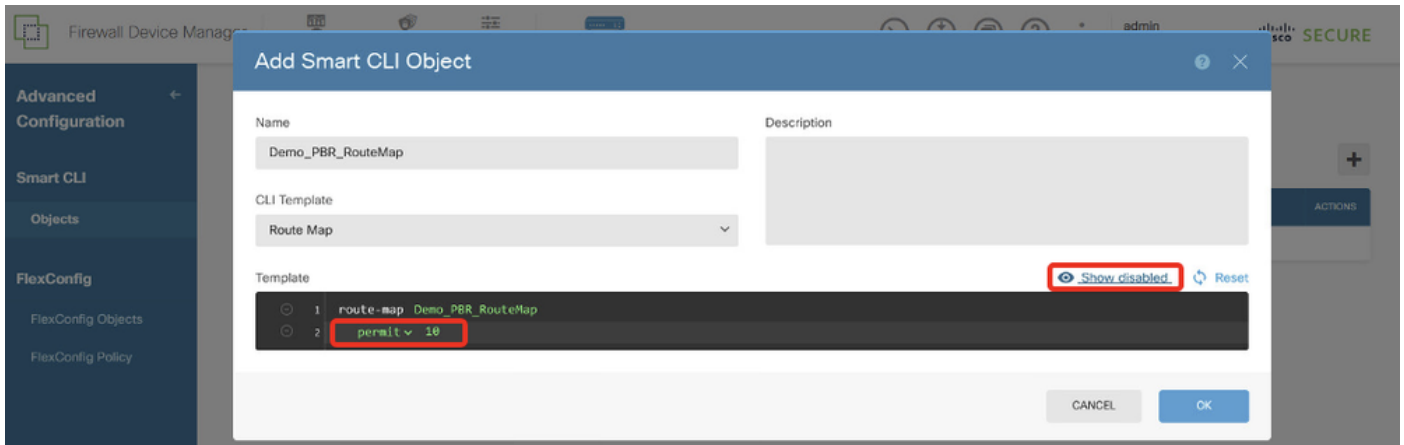
رـمـاوـالـا رطـس ةـهـجـاو بـلـاق رتـخـاو نـئـالـل امـسـا لـخـدا 13.1. ةـوـطـخـالـ

- راسـمـالـا ةـطـيـر خـا :رـمـاوـالـا رطـس ةـهـجـاو بـلـاق
- PBR_RouteMap يـحـيـضـوتـالـا ضـرـعـالـا :مـسـالـا



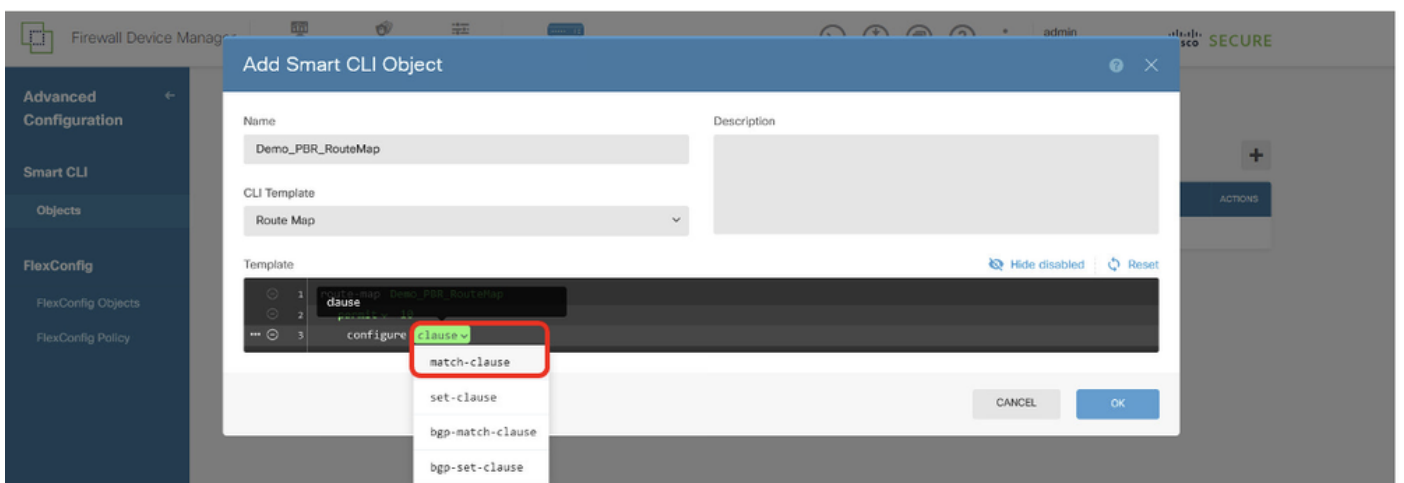
ظـفـحـلـل "قـفـاوـم رزـالـا قـوـف رـقـنـا .نـيـو كـتـالـاو بـلـاقـالـى إـلـى لـقـتـنا 13.2. ةـوـطـخـالـ

رـقـنـا 10. يـوـديـالـا لـا خـدـالـا ، sequence-number قـوـف رـقـنـا .حـامـس رتـخـا .عـيـزـوت ةـدـاع رـقـنـا ، 2 رطـسـالـا لـطـعـمـالـا رـاهـظـا قـوـف



Site1FTD_Create_PBR_RouteMap_2

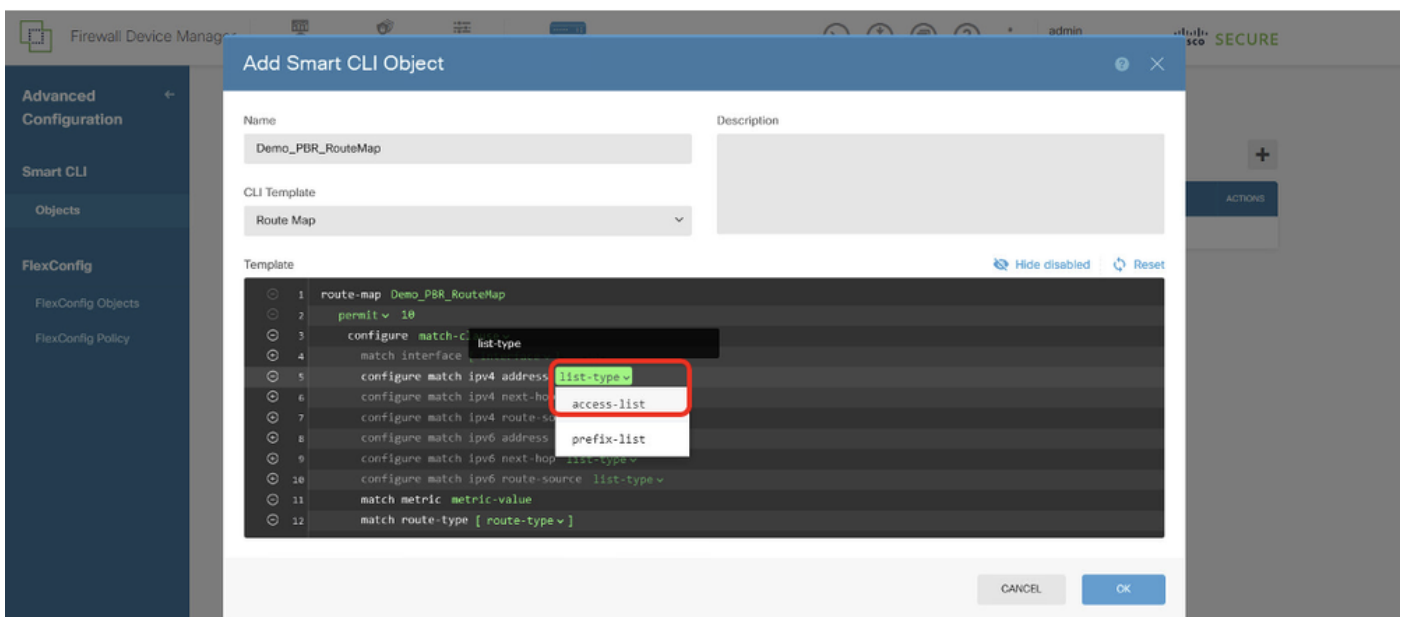
ةقباطلم ةرابع رتخأ .ةرابع ةقطق .رطسلل نيكم تل + قوف رقنا ،3 رطسلل



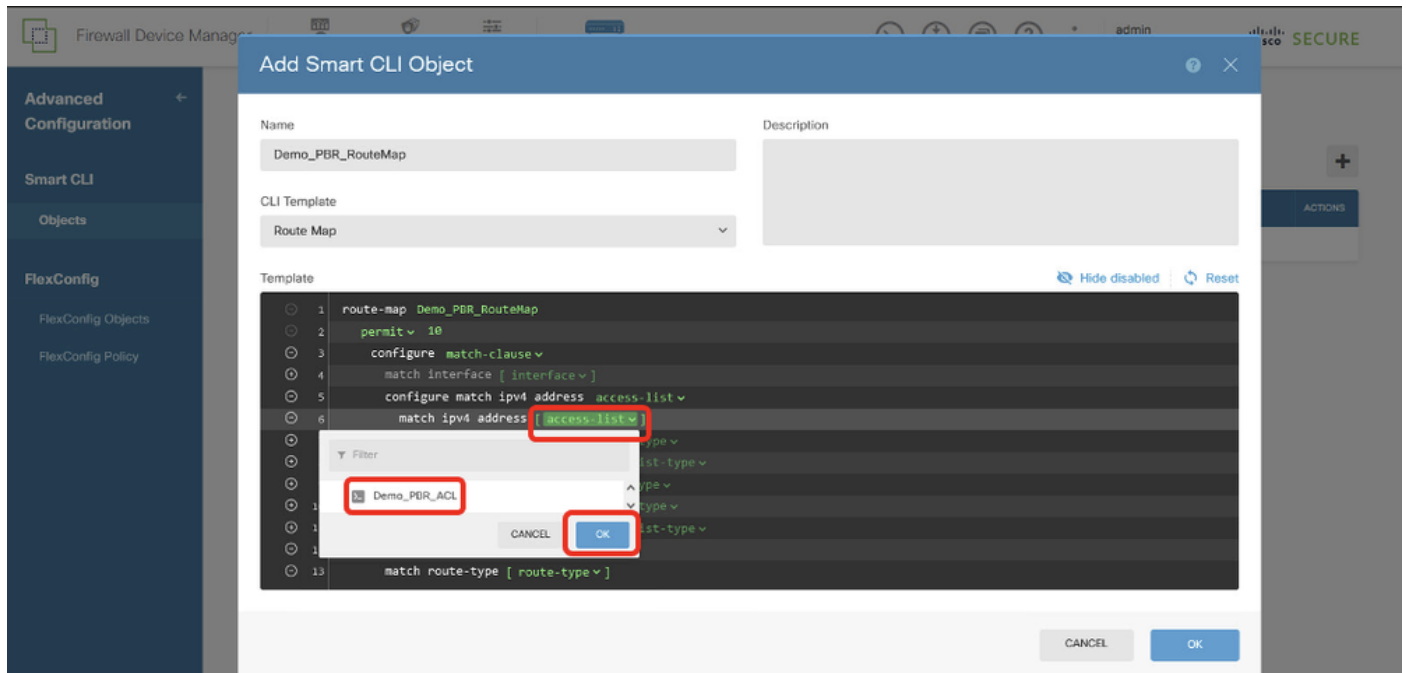
Site1FTD_Create_PBR_RouteMap_3

طخلال ليطعتل - رقنا ،4 رطسلل

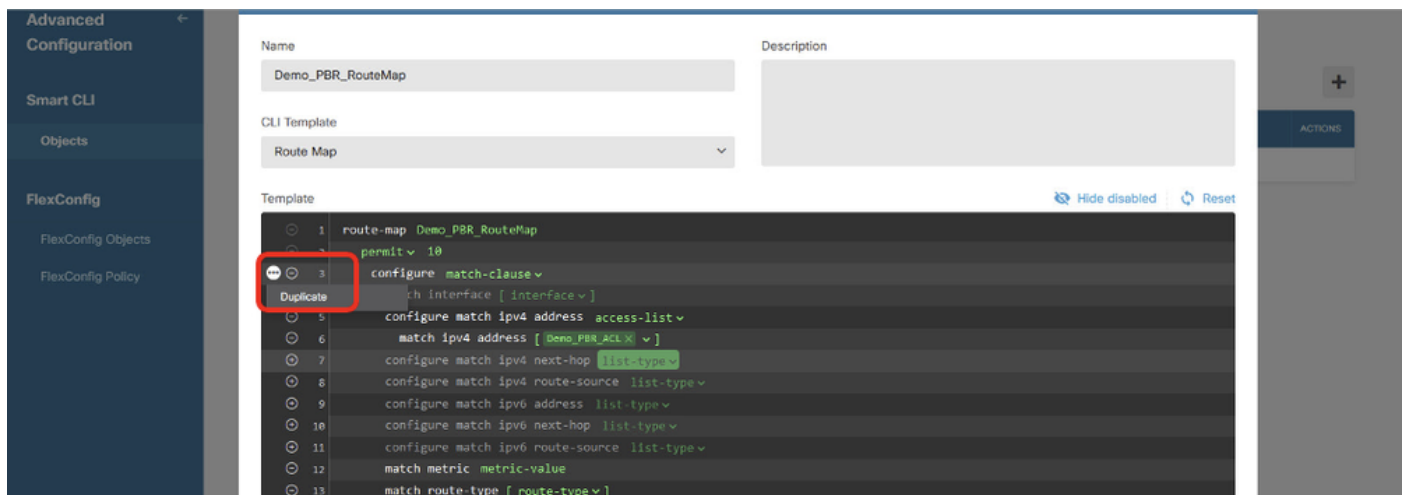
لوصول ةمئاق رتخأ .ةمئاقلا عون قوف رقنا .رطسلل نيكم تل + رقنا ،5 رطسلل



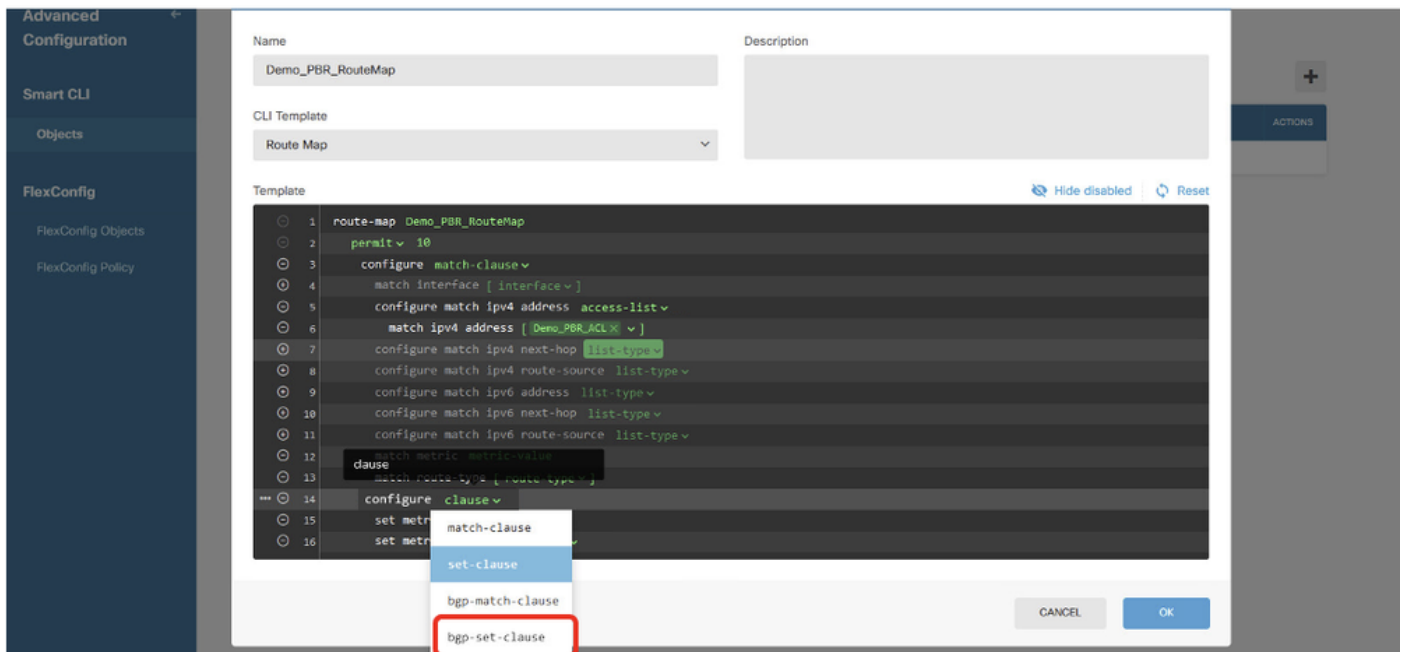
مت يذال (ACL) لوصولي ف مكحتال عمئاق مسارتخأ. لوصولال عمئاق قوف رقنا 6، رطسلا
demo_pbr_acl، لاثمل اذه في 12. ةوطخلال في هؤاشنإ



ة.عاضم رتخأ ... تارايخلال قوف رقنا 3. رطسلا إلى لقنا



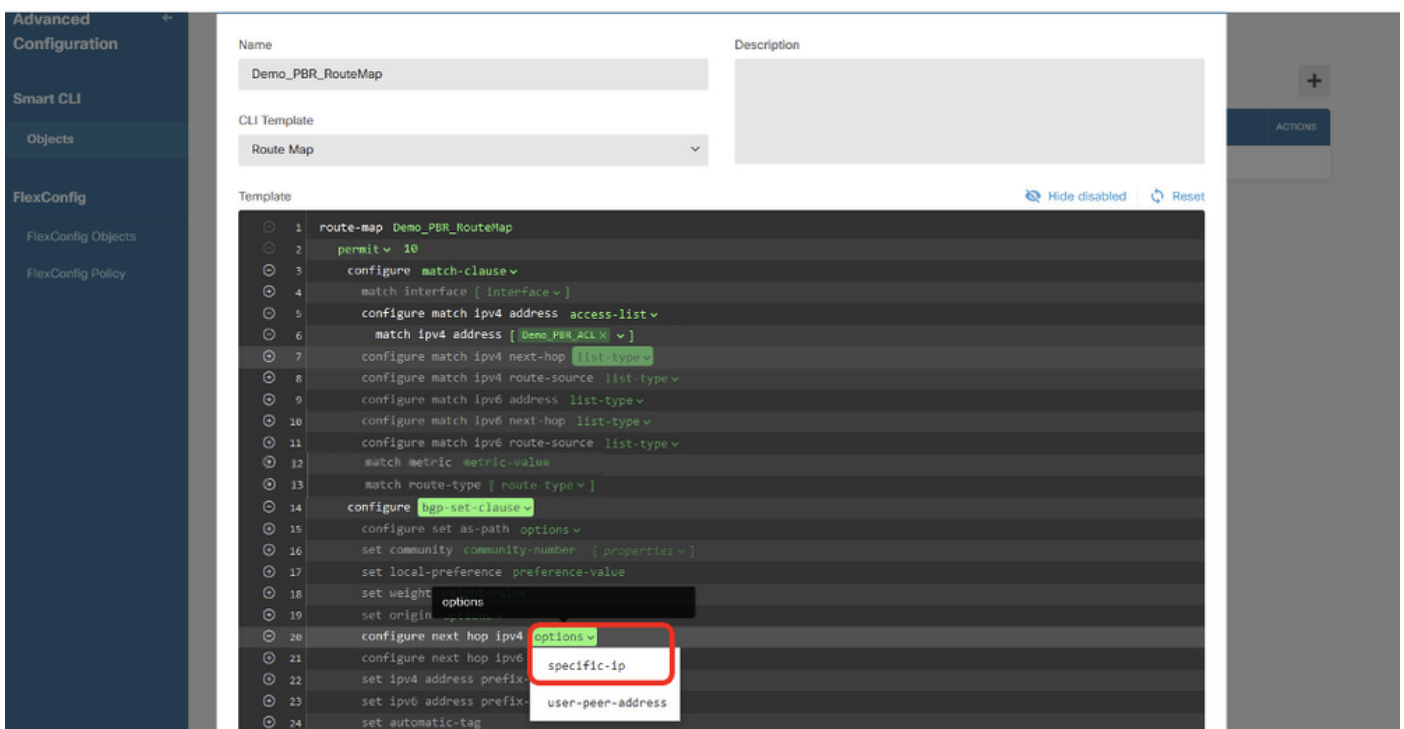
bgp-set-clause. رتخاو ةرابع قوف رقنا 14، رطس



Site1FTD_Create_PBR_RouteMap_7

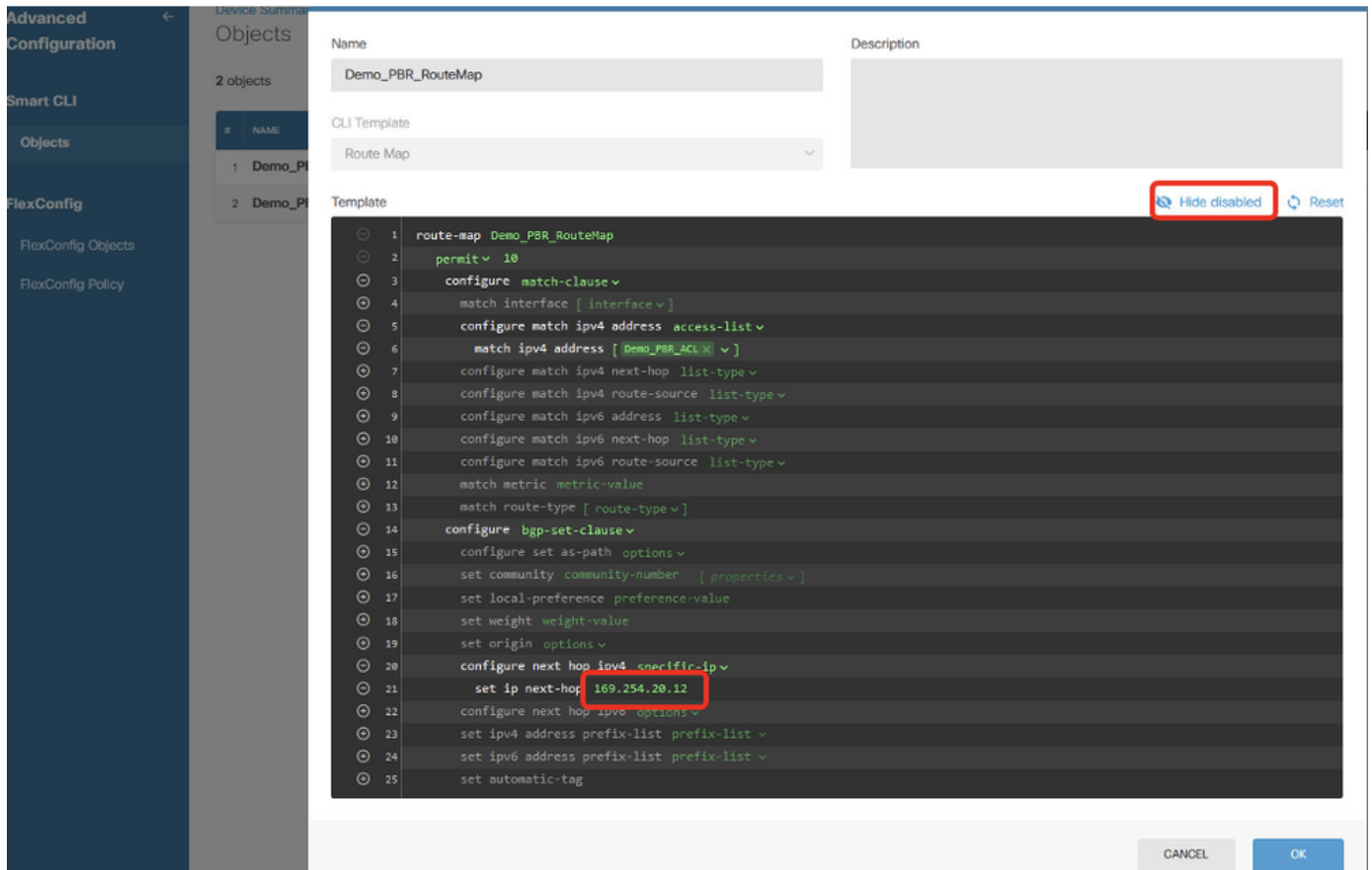
لجأ نم رز - قوف رقنا، 24 و 23 و 22 و 21 و 19 و 18 و 17 و 16 و 15 و 13 و 12 رطسألأ يف ل.ل.طعتل.

صاخ ip رتخاو تارايخ قوف رقنا، 20 رطسلل.



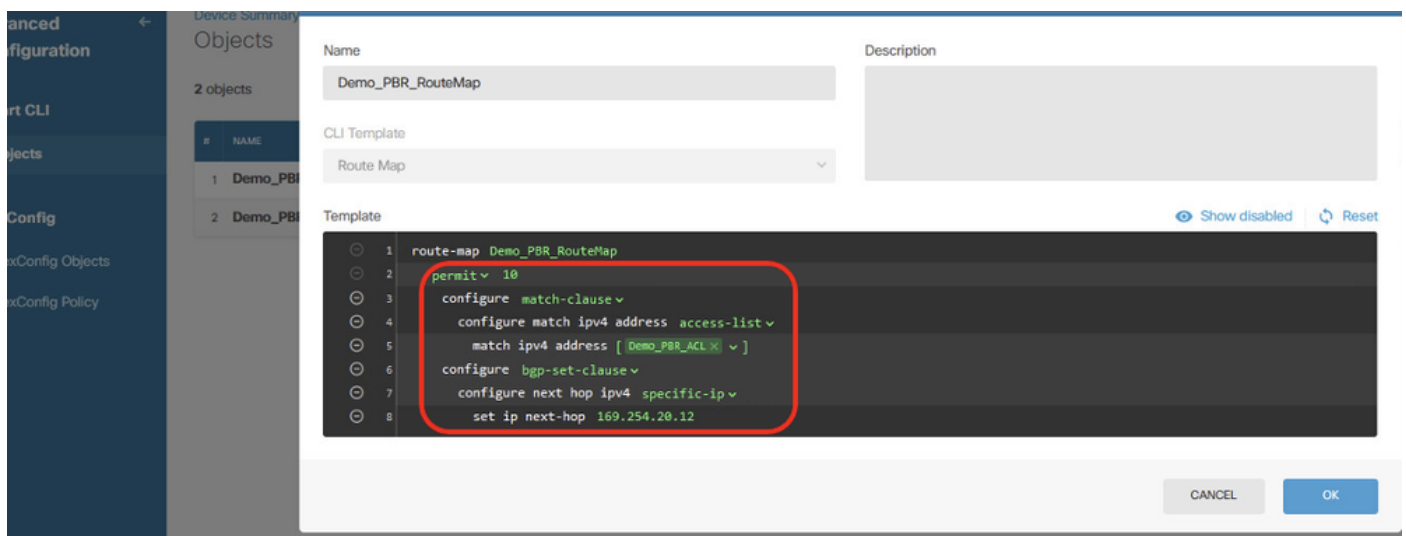
Site1FTD_Create_PBR_RouteMap_8

ل.ل.طعتل اذه يف .ة.ل.ل.ة ووطخل يف يودي ل.ل.ل.ل.ل IP ناوع . IP ناوع قوف رقنا، 21 رطسلل عافخ إىلع رقنا . (169.254.20.12) FTD 2 ل VTI ق فن 2 ريظنل ع قووم ب صاخ ل IP ناوع نوكي ل.ل.طعم.



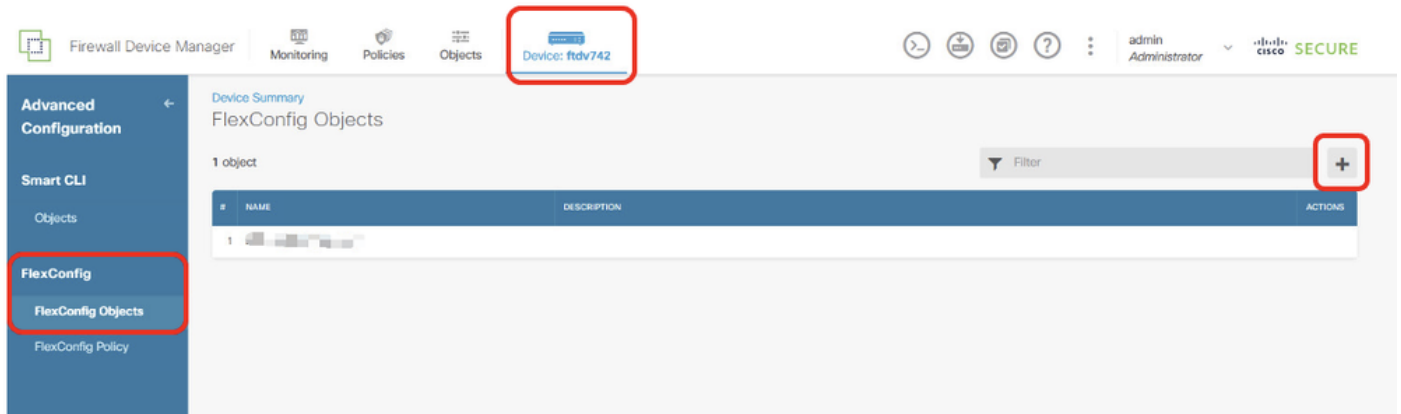
Site1FTD_Create_PBR_RouteMap_9

راسم الة طيرخ نيوك ت عجار.



Site1FTD_Create_PBR_RouteMap_10

> مدقتم الة نيوك ت ال > زاهج الة ل ل ق ت نا PBR. FlexConfig ل ئاك ءاشن اب مق 14. ةوطخل
رز + رقناو FlexConfig تانئاك.



Site1FTD_Create_PBR_FlexObj_1

في Template و Negative Demo_PBR_FlexObj.، لاثم ال اذه في .نئاكلل مس لخدأ 14.1. ةوطخل Template Editor، رماوأل رطسأ لخدأ.

- بلالاق:

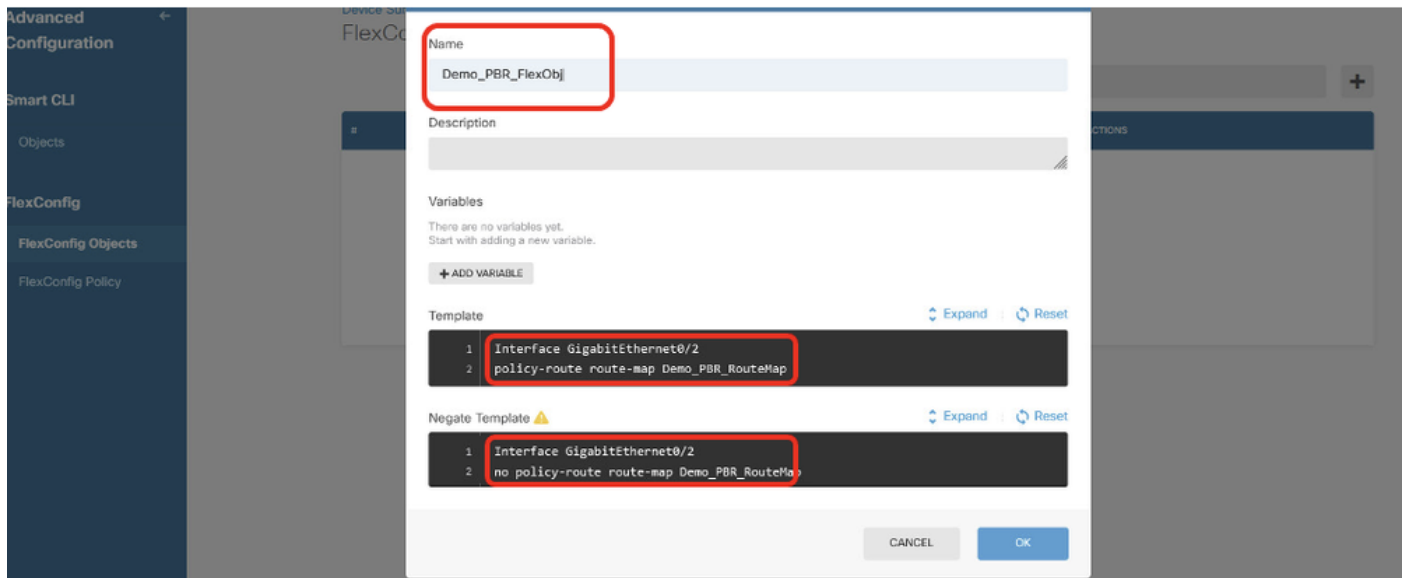
interface GigabitEthernet0/2

policy-route route-map demo_pbr_routeMap_site2

- حل اص ريغ بلالاق:

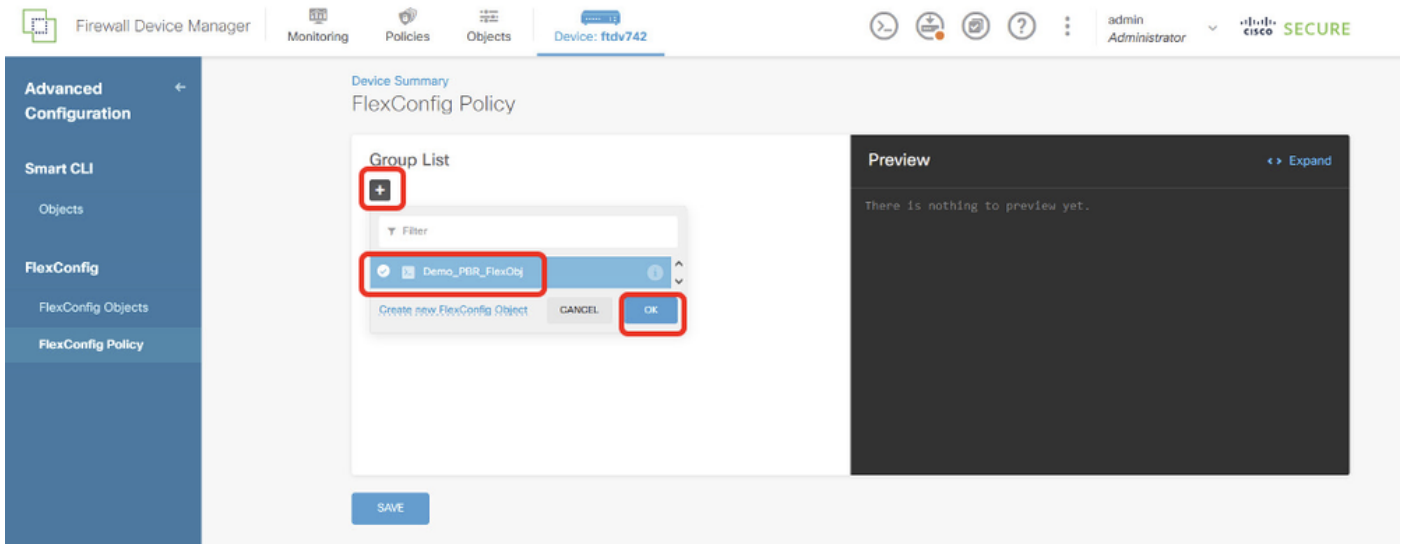
interface GigabitEthernet0/2

Policy-route-map demo_PBR_RouteMap_Site2 دجوي ال



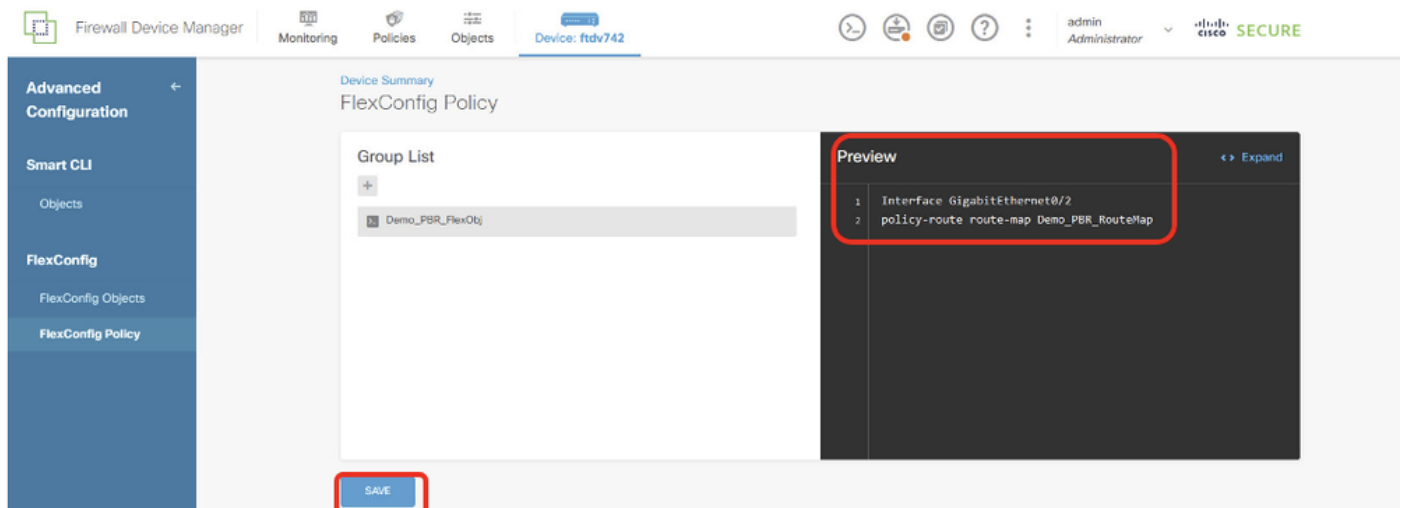
Site1FTD_Create_PBR_FlexObj_2

> مدقتم نيوكت > زاهج لىل لقتنا . PBR ل FlexConfig ةسايس عاشناب مق 15. ةوطخل 14. ةوطخل في هؤاشنإ مت يذل FlexConfig نئاكل مس رتخأ . رز + قوف رقنا . FlexConfig ةسايس ققافوم رزلا قوف رقنا .



Site1FTD_Create_PBR_FlexPolicy_1

ظفح قوف رقنا ،اديح ناك اذا .ةنياعمل اذفان في رمأل نم ققحت 15.1 ةوطخل



Site1FTD_Create_PBR_FlexPolicy_2

نيوكتل تاريغي رشن 16 ةوطخل



site1FTD_DEPLOYMENT_CHANGES

Site2 FTD ب صااال PBR نيوكت

ةلباقملا تاملعمل مادختساب PBR عاشنإ لجأ نم 16 ةوطخل إلى 11 ةوطخل ارر 17 ةوطخل 2 FTD عقوملل

Firewall Device Manager

Advanced Configuration

Smart CLI

Objects

FlexConfig

FlexConfig Objects

FlexConfig Policy

Add Smart CLI Object

Name: Demo_PBR_ACL_Site2

Description:

CLI Template: Extended Access List

Template

```
1 access-list Demo_PBR_ACL_Site2 extended
2 configure access-list-entry permit
3 permit network source [ local_192.168.50.10 % ] destination [ remote_192.168.70.10 % ]
4 configure permit port any
5 permit port source ANY destination ANY
6 configure logging disabled
7 disabled log set log-level INFORMATIONAL log-interval 300
```

Show disabled Reset

CANCEL OK

Site2FTD_Create_PBR_ACL

Firewall Device Manager

Advanced Configuration

Smart CLI

Objects

FlexConfig

FlexConfig Objects

FlexConfig Policy

Add Smart CLI Object

Name: Demo_PBR_RouteMap_Site2

Description:

CLI Template: Route Map

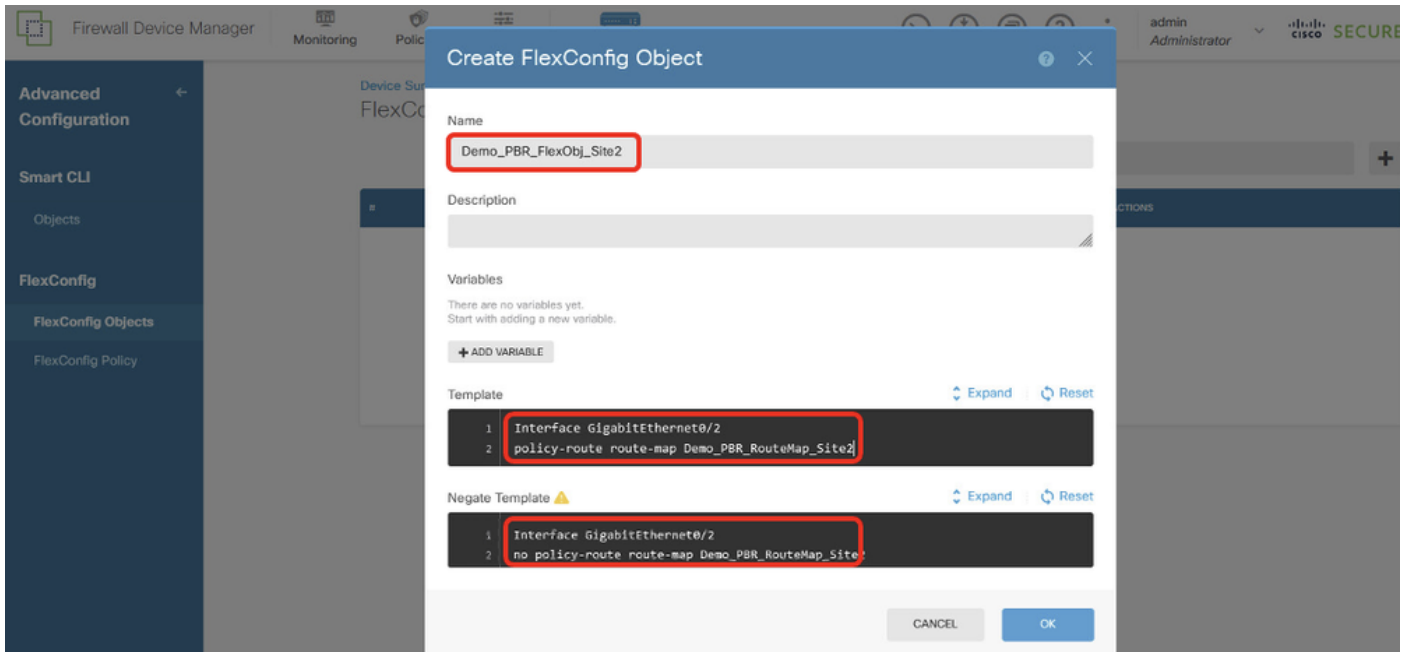
Template

```
1 route-map Demo_PBR_RouteMap_Site2
2 permit 10
3 configure match-clause
4 configure match ipv4 address access-list
5 match ipv4 address [ Demo_PBR_ACL_Site2 % ]
6 configure bgp-set-clause
7 configure next hop ipv4 specific-ip
8 set ip next-hop 169.254.20.11
```

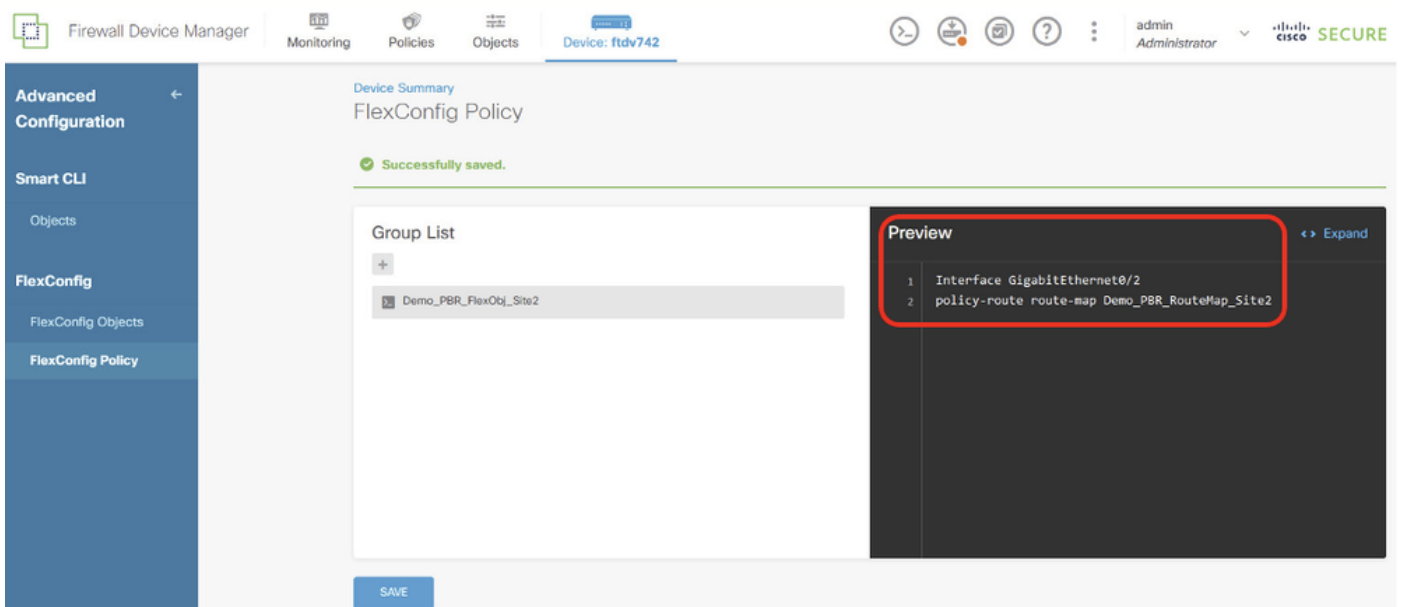
Show disabled Reset

CANCEL OK

Site2FTD_Create_PBR_RouteMap



Site2FTD_Create_PBR_FlexObj

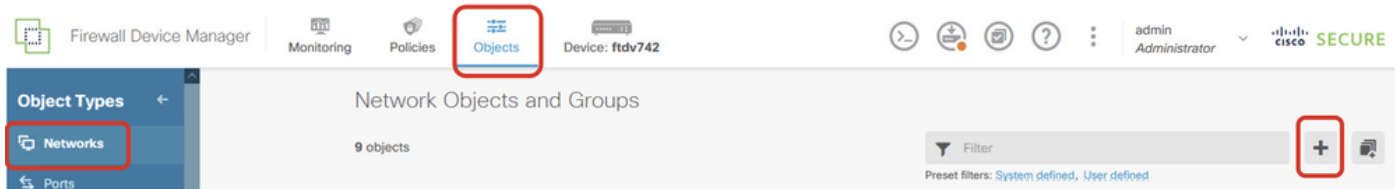


Site2FTD_Create_PBR_FlexPolicy

SLA ةشاش ىلع ةئيهتلا تايلمع

SLA ةبقارم نيوكت SITE1 FTD ل

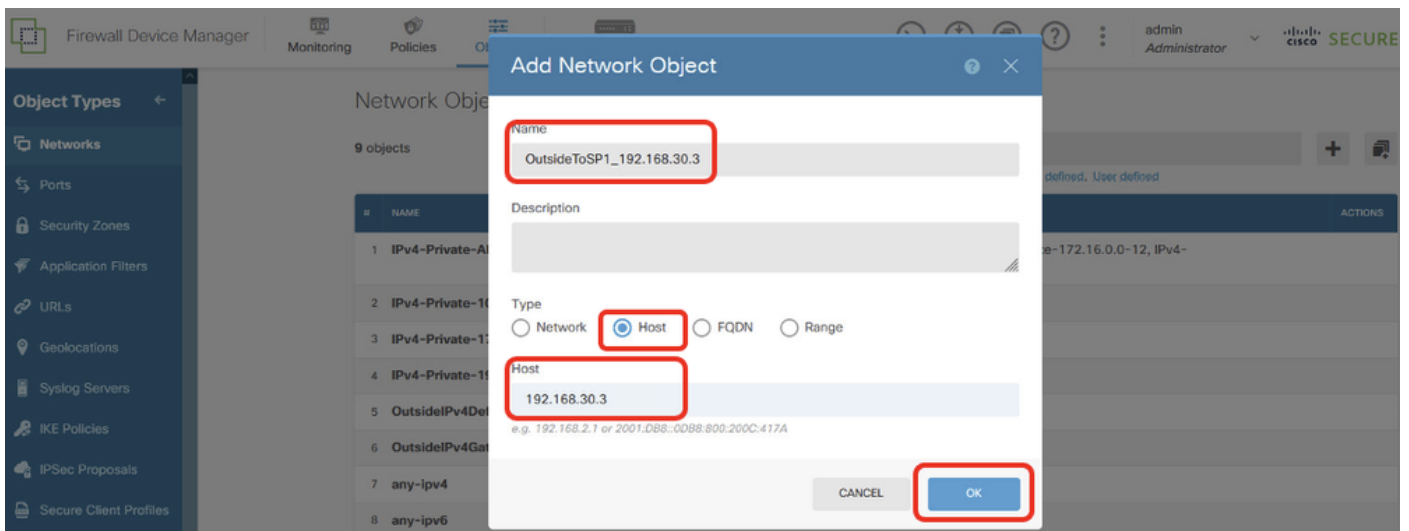
عقوملل SLA تاشاش لبق نم اهم ادخست متيل ةديج ةكبش تانئاك ءاشناب مق 18. ةوطخل رز + قوف رقنا ، تاكبش > تانئاك ىل لقتنا 1 FTD.



site1FTD_CREATE_NETWORK_OBJECT

ةمزالل تامولعمل ري فوتب مق ISP1 ةب اوبل IP ناونعل نئاك عاشنإب مق 18.1 ةوطخل رز. ok تق طوط

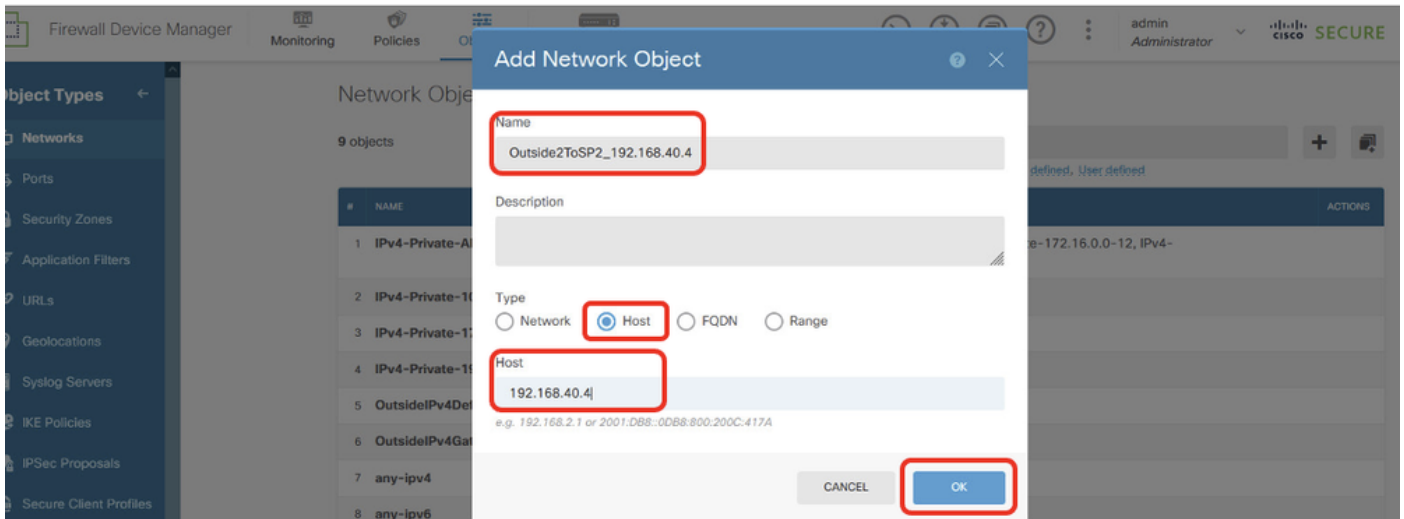
- مرسال: OutsideToSP1_192.168.30.3
- فيضم: عونل
- فيضم: 192.168.30.3



Site1FTD_Create_SLAMonitor_NetObj_ISP1

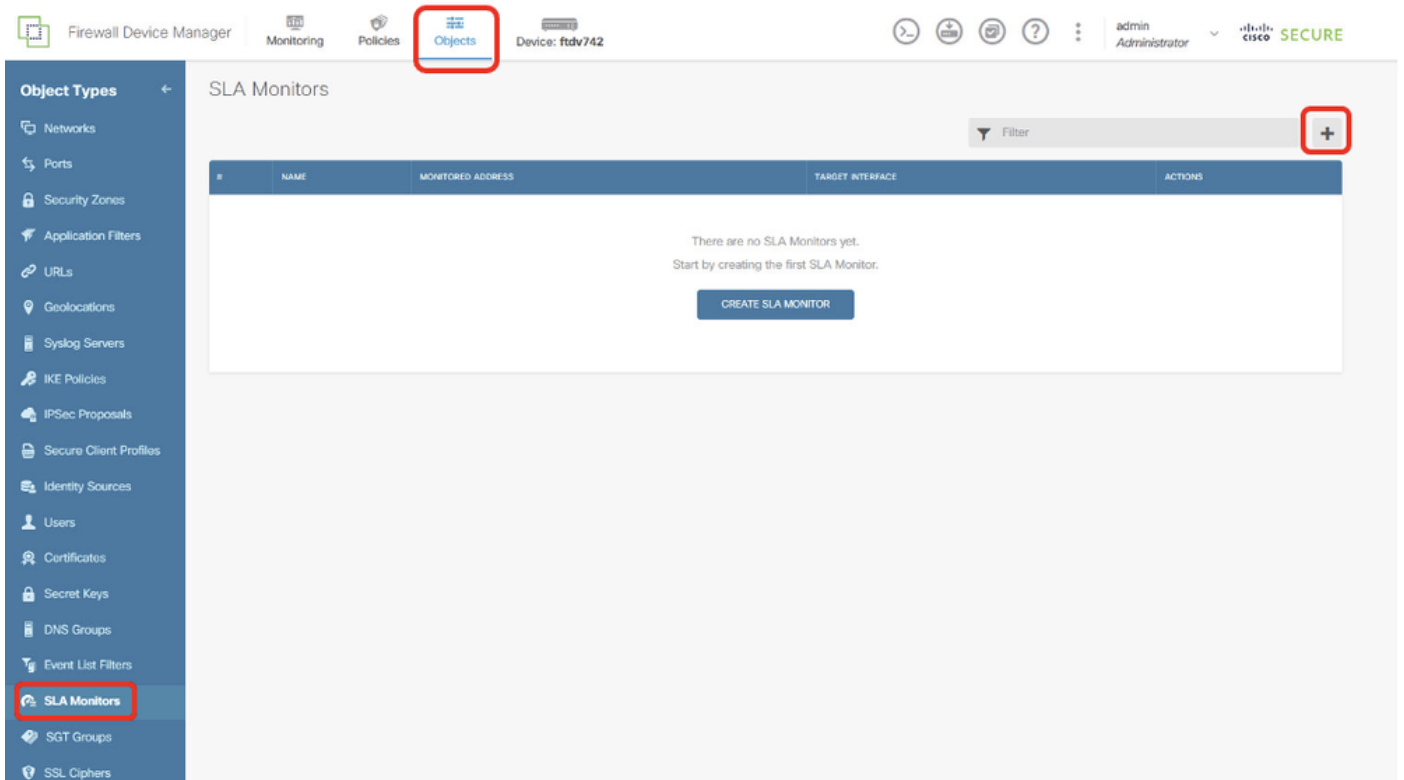
ةرورضل تامولعمل ري فوتب مق ISP2 ةب اوبل IP ناونعل نئاك عاشنإب مق 18.2 ةوطخل رز. ok تق طوط

- مرسال: Outside2ToSP2_192.168.40.4
- فيضم: عونل
- فيضم: 192.168.40.4



Site1FTD_Create_SLAMonitor_NetObj_ISP2

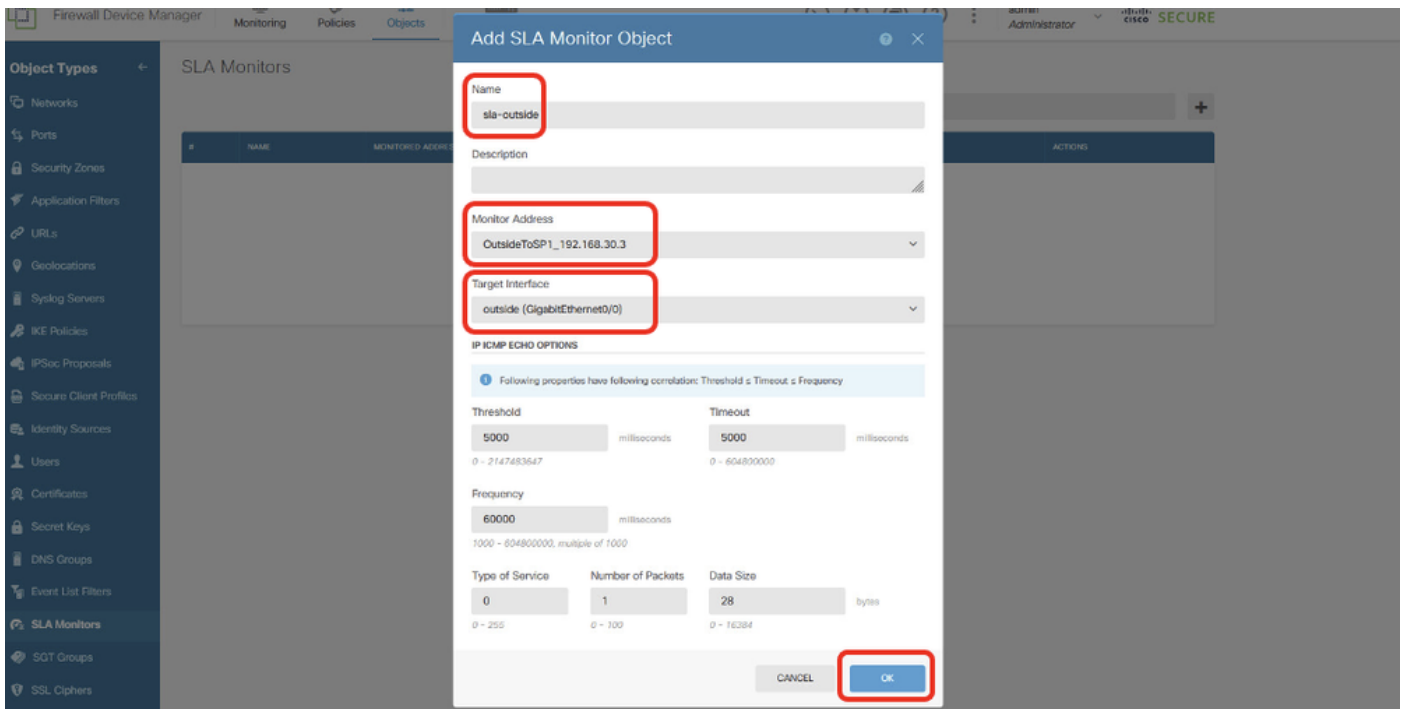
رز + قوف رقا. SLA تاشاش > نئاك عاونأ > تانئاك ىلإ لق تئا. SLA ةشاش عاشنإ. 19. ةوطخال ةديج SLA ةشاش عاشنإل.



Site1FTD_Create_SLAMonitor

ةباوبل ةمزالال تامولعمل ري فو تب مق SLA ةبقارم نئاك ةفاضل ةذفان ف. 19.1. ةوطخال ظحلل "قف او م رزا قوف رقا. ISP1.

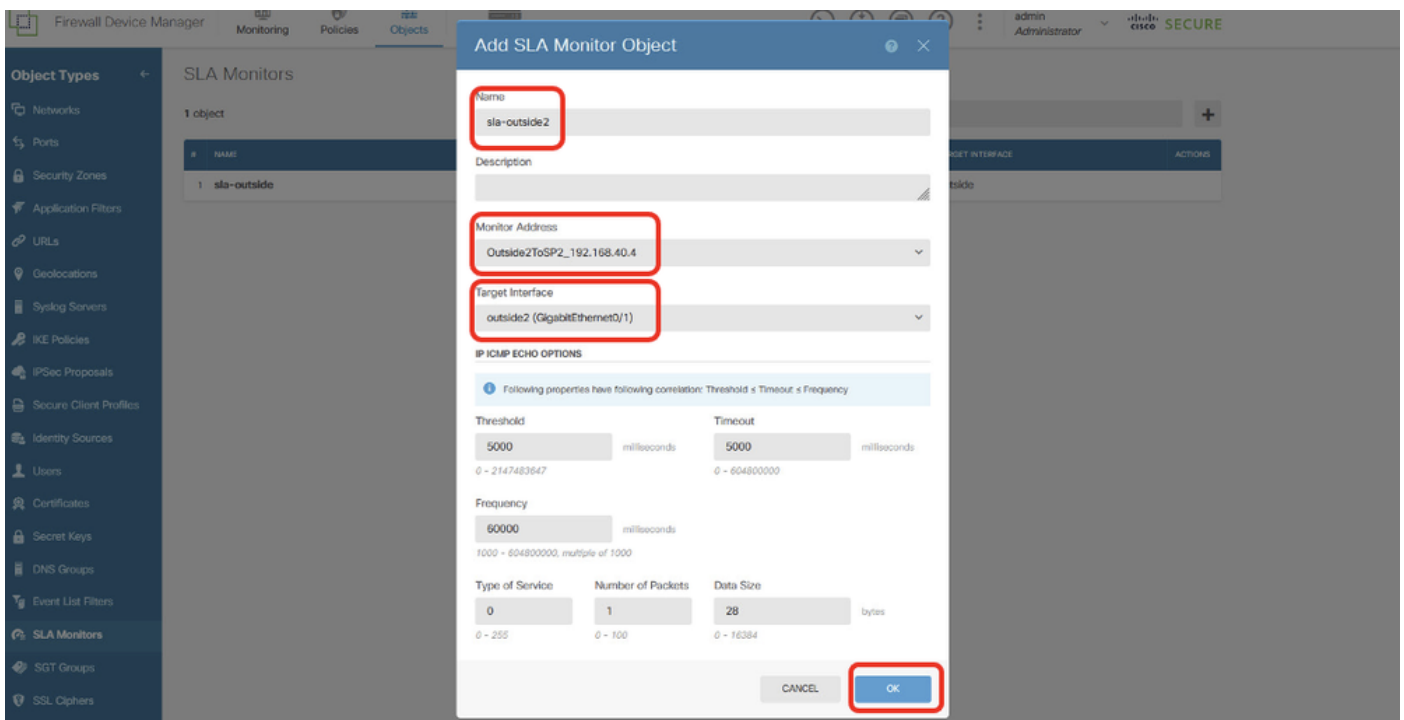
- ةجراخال (SLA) ةمدخال ىوتسم ةيقافاتل: م سال
- ةشاشال ناو نع: OutsideToSP1_192.168.30.3
- جراخ: فدهل ةهجال
- ىضارتفا: IP ل ICMP ىص تاراخ



Site1FTD_Create_SLAMonitor_NetObj_ISP1_Details

ةذفان يف ISP2 ةباوبل ةديج SLA ةشاش ءاشنال رز + قوف رقنلا يف رمتسا 19.2 ةوطخل رزلا قوف رقنا ISP2 ةباوبل ةرورضل تامولعمل ريفوتب مق SLA ةبقارم نئاك ةفاضإ ظحلل "قفافوم".

- ةيچراخلا (SLA) ةمدخلال يوتسم ةيقاتإ :مسالا
- ةشاشلا ناوع : Outside2ToSP2_192.168.40.4
- فدهلا ةهاولا : 2جراخ (GigabitEthernet0/1)
- يضارتفا : IP ل ICMP يدص تاراخي



Site1FTD_Create_SLAMonitor_NetObj_ISP2_Details

ن.يوكتل التاريخي غت رشن 20. ةوطخل



site1FTD_DEPLOYMENT_CHANGES

ةبقارم نيوكت SLA ل SITE2 FTD

ةلباقملا تاملعمل عم SLA ةبقارم عاشنإب مق 20. ةوطخل إلى 18. ةوطخل الررك 21. ةوطخل Site2 FTD.

SLA Monitor configuration details:

- Name: sla-outside
- Description:
- Monitor Address: OutsideToSP1_192.168.10.3
- Target Interface: outside (GigabitEthernet0/0)
- IP ICMP ECHO OPTIONS:
 - Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency
 - Threshold: 5000 milliseconds (0 - 2147483647)
 - Timeout: 5000 milliseconds (0 - 604800000)
 - Frequency: 60000 milliseconds (1000 - 604800000, multiple of 1000)
 - Type of Service: 0 (0 - 255)
 - Number of Packets: 1 (0 - 100)
 - Data Size: 28 bytes (0 - 16384)

Buttons: CANCEL, OK

Site2FTD_Create_SLAMonitor_NetObj_ISP1_Details

Object Types

SLA Monitor

2 objects

NAME

1 sla-outside2

2 sla-outside2

Name

sla-outside2

Description

Monitor Address

Outside2ToSP2_192.168.20.4

Target Interface

outside2 (GigabitEthernet0/1)

IP ICMP ECHO OPTIONS

Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold

5000 milliseconds

0 - 2147483647

Timeout

5000 milliseconds

0 - 604800000

Frequency

60000 milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0

0 - 255

Number of Packets

1

0 - 100

Data Size

28 bytes

0 - 16384

CANCEL OK

Site2FTD_Create_SLAMonitor_NetObj_ISP2_Details

تباثال راسمال ىلع تانيوكثال

ل SITE1 FTD تباثال راسمال نيوكث

ل تباثال راسمال لبق نم اهمادختسا متيل ةديج ةكبش تانيك عاشناب مق 22. ةوطخل
Site1 FTD. رز + قوف رقنا ، تاكبشال > تانيكال ىلى لقتنا .

Firewall Device Manager

Monitoring Policies Objects

Device: ftdv742

Object Types

Networks

Network Objects and Groups

9 objects

Filter

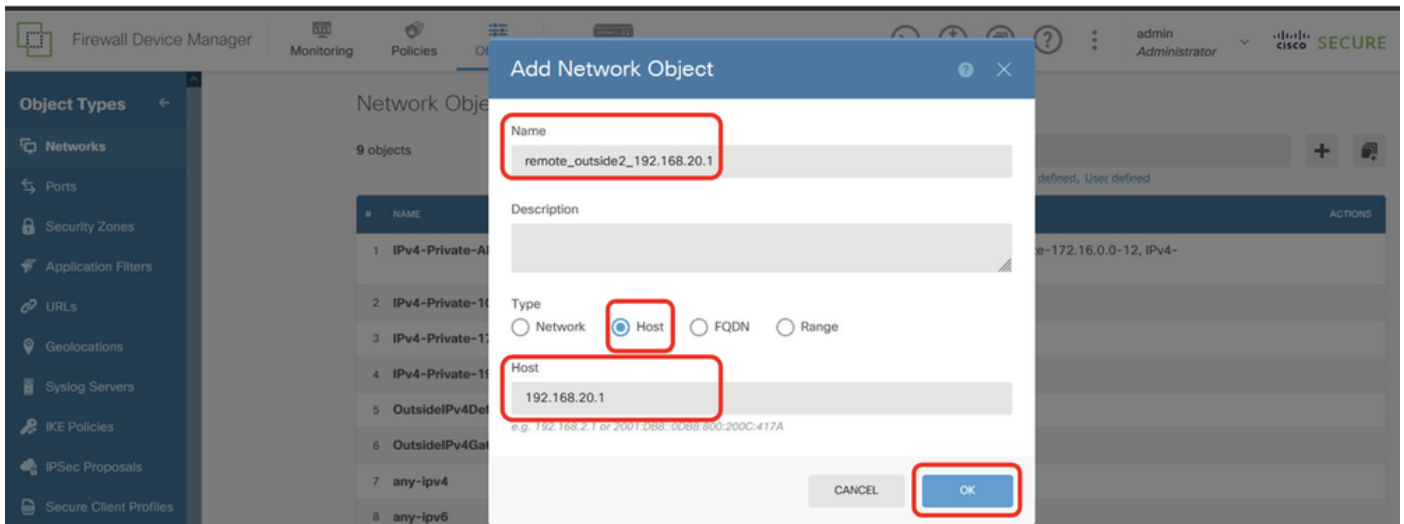
Preset filters: System defined, User defined

+

Site1FTD_Create_Obj

ريفوتب مق 2 FTD. ريظنل عقومل 2يچراخل IP ناوغل نئك عاشناب مق 22.1. ةوطخل
رز. ok تقطقط . ةيروزضال تامولعمل

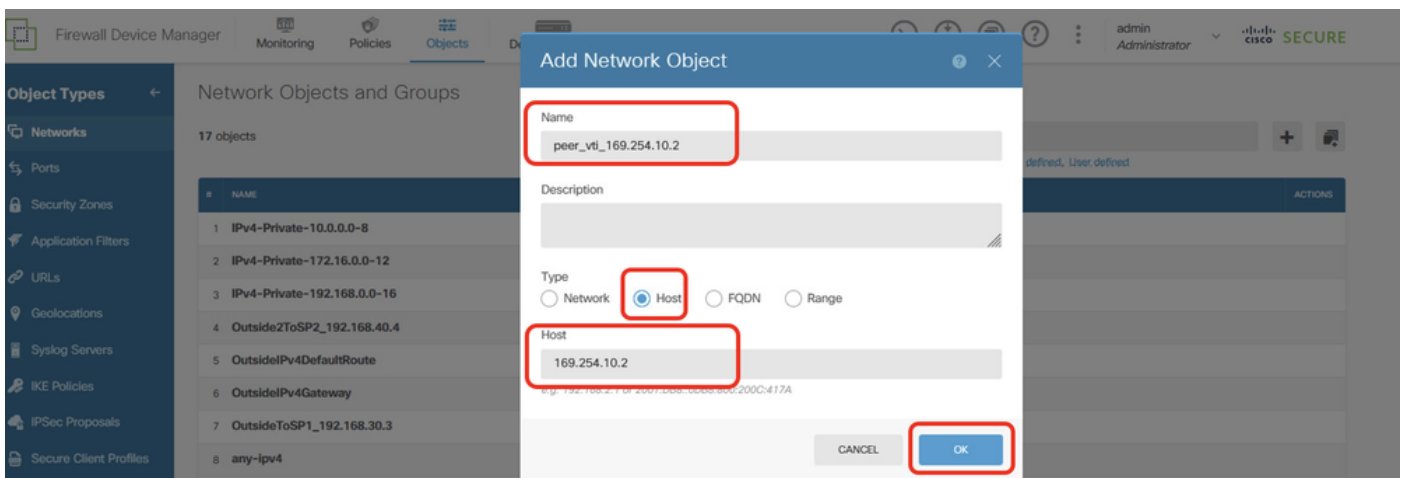
- رسال: remote_outside2_192.168.20.1
- فيضم: عونل
- ةكبشال: 192.168.20.1



Site1FTD_Create_NetObj_StaticRoute_1

مق 2 FTD. ريظننل عقوم ب صاخ ال IP ناونعل نئاك عاشنإب مق 22.2 ةوطخل رز. ok تقطق ط. ةمزالل تامولعمل ري فو تب

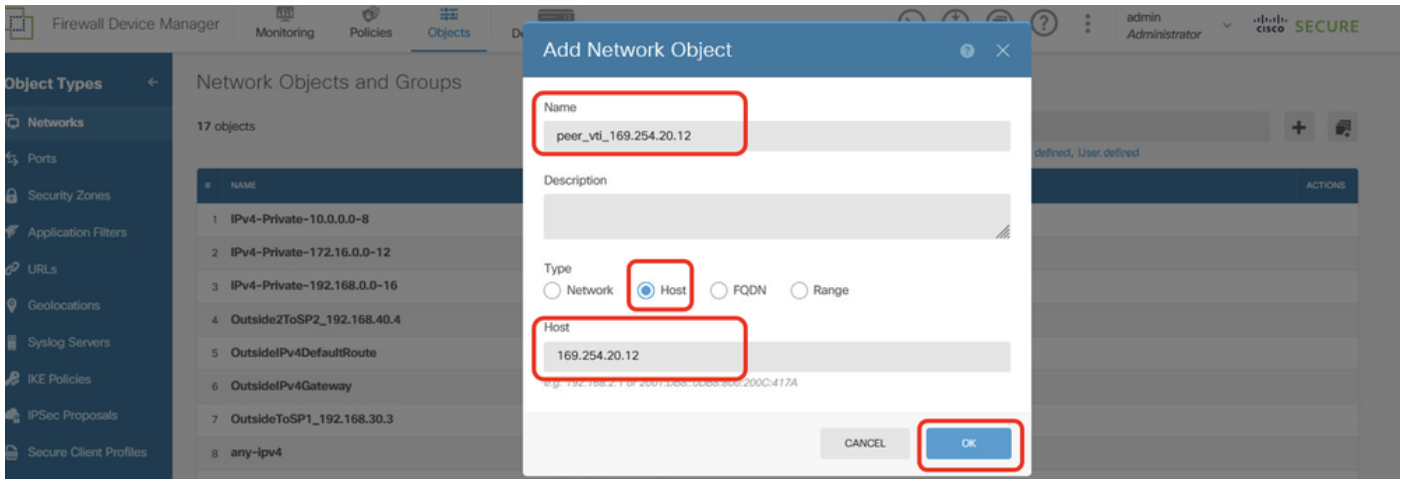
- مرسال: peer_vti_169.254.10.2
- فيضم: عونل
- ةكبشل: 169.254.10.2



Site1FTD_Create_NetObj_StaticRoute_2

مق 2 FTD. ريظننل عقوم ب صاخ ال VTI Tunnel2 ل IP ناونعل نئاك عاشنإب مق 22.3 ةوطخل رز. ok تقطق ط. ةمزالل تامولعمل ري فو تب

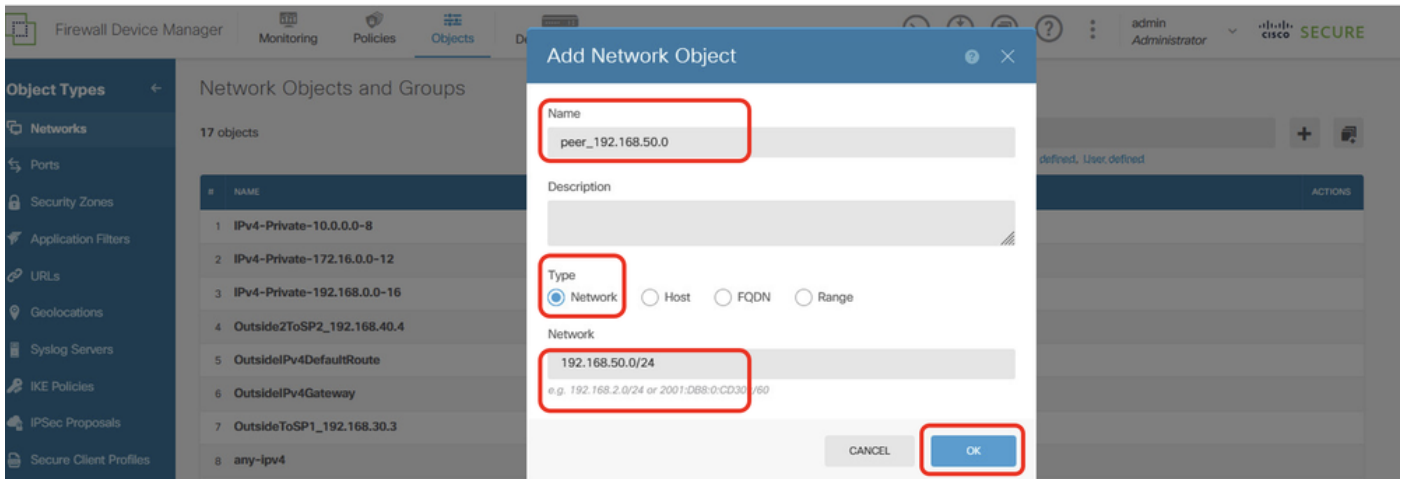
- مرسال: peer_vti_169.254.20.12
- فيضم: عونل
- ةكبشل: 169.254.20.12



Site1FTD_Create_NetObj_StaticRoute_3

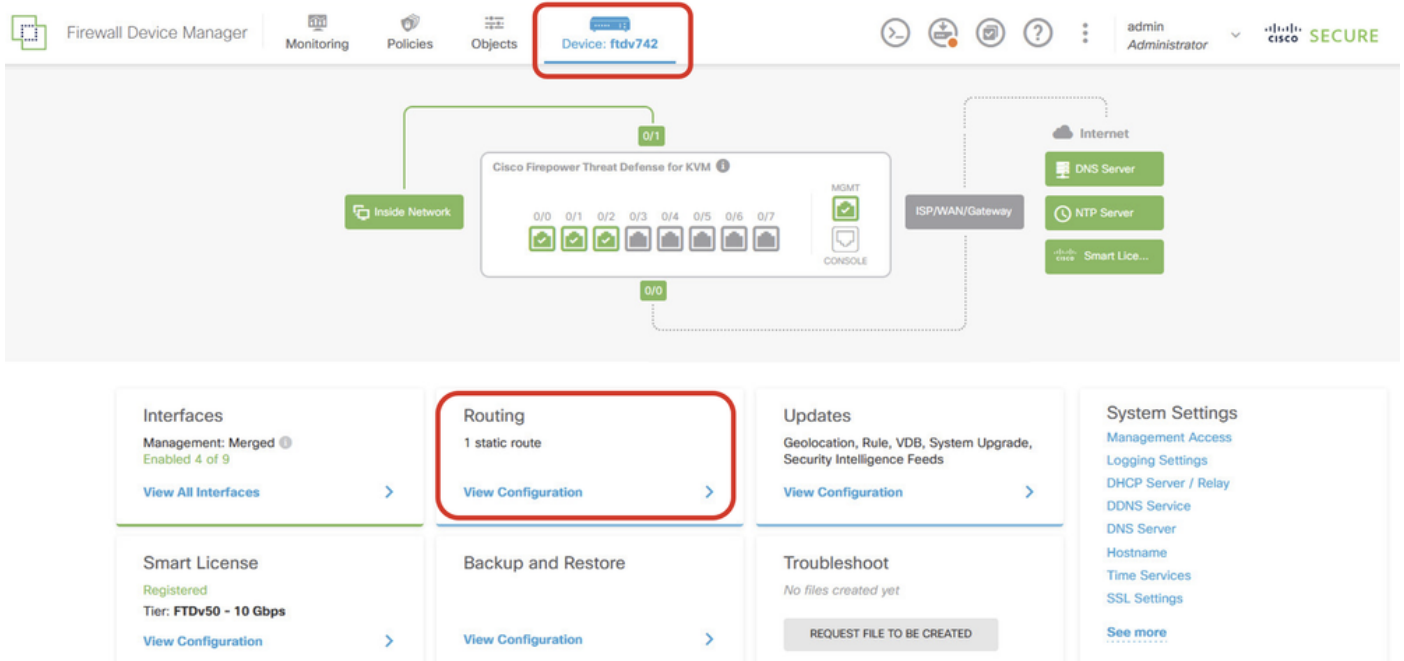
تامولعملالري فو تب مق Peer Site2 FTD ل ةيلخادال ةكبش لل نئاك ءاشنإب مق 22.4 ةوطخلال رز. ok تق طقط . ةي رورضل

- م سالا : peer_192.168.50.0
- ةكبشال : عونلا
- ةكبشال : 192.168.50.0/24



Site1FTD_Create_NetObj_StaticRoute_4

هيجوت بيوبت ةمالع ىلع رقنا . لىكشت ضرع ةق طقط . هيجوت > زا هج ىلإ لقتنا 23 ةوطخلال . ديدج تباث راسم ةفاضلإ رز + قوف رقنا . ةكيتاتسإ نكاس



site1FTD_VIEW_ROUTE_CONFIGURATION



Site1FTD_Add_STATIC_Route

تضرعت اذا SLA. عبقارم عم ISP1 عباوب ماخذتساب يضا رتفا راسم عاشناب مق 23.1. عوطخلا يضا رتفال راسم الى تانايبال رورم كرح تالوحم موقتسف ،ةعطاقم الى ISP1 عباوب ماخذتسا الى تانايبال رورم كرح عجرت ،ISP1 دادرتسا درجم ب ISP2. رب ع يطايتحالال خسنلل ظفحلل "قف اوام رزلا قوف رقنا .ةمزالل تامولعمل ري فو تب مق ISP1.

- مرسال: ToSP1GW
- جراخ :ةهاولا (GigabitEthernet0/0)
- لوكوتوربال: IPv4
- اكاك بشل: IPv4-يأ
- عباوبال: OutsideToSP1_192.168.30.3
- سايقلا: 1
- عي جراخلا (SLA) ةمدخلا يوتسم عي قافات: SLA ةشاش

Add Static Route



Name

ToSP1GW

Description

Interface

outside (GigabitEthernet0/0)

Protocol



IPv4



IPv6

Networks



any-ipv4

Gateway

OutsideToSP1_192.168.30.3

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside

CANCEL

OK

نوكي نأ بجي ISP2. ةبأوب رب ع يضارتفالا يطايتحالاسننلا راسم عاشنإ 23.2 ةوطخلال
رقنا. ةرورضللا تامولعمل ري فوتب مق 2. وه سايقملا، لاثملا اذه في 1. نم يلعلأ سايقملا
ظفحلل "قف اوم رزلال قوف

- DefaultToSP2GW: مسال
- 2(GigabitEthernet0/1) جراخ: ةهجاوال
- IPv4: لوكوتوربل
- IPv4-ي: تالكبشل
- Outside2ToSP2_192.168.40.4: ةبأوبل
- 2: سايقلل

Add Static Route



Name

DefaultToSP2GW

Description

Interface

outside2 (GigabitEthernet0/1)

Protocol



IPv4



IPv6

Networks



any-ipv4

Gateway

Outside2ToSP2_192.168.40.4

Metric

2

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

عقوم ب صاخال IP ناووع 2 چراخ ىلإ هجولا رورم ةكرحل تباث راسم عاشنإب مق 23.3 ةوطخال
Site2 نم 2 چراخ عم VPN عاشنإل ةمدختسملا SLA ةبقارم عم ،ISP2 ةباوب ربع FTD 2 ريظنلا
ظفحلل "قفاووم رزلا قوف رقنا .ةرورضللا تامولعمل ريوفوتب مق .FTD

- مسالا: SpecificToSP2GW
- ةهجاوال (GigabitEthernet0/1)2 چراخ:
- لوكوتوربل IPv4:
- تاكبشل: remote_outside2_192.168.20.1
- ةباوبلا: Outside2ToSP2_192.168.40.4
- سايقلا 1:
- 2يچراخال (SLA) ةمدخللا ىوتسم ةيقافتا: SLA ةشاش

Add Static Route



Name

SpecificToSP2GW

Description

Interface

outside2 (GigabitEthernet0/1)

Protocol

☒ IPv4

☐ IPv6

Networks



remote_outside2_192.168.20.1

Gateway

Outside2ToSP2_192.168.40.4

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside2

CANCEL

OK

ريظننل عقوقم لةيخلخالل ةكبشلل ىلإ ةهجولل رورم ةكرجل تباث راسم عاشنإب مق 23.4 ةوطخلل رورم ةكرج ريفشتل SLA ةبقارم عم ،ةباوبك SITE2 FTD نم 1 VTI ريظننل قفنل ربع 2 FTD ىلإ VPN رورم ةكرج تالوحم هجاوتس ف ،ةعطاقم ISP1 ةباوب تهجاوا اذإ 1. قفنل ربع ليمعمل مق ISP1. نم 1 VTI قفن ىلإ تانايبلا رورم ةكرج عجرت ،ISP1 دادرتسإ درجمب ISP2. نم 2 قفنللا ظفحلل "قفاووم رزلا قوف رقنا .ةمزاللا تامولعمل ريفوتب

- مرسال: ToVTISP1
- ةهجاولل: demovti(Tunnel1)
- لوكوتوربلل: IPv4
- تالكبشلل: peer_192.168.50.0
- ةباوبلل: peer_vti_169.254.10.2
- سايقلل: 1
- ةيجراخلا (SLA) ةمدخلل ىوتسم ةيقافتإ: SLA ةشاش

Add Static Route



Name

ToVTISP1

Description

Interface

demovti (Tunnel1)

Protocol



IPv4



IPv6

Networks



peer_192.168.50.0

Gateway

peer_vti_169.254.10.2

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside

CANCEL

OK

ةكبشلا ىلإ ةهجولا رورم ةكرحل يطايتحال خسنلل تبات راسم عاشنإب مق 23.5 ةوطخل مدختست ،ةباوبك 2 FTD عقوملل 2 ريظنلل VTI قفن ربع 2 FTD ريظنلل عقومل ةيلخادل في 1. نم ىلعأ ةميق ىلإ سايقملا نييعتب مق 2. قفنل ربع ليمعلا رورم ةكرح ريفشتل "قفاوم رزلا قوف رقنا .ةرورضل تامولعمل ريفوتب مق 22. وه سايقملا ،لاثملا اذه ظفحلل.

- مرسال: ToVTISP2_Backup
- ةهجال: demovti_sp2(Tunnel2)
- لوكوتوربل: IPv4
- تالكبشل: peer_192.168.50.0
- ةباوبل: peer_vti_169.254.20.12
- سايقلل: 22

Add Static Route



Name

ToVTISP2_Backup

Description

Interface

demovti_sp2 (Tunnel2)

Protocol



IPv4



IPv6

Networks



peer_192.168.50.0

Gateway

peer_vti_169.254.20.12

Metric

22

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

رَبْع Site2 Client2 ىل إهَجول رورم ةكِرْج. PBR رورم ةكِرْج ل تَبَاث راسم ءاشن إِب مق 23.6 ةوطخل رَقنَا. ةرورضلَا تامولعمل ريفوت SLA ةبقارم عم، ةبَابك Site2 FTD ل Peer VTI Tunnel 2. ظفحلل "قفاوَم رزلَا قوف

- مَسَال: ToVTISP2
- ةَهَاول: demovti_sp2(Tunnel2)
- لوكوتوربَل: IPv4
- تَاكِبَشَل: remote_192.168.50.10
- ةَبَاول: peer_vti_169.254.20.12
- سَايَقَل: 1
- 2ءيجراخلَا (SLA) ةمدخلَا ىوتسم ةيَقَات: SLA ةشاش

Add Static Route



Name

ToVTISP2

Description

Interface

demovti_sp2 (Tunnel2)

Protocol

☒ IPv4

☐ IPv6

Networks



remote_192.168.50.10

Gateway

peer_vti_169.254.20.12

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside2

CANCEL

OK

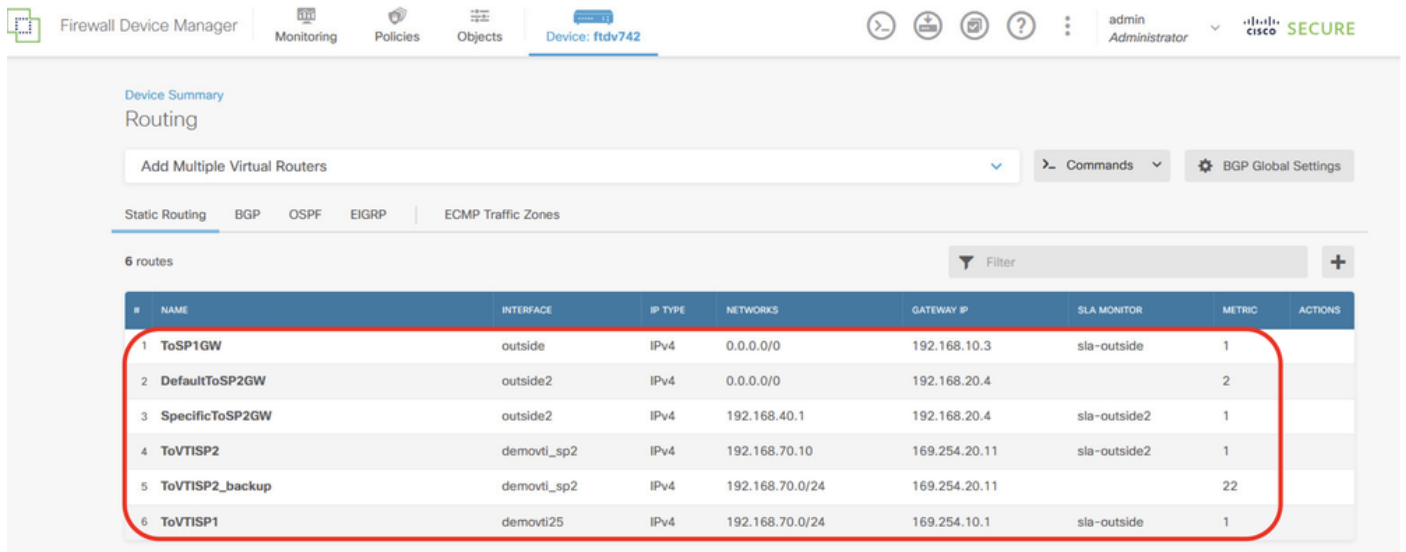
نيوكتال تاريخي غت رشن ب مق. 24 ةوطخلا



site1FTD_DEPLOYMENT_CHANGES

SITE2 FTD ل تباثال راسم ل نيوكت

قلا ب اقم ل تام ل عمل م ادخ تس اب تباث راسم عاشن ل ل ا نم 24 ل ا نم 22 نم تا و طخلا ررك. 25 ةوطخلا ل Site2 FTD.



Site2FTD_Create_StaticRoute

ةحصل ل نم ق قحت ل

(CLI) رم او ال رطس ةه جاو ل ل قتنا. ج حص ل كش ب نيوكتال لم ع ديك اتل مسق ل اذه مدخ تس SSH. و ا م كحتال دحو رب ع Site1 FTD و Site2 FTD ب ة صاخ ل

ديج ل كش ب لم ع ي ISP2 و ISP1 نم ال ك

VPN

//Site1 FTD:

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

IKEv2 SAs:

Session-id:156, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local	Remote
1072332533 192.168.30.1/500	192.168.10.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK	
Life/Active Time: 86400/44895 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: 0xec031247/0xc2f3f549

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote
1045734377 192.168.40.1/500 192.168.20.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/77860 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: 0x47bfa607/0x82e8781d

// Site2 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:44, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote
499259237 192.168.10.1/500 192.168.30.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/44985 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: 0xc2f3f549/0xec031247

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote
477599833 192.168.20.1/500 192.168.40.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/77950 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: 0x82e8781d/0x47bfa607

قيرط

// Site1 FTD:

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
C       169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L       169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S       192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
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
C       192.168.40.0 255.255.255.0 is directly connected, outside2
L       192.168.40.1 255.255.255.255 is directly connected, outside2
S       192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
S       192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C       192.168.70.0 255.255.255.0 is directly connected, inside
L       192.168.70.1 255.255.255.255 is directly connected, inside
```

// Site2 FTD:

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 192.168.10.3 to network 0.0.0.0

```
S*      0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C       169.254.10.0 255.255.255.0 is directly connected, demovti25
L       169.254.10.2 255.255.255.255 is directly connected, demovti25
C       169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L       169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C       192.168.10.0 255.255.255.0 is directly connected, outside
L       192.168.10.1 255.255.255.255 is directly connected, outside
C       192.168.20.0 255.255.255.0 is directly connected, outside2
L       192.168.20.1 255.255.255.255 is directly connected, outside2
S       192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C       192.168.50.0 255.255.255.0 is directly connected, inside
L       192.168.50.1 255.255.255.255 is directly connected, inside
S       192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
S       192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

SLA عشان

// Site1 FTD:

ftdv742# show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 188426425
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.40.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 855903900
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.30.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.173 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30 RTTMin: 30 RTTMax: 30
NumOfRTT: 1 RTTSum: 30 RTTSum2: 900

Entry number: 855903900
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.178 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30 RTTMin: 30 RTTMax: 30
NumOfRTT: 1 RTTSum: 30 RTTSum2: 900

// Site2 FTD:

ftdv742# show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 550063734
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.20.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 609724264
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.10.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never

Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

```
ftdv742# show sla monitor operational-state
Entry number: 550063734
Modification time: 09:05:52.864 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.916 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100
```

```
Entry number: 609724264
Modification time: 09:05:52.856 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.921 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100
```

غ ن ب ر ا ب ت خ |

1. Site1 Client1 ping Site2 Client1.

Site1 على inc:|encap|decap | show crypto ipSec |، الاصل الى ر ا ب ت خ | ل ب ق
FTD.

ة. ل س ب ك ل ل ز ع ل ة م ز ح 1498 و ن ي م ض ت ل ا ة ي ل م ع ل ة م ز ح 1497 ق ف ن ل ل ض ر ع ي ، ل ا ث م ل ا ذ ه ي ف

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 1497, #pkts encrypt: 1497, #pkts digest: 1497
    #pkts decaps: 1498, #pkts decrypt: 1498, #pkts verify: 1498
```

```
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
#pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
#pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

حاجنب Site1 Client1 ping Site2 Client1

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/97/227 ms
```

رابتخ|دعب Site1 FTD ىلع inc:|encap|decap ةهجاو | show crypto ipSec sa تادادع نم ققحت حاجنب لاصتالا

الك عم، ةلسبك عطقل طبر 1503 و ةلسبك ةيلمعل طبر 1502 قفن يدبي، لاثم اذه يف هيجوت متي هنا ىلى ريشي اذهو. بلط يدص زيزا ةيلمع 5 ل لثامي، طبر 5 ب ديزي نراق يف ةدايزي 2 قفنل رهظي ال. ISP1 قفن ربع Site2 Client1 ىلى Site1 Client1 لاصتا تارابتخ| هذه رورملا ةكرحل همادختس| متي ال هنا دكؤي امم، ةلسبكلا ةلازا و اني مضا تادادع

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
#pkts encaps: 1502, #pkts encrypt: 1502, #pkts digest: 1502
#pkts decaps: 1503, #pkts decrypt: 1503, #pkts verify: 1503
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
#pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
#pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

ويرانيسل 2. Site1 Client2 ping Site2 Client2.

Site1 فTD ىلع inc:|encap|decap ةهجاو | show crypto ipSec تادادع نم ققحت، لاصتالا رابتخ| لبق FTD.

ةلسبكلا ةلازال ةمزح 20 و ني مضا تال ةيلمعل ةمزح 21 قفنل ضرعي، لاثملا اذه يف

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
#pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
```

```
#pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
#pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
#pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

حاجن ب Site2 Client2 Ping Site1 Client2

```
Site1_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 = 4/39/87 ms
```

رابتخا دع ب Site1 FTD ىل ع |encap|decap inc: |show crypto ipSec sa | تادادع نم ققحت
حاجن ب لاصتالا

5 ب دي زي نراق الك عم ،لزع ل طبر 25 و ةلسبك ةي لمعل طبر 26 ق فن ي دبي ،لاثم اذه ي ف
ىل Site1 Client2 لاصتات تارابتخا نأ ىل ري شي اذهو .بل ط يدص زى ةي لمع 5 ل لثامى ،طبر
ني مضتلا تادادع ي ف ةدايز ةي 1 ق فن ل رهظي ال .2 ISP ق فن ربع اههيجوت متي Site2 Client2
هذه رورملا ةكرحل همادختسا متي ال هنا دكوي امم ،ةلسبكلا ةلازا وأ

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface: |encap|decap
interface: demovti
#pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
#pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
#pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
#pkts decaps: 25, #pkts decrypt: 25, #pkts verify: 25
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

ديج وحن ىل ع ISP2 لمع ءانثأ ةعطاقم ISP1 هجاوي

هجاوي ي ذل ISP1 ةكاحم ل ISP1 ىل ع E0/1 هجاو ل ي ودي ل لي غشتلا فاقيا ب مق ،لاثم ل اذه ي ف
ةعطاقم.

```
Internet_SP1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Internet_SP1(config)#
Internet_SP1(config)#interface E0/1
Internet_SP1(config-if)#shutdown
Internet_SP1(config-if)#exit
```

Internet_SP1(config)#

VPN

IKEv2 SA. عم اشن طقف Tunnel2 نوئي 1. قف لل لزن

// Site1 FTD:

```
ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
  IP address 169.254.10.1, subnet mask 255.255.255.0
Tunnel Interface Information:
  Source interface: outside    IP address: 192.168.30.1
  Destination IP address: 192.168.10.1
  IPsec MTU Overhead : 0
  Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
```

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local	Remote
1045734377 192.168.40.1/500	192.168.20.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK	
Life/Active Time: 86400/80266 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: 0x47bfa607/0x82e8781d	

// Site2 FTD:

```
ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti25", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
  IP address 169.254.10.2, subnet mask 255.255.255.0
Tunnel Interface Information:
  Source interface: outside    IP address: 192.168.10.1
  Destination IP address: 192.168.30.1
  IPsec MTU Overhead : 0
  Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
ftdv742#
```

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local	Remote
477599833 192.168.20.1/500	192.168.40.1/500

```
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/80382 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: 0x82e8781d/0x47bfa607
```

قيرط

يطايت حال خسننل تاراسم ليعفت متي، هي جوتل لودج في

```
// Site1 FTD:
```

```
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 192.168.40.4 to network 0.0.0.0
```

```
S*      0.0.0.0 0.0.0.0 [2/0] via 192.168.40.4, outside2
C       169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L       169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S       192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
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
C       192.168.40.0 255.255.255.0 is directly connected, outside2
L       192.168.40.1 255.255.255.255 is directly connected, outside2
S       192.168.50.0 255.255.255.0 [22/0] via 169.254.20.12, demovti_sp2
S       192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C       192.168.70.0 255.255.255.0 is directly connected, inside
L       192.168.70.1 255.255.255.255 is directly connected, inside
```

```
// Site2 FTD:
```

```
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 192.168.10.3 to network 0.0.0.0
```

```
S*      0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C       169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L       169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
```

```
C      192.168.10.0 255.255.255.0 is directly connected, outside
L      192.168.10.1 255.255.255.255 is directly connected, outside
C      192.168.20.0 255.255.255.0 is directly connected, outside2
L      192.168.20.1 255.255.255.255 is directly connected, outside2
S      192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C      192.168.50.0 255.255.255.0 is directly connected, inside
L      192.168.50.1 255.255.255.255 is directly connected, inside
S      192.168.70.0 255.255.255.0 [22/0] via 169.254.20.11, demovti_sp2
S      192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

SLA ةشاش

ل (192.168.30.3 وه فدهل ناونعلا) 855903900 لاخدإلا ةلهم SLA ةشاش رهظت، Site1 FTD يي ISP1.

// Site1 FTD:

```
ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.131 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 100
Latest operation start time: 14:22:05.132 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 100    RTTMin: 100    RTTMax: 100
NumOfRTT: 1    RTTSum: 100    RTTSum2: 10000
```

```
Entry number: 855903900
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:22:05.134 UTC Thu Aug 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0
```

```
ftdv742# show track
Track 1
```

```
Response Time Reporter 855903900 reachability
Reachability is Down
7 changes, last change 00:11:03
Latest operation return code: Timeout
Tracked by:
  STATIC-IP-ROUTING 0
Track 2
Response Time Reporter 188426425 reachability
Reachability is Up
4 changes, last change 13:15:11
Latest operation return code: OK
Latest RTT (milliseconds) 140
Tracked by:
  STATIC-IP-ROUTING 0
```

غنيب رابتخا

Site1 ىلع inc:|encap|decap ةهجاو | show crypto ipSec تادادع نم ققحت ،لاصتالا رابتخا لبق FTD.

ةلسبكلا ةلازال ةمزح 35 و ني مضتلا ةيلمعل ةمزح Tunnel2 36 ضرعي ،لاثملا اذه ي ف.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
  #pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
  #pkts decaps: 35, #pkts decrypt: 35, #pkts verify: 35
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

حاجنب Site2 Client1 ping Site1 Client1.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/133/253 ms
```

حاجنب Site2 Client2 Ping Site1 Client2.

```
Site1_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 = 34/56/87 ms
```

رابطه دعب Site1 FTD ىلع |encap|decap | inc: |هجاو | show crypto ipSec sa | تادادع نم ققحت
حاجنب لاصتالا

نراق الك عم، ةلسبكلا كفل طبر 45 و ةلسبك ةيلمعل طبر 46 قفن يدبي، لاثم اذه في
رابطه مزح هيحوت ىل ريشي اذهو. بلط يدص زبأ ةيلمع 10 لا لثامي، طبر 10 ب ديزي
ISP2 2. قفن ربع لاصتالا

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
    #pkts encaps: 46, #pkts encrypt: 46, #pkts digest: 46
    #pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

ديج لكشب ISP1 لمع ءانثأة عطاقم ISP2 هجاوي

هجاوي يذلا ISP2 ةاكاحمل ISP2 ىلع E0/1 ةهجاو لل يودي لا ليغشتلا فاقيا ب مق، لاثملا اذه في
ةعطاقم.

```
Internet_SP2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Internet_SP2(config)#
Internet_SP2(config)#int e0/1
Internet_SP2(config-if)#shutdown
Internet_SP2(config-if)#^Z
Internet_SP2#
```

VPN

SA. IKEV2 عم اطشن طقف Tunnel1 نوكي. 2. قفنلا لزن

// Site1 FTD:

```
ftdv742# show interface tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
IP address 169.254.20.11, subnet mask 255.255.255.0
Tunnel Interface Information:
Source interface: outside2    IP address: 192.168.40.1
Destination IP address: 192.168.20.1
IPsec MTU Overhead : 0
Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
```

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

IKEv2 SAs:

Session-id:159, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
1375077093 192.168.30.1/500 192.168.10.1/500
  Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
  Life/Active Time: 86400/349 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: 0x40f407b4/0x26598bcc
```

// Site2 FTD:

```
ftdv742# show int tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel MAC address N/A, MTU 1500
  IP address 169.254.20.12, subnet mask 255.255.255.0
Tunnel Interface Information:
  Source interface: outside2 IP address: 192.168.20.1
  Destination IP address: 192.168.40.1
  IPsec MTU Overhead : 0
  Mode: ipsec ipv4 IPsec profile: ipsec_profile|e4084d322d
```

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:165, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
1025640731 192.168.10.1/500 192.168.30.1/500
  Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
  Life/Active Time: 86400/379 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: 0x26598bcc/0x40f407b4
```

قيرط

PBR. رورم ةكرحل ISP2 ب طبت رمل راسم ل يفتخي، تاراسم ل لودج ي ف

// Site1 FTD:

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
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
C     192.168.40.0 255.255.255.0 is directly connected, outside2
L     192.168.40.1 255.255.255.255 is directly connected, outside2
S     192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
C     192.168.70.0 255.255.255.0 is directly connected, inside
L     192.168.70.1 255.255.255.255 is directly connected, inside
```

// Site2 FTD:

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 192.168.10.3 to network 0.0.0.0

```
S*    0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C     169.254.10.0 255.255.255.0 is directly connected, demovti25
L     169.254.10.2 255.255.255.255 is directly connected, demovti25
C     192.168.10.0 255.255.255.0 is directly connected, outside
L     192.168.10.1 255.255.255.255 is directly connected, outside
C     192.168.20.0 255.255.255.0 is directly connected, outside2
L     192.168.20.1 255.255.255.255 is directly connected, outside2
S     192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C     192.168.50.0 255.255.255.0 is directly connected, inside
L     192.168.50.1 255.255.255.255 is directly connected, inside
S     192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
```

عشاش SLA

ل (192.168.40.4) فدهل ناوعلا 188426425 لاخدإل اقلهم SLA بردم رهظي، Site1 FTD ي ف ISP2.

// Site1 FTD:

```
ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
```

Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:52:05.174 UTC Thu Aug 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0 RTTMin: 0 RTTMax: 0
NumOfRTT: 0 RTTSum: 0 RTTSum2: 0

Entry number: 855903900
Modification time: 08:37:05.135 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 10
Latest operation start time: 14:52:05.177 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 10 RTTMin: 10 RTTMax: 10
NumOfRTT: 1 RTTSum: 10 RTTSum2: 100

ftdv742# show track

Track 1

Response Time Reporter 855903900 reachability
Reachability is Up
8 changes, last change 00:14:37
Latest operation return code: OK
Latest RTT (millisecs) 60
Tracked by:
STATIC-IP-ROUTING 0

Track 2

Response Time Reporter 188426425 reachability
Reachability is Down
5 changes, last change 00:09:30
Latest operation return code: Timeout
Tracked by:
STATIC-IP-ROUTING 0

غنيب رابتخا

Site1 ىلع inc|encap|decap ةهجاو | show crypto ipSec تادادع نم ققحت ،لاصتالا رابتخا لب ق
FTD.

ةلسبكلا كفل طبر 73 و ةلسبك ةيلمعل طبر 174 ق فن يدبي ،لاثم اذه ي ف

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 74, #pkts encrypt: 74, #pkts digest: 74
    #pkts decaps: 73, #pkts decrypt: 73, #pkts verify: 73
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

حاجنب Site1 Client1 ping Site2 Client1

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/158/255 ms
```

حاجنب Site1 Client2 Ping Site2 Client2

```
Site1_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 = 6/58/143 ms
```

رابتخا دعب Site1 FTD ىلع inc:|encap|decap ةهجاو | show crypto ipSec sa تادادع نم ققحت حاجنب لاصتالا

10 ب دي زي نراق الك عم ،لزعل طبر 83 و ةلسبك ةيلمعل طبر 84 1 ق فن يدبي ،لاثم اذه ي ربع لاصتالا رابتخا مزح هي جوت ىلا ريشي اذهو .بلط يدص زيزا ةيلمع 10 لا لثامي ،طبر 1 ISP1 ق فن

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 84, #pkts encrypt: 84, #pkts digest: 84
    #pkts decaps: 83, #pkts decrypt: 83, #pkts verify: 83
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

اهحالصا وءاطخالا فاشكتسا

اهحالصا ونيوكتالا ءاطخا فاشكتسال اهمادختسا كنكمي تامولعم مسقلا اذه رفوي

مسق VPN لا تي رحت in order to رمأ طبضي اذه تلمعتسا عي طتسي تنأ

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

مسق PBR لا یرحتي نأ رمأ طبضي اذه تلمعتسا عي طتسي تنأ

```
debug policy-route
```

مسق بردم SLA لا یرحتي نأ رمأ طبضي اذه تلمعتسا عي طتسي تنأ

```
ftdv742# debug sla monitor ?
error   Output IP SLA Monitor Error Messages
trace   Output IP SLA Monitor Trace Messages
```

ةمچرتل هذه ل و ح

ةل آل ا ت ا ي 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 ي 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 ل آل ا 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