

رَبْع AnyConnect to Access Server نيوك تَب مق ق IPsec فن

تايوت حمل

ةم دق م ل ا

ةي س اس ا ل ا ت ا ب ل ط ت م ل ا

ةي س اس ا ل ا ت ا ب ل ط ت م ل ا

ةم د خ ت س م ل ا ت ا ن و ك م ل ا

ة ك ب ش ل ل ا ي ط ي ط خ ت ل ا م س ر ل ا

FMC ل ع ت ا ن ي و ك ت ل ا

FMC ة ط س ا و ب ه ت ر ا د ا م ت ت ي ذ ل ا FTD ل ع ر AVPN نيوك ت

FMC ة ط س ا و ب FTD ة ر ا د ا ل ع IKEv2 VPN

ة ح ص ل ا ن م ق ق ح ت ل ا

ا ه ج ا ل ص ا و ا ط خ ا ل ا ف ا ش ك ت س ا

ةم دق م ل ا

ق ف ن و FMC ة ط س ا و ب ه ت ر ا د ا م ت ت ي ذ ل ا FTD ل ع RAPN د ا د ع ر ش ن ت ا ع ا ر ج د ن ت س م ل ا ا ذ ه ف ص ي
FTDs ني ب ع ق و م ل ا ع ق و م ن م

ةي س اس ا ل ا ت ا ب ل ط ت م ل ا

ةي س اس ا ل ا ت ا ب ل ط ت م ل ا

- ة ك ب ش ل ل ا و (VPN) ة ي ر ه ا ط ل ا ة ص ا خ ل ا ت ا ك ب ش ل ل ا ي س ا س ا م ه ف ل ا ل ص و ت ل ا د ي ف م ل ا ن م و
ع ق و م ل ا ع ق و م ن م (RAVPN) ة ي ر ه ا ط ل ا ة ص ا خ ل ا
- ل ع IKEv2 ة س ا ي س ل ا د ن ت س ي ق ف ن ني و ك ت ل ا ة م ز ا ل ل ا س س ا ل ا م ه ف ي ر و ر ض ل ا ن م
Cisco Firepower ة ص ن م

ن م ق ف ن و FMC ة ط س ا و ب ه ت ر ا د ا م ت ت ي ذ ل ا FTD ل ع RAPN د ا د ع ر ش ن و ه ع ا ر ج ل ا ا ذ ه ن م ض ر غ ل ا
ف ل خ م د ا خ ل ا ل ا ل ا ل و ص و ل ا AnyConnect م د خ ت س م ل ن ك م ي ش ي ح FTDs ني ب ع ق و م ل ا ع ق و م
FTD ل ر خ ا ل ا ر ي ط ن ل ا

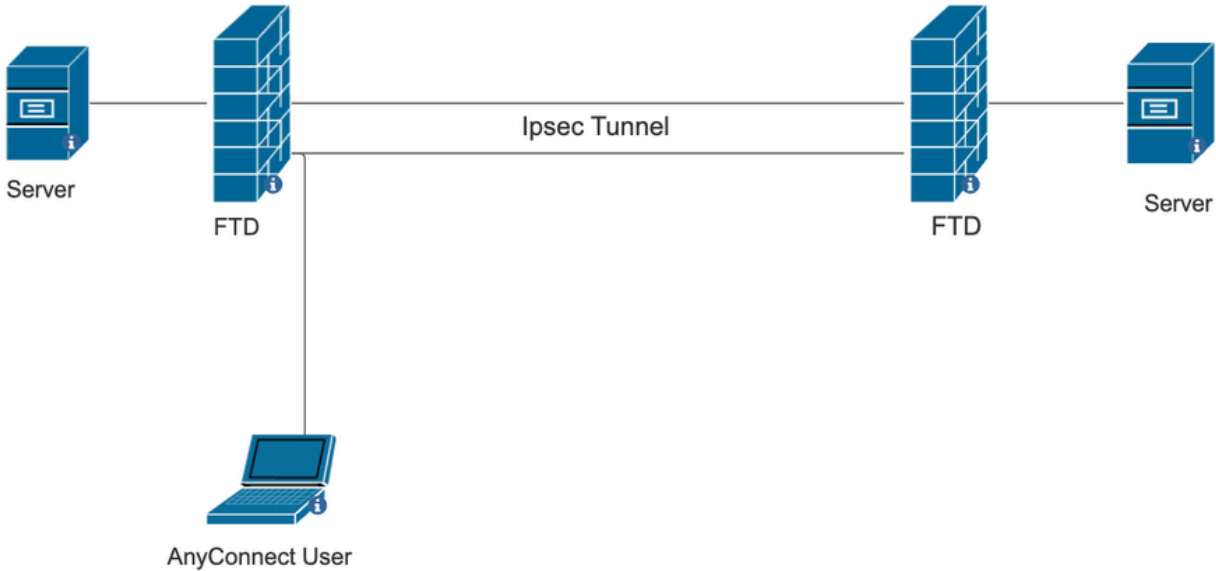
ةم د خ ت س م ل ا ت ا ن و ك م ل ا

- 7.0.0 ر ا د ص ل ا Cisco: ن م VMware ل FirePOWER د ي د ه ت د ض ع ا ف د ل ا ج م ا ن ر ب
- 7.2.4 ر ا د ص ل ا Firepower: ة ر ا د ا ز ك ر م (169 ة ي ن ب)

ة ص ا خ ة ي ل م ع م ة ئ ي ب ي ف ة د و ج و م ل ا ة ز ه ا ل ا ن م د ن ت س م ل ا ا ذ ه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا ع ا ش ن ا م ت
ت ن ا ك ا ذ ا (ي ض ا ر ت ف ا) ح و س م م ني و ك ت ت د ن ت س م ل ا ا ذ ه ي ف ة م د خ ت س م ل ا ة ز ه ا ل ا ع ي م ج ت ا د ب

..رمأ يأل لم تحملا ريثأتلل كمهف نم دكأتف ،ةرشابم كتككباش

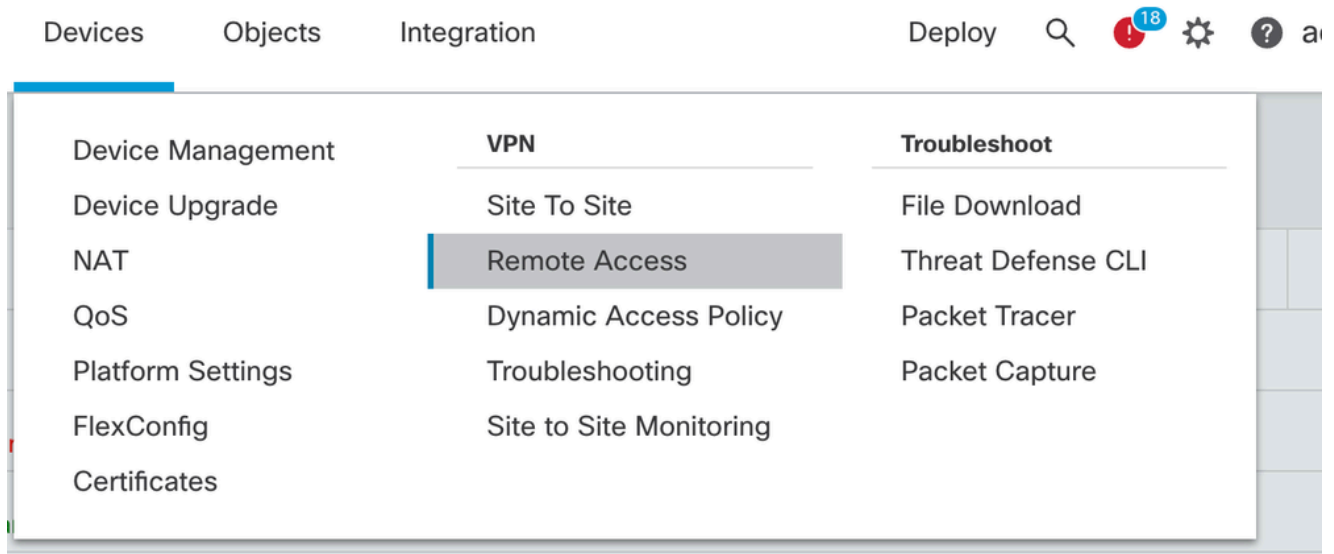
ةكبش لل يطي طختلا مسرلا



FMC يلع تانيوكتلا

FMC ةطساوب هترادإ متت يذلا FTD يلع RAVPN نيوكت

1. دعب نع لوصولا > ةزهجالا يلا لقتنا.



2. (Add) ةفاضل قوف رقنا.

3. يلاتلا قوف رقناو ةحاتملا ةزهجالا نم FTD دحو مسانيوكتب مق.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:*
RAVPN

Description:

VPN Protocols:

SSL
 IPsec-IKEv2

Targeted Devices:

Available Devices	Selected Devices
<input type="text" value="Search"/> 10.106.50.55 10.88.146.35 New_FTD	10.106.50.55

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure [LOCAL](#) or [Realm](#) or [RADIUS Server Group](#) or [SSO](#) to authenticate VPN clients.

AnyConnect Client Package

Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted [devices](#) so that they can be used as a security zone or interface group to enable VPN access.

4. قداصلم لبولسأرتخا وليصوت فيصوت مسا نيوكتب مق .

بساحم ل او ضيوفت لاو قداصلم لم دختسن ، هذه نيوكت لا ة ني عمل بسن ل اب : ة طحالم كتابلطتم ل ا ادانتسا نيوكت ل اب مق ، كلذ عمو . ة ل حملم ة قداصلم ل او طقف (AAA)

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:* RAVPN

This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: AAA Only

Authentication Server:* LOCAL (LOCAL or Realm or RADIUS)

Local Realm:* sid_tes_local

Authorization Server: (Realm or RADIUS)

Accounting Server: (RADIUS)

5. AnyConnect ل IP ناو نع نييعتل هم ادختسا متي يذلا VPN عمجت نيوكتب مق .

(RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ●

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: 

IPv6 Address Pools: 

6. ةومجملا جهن مسا ةفاضلا. ةومجم جهن عاشنإل + قوف رقنا. ةومجملا جهن عاشنإ.

Edit Group Policy ?

Name:*

Description:

General AnyConnect Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

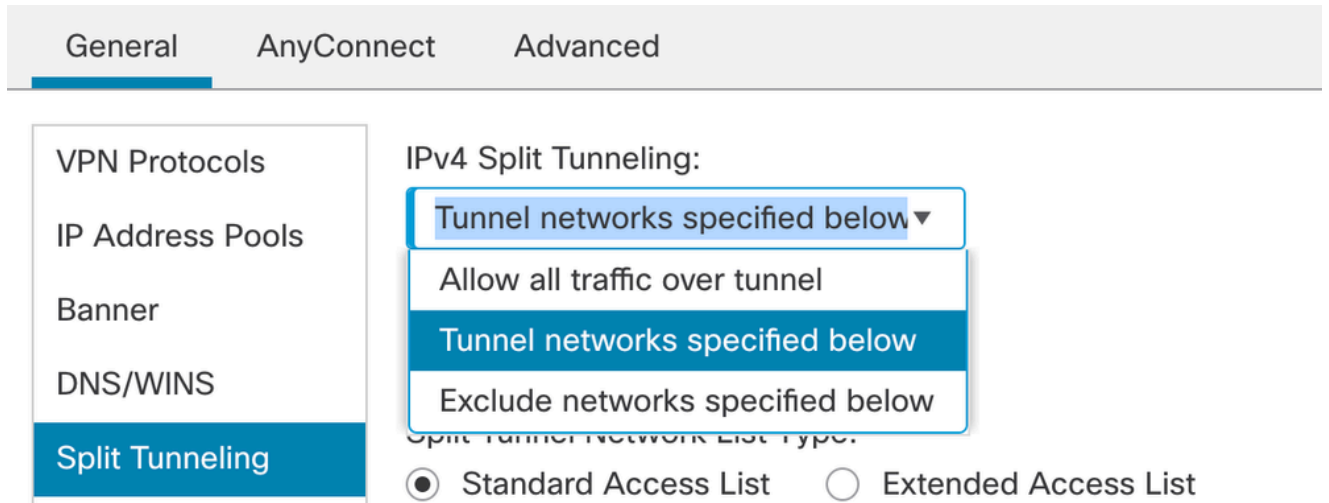
Split Tunneling

VPN Tunnel Protocol:
Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

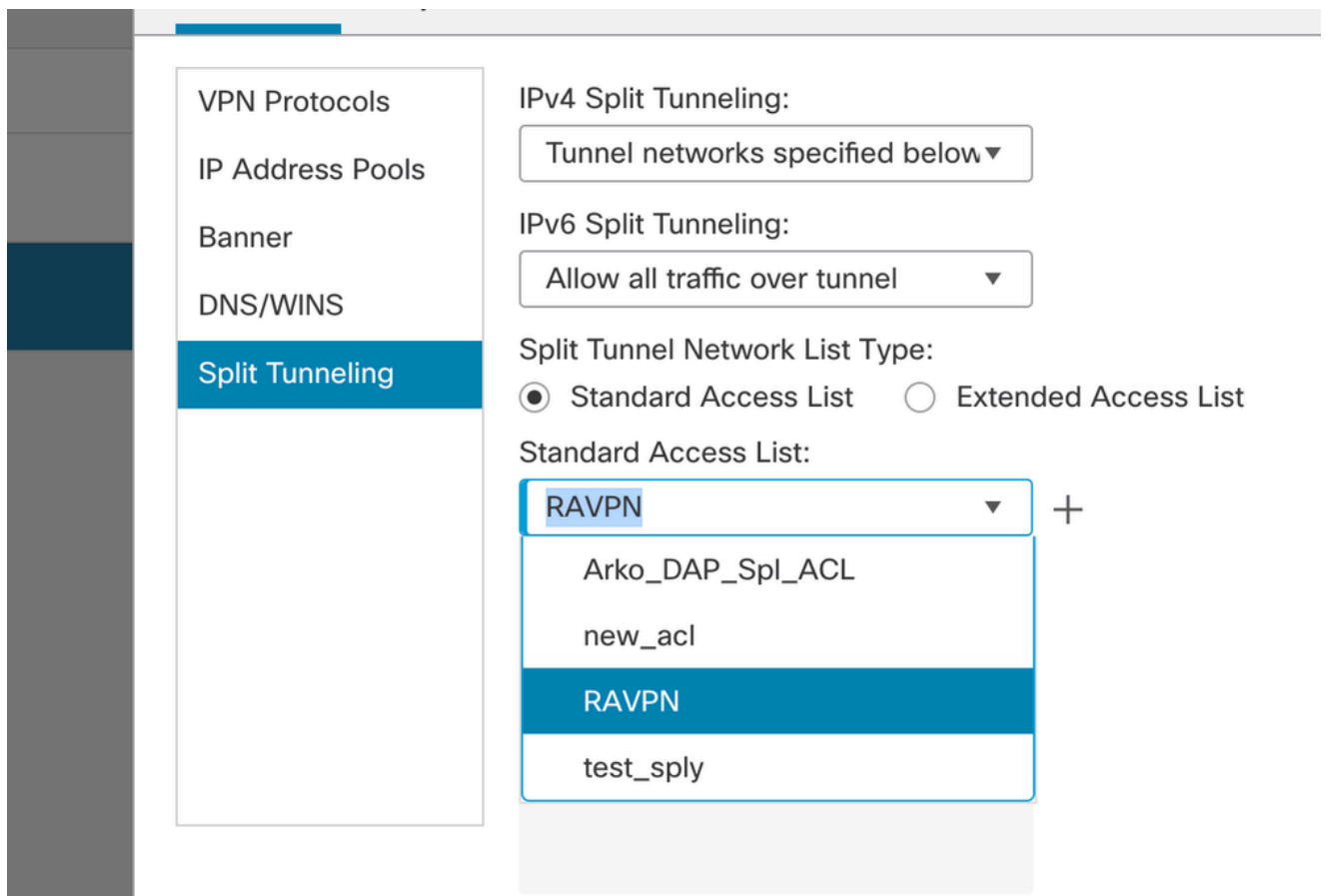
SSL

IPsec-IKEv2

7. انه ةدجملا قفنلا تاكبش دح. مسقنملا يقفنلا لاصتالا للاقنا.



8. مكحت ةمئاق نيوكت متي مل اذا. ةلدسنملا ةمئاقلا نم ةحيجصلا لوصولا ةمئاق ددح ةيسايقلا لوصولا ةمئاق ةفاضل + ةنوقيأ قوف رقنا: لعفلا ب (ACL) لوصولا يف ةديج لوصولو ةمئاق عاشنإو ظفح قوف رقنا.



9. يلاتلا قوف رقناو ةفاضل متت يذلا ةعومجملا جهن ددح.

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* +

[Edit Group Policy](#)

10. AnyConnect ةروص ددح.

AnyConnect Client Image

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

[Show Re-order buttons](#) +

<input type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input type="checkbox"/>	anyconnect	anyconnect410.pkg	Windows
<input checked="" type="checkbox"/>	anyconnect-win-4.10.07073-we...	anyconnect-win-4.10.07073-webdeploy-k9...	Windows
<input type="checkbox"/>	secure_client_5-1-2	cisco-secure-client-win-5_1_2_42-webde...	Windows

11. چهن ددحو، ةداهشلا ةفاضإب مقو، AnyConnect لاصتال اهنكمت بجي يتلا ةهجاولال ددح. قوف رقن او، اهري فشت ك ف مت يتلا رورملا ةكرحل يفافتلال لوصولال يف مكحتلال يتلا.

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* +
 Enable DTLS on member interfaces

⚠ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

زاجن اة ق ط و ل ي ك ش ت ل ا ت ع ج ا ر . 12.

Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name:	RAVPN
Device Targets:	10.106.50.55
Connection Profile:	RAVPN
Connection Alias:	RAVPN
AAA:	
Authentication Method:	AAA Only
Authentication Server:	sid_tes_local (Local)
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn_pool
Address Pools (IPv6):	-
Group Policy:	DfltGrpPolicy
AnyConnect Images:	anyconnect-win-4.10.07073-webdeploy-k9.pkg
Interface Objects:	sid_outside
Device Certificates:	cert1_1

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update**
An **Access Control** rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption**
If NAT is enabled on the targeted devices, you must define a **NAT Policy** to exempt VPN traffic.
- DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using **FlexConfig Policy** on the targeted devices.
- Port Configuration**
SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Anyconnect image download. NAT-Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in **NAT Policy** or other services before deploying the configuration.

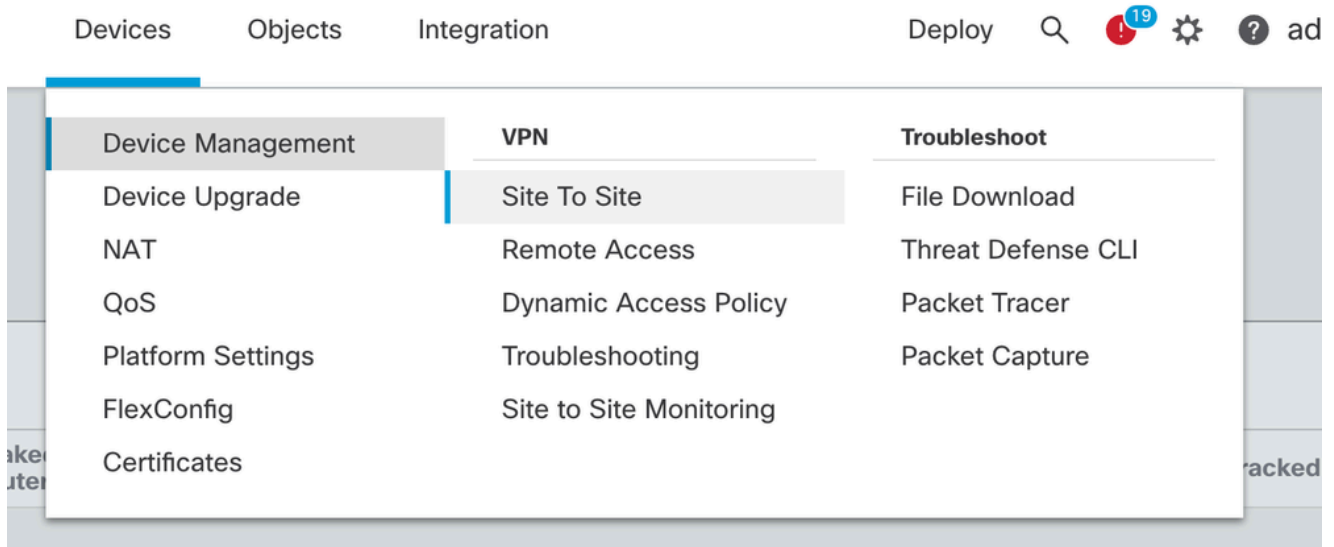
Cancel Back Finish

رشن و ظ ف ح ق و ف ر ق ن ا . 13.

RAVPN		You have unsaved changes Save Cancel	
Enter Description		Policy Assignments (1)	
Connection Profile		Local Realm: New_Realm	
Access Interfaces		Dynamic Access Policy: None	
Advanced			
Name	AAA	Group Policy	
DefaultWEBVpnGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy	
RAVPN	Authentication: LOCAL Authorization: None Accounting: None	RAVPN	

IKEv2 VPN FMC ةطساوب FTD ةرادإ ىلع:

1. ةقوم ىلإ ةقوم > ةزهجألا ىلإ لقتنا.



2. ةفاضل قوف رقنا (Add).

3. ةدق لىل + رقنا A:

Center

Create New VPN Topology

Topology Name:*

Policy Based (Crypto Map)
 Route Based (VTI)

Network Topology:

IKE Version:*

IKEv1
 IKEv2

Endpoints IKE IPsec Advanced

Node A: +

Device Name	VPN Interface	Protected Networks	

Node B: +

Device Name	VPN Interface	Protected Networks	

4. بجي يتلا ةي لحمل ةي عرفلا ةكبشلا ةفاضاب مقو ، ةهجاو لا ددحو ، زاهجال نم FTD ددح ،
 VPN) عمجت نيوانع ىلع اضيا يوتحت ، ةلاجال هذه يفو) IPsec قف لالخنم اهري فشت
 قفاوم قوف رقناو .

Edit Endpoint



Device:*

10.106.50.55

Interface:*

outside1

IP Address:*

10.106.52.104

This IP is Private

Connection Type:

Bidirectional

Certificate Map:

+

Protected Networks:*

Subnet / IP Address (Network) Access List (Extended)

FTD-Lan

VPN_Pool_Subnet



5. بةدقعلل + قوف رقنا .

رظنللا زاهج مسا طعأو، زاهجال نم تنارتسكإ دح >

لوصولا مزلي يتلا ةديعبلا ةعرفلا ةكبشلا ةفاضل او رظنلا لىصافت نيوكت <
قف اوم قوف رقناو (VPN) ةيرهاظلا ةصاخلا ةكبشلا قفن ربع اهليل

Edit Endpoint ?

Device:*

Device Name:*

IP Address:*
 Static Dynamic

Certificate Map:
 +

Protected Networks:*
 Subnet / IP Address (Network) Access List (Extended)

Remote-Lan2 +

Remote-Lan +

6. كتاب لطلتمل اق فو IKEv2 تادادع | نيوكتب مق: IKE بيوبتلا ةمالع قوف رقنا .

Edit VPN Topology



Topology Name:*

FTD-S2S-FTD

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

Point to Point Hub and Spoke Full Mesh

IKE Version:*

IKEv1

IKEv2

Endpoints **IKE** IPsec Advanced

IKEv2 Settings

Policies:*

FTD-ASA

Authentication Type:

Pre-shared Manual Key

Key:*

.....

Confirm Key:*

.....

Enforce hex-based pre-shared key only

Cancel

Save

7. كتاب لطلتمل اق فو IPsec تادادع| نيوكتب مق: IPsec بيوبت لة مالع قوف رقنا .

Edit VPN Topology



Topology Name:*
FTD-S2S-FTD

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:
 Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE **IPsec** Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

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

Modulus Group:

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)
Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

8. (يراي تخ) مامته الة رير ثمل رورم الة كرحل NAT-Exempt ني وكت
NAT > ةزه جأل الة ل ع رقنا

Devices Objects Integration Deploy

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

9. الة ل لوصول اب ني ل خ ادل ني مدخت سمل او RAVPN ل انه ه ني وكت مت ي ذل NAT حم سي
S2S IPsec ق فن لال خ نم مداوخل

						Original Packet			Translated Packet				
<input type="checkbox"/>	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
<input type="checkbox"/>	3	→	Static	sid_outside	sid_outside	VPN_Pool_Subnet	Remote-Lan		VPN_Pool_Subnet	Remote-Lan		Dns: false route-lookup no-proxy-arp	
<input type="checkbox"/>	4	→	Static	sid_inside	sid_outside	FTD-Lan	Remote-Lan2		FTD-Lan	Remote-Lan2		Dns: false route-lookup no-proxy-arp	
<input type="checkbox"/>	5	→	Static	sid_inside	sid_outside	FTD-Lan	Remote-Lan		FTD-Lan	Remote-Lan		Dns: false route-lookup no-proxy-arp	

10. م تيسر يذال S2S ق فنب صاخلا ريظنلل رخآلا فرطلا ىلع نيوكتلاب مق، لثملابو هؤاشنإ.

تاكبشلا وأري فشتلل (ACL) لوصولا يف مكحتلا مئوق نوكت نأ بجي: ةظحالم الك ىلع ضعبل اهضعبل ةقباطم اخسن مامت هالل ةريثملا رورملا ةكرحلا ةيعرفلا نيماظنلا.

ةحصل نم ققحتلا

1. RAVPN لاصتا نم ققحتلل.

<#root>

```
firepower# show vpn-sessiondb anyconnect
```

Session Type: AnyConnect

Username : test

Index : 5869

Assigned IP : 2.2.2.1 Public IP : 10.106.50.179

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel

License : AnyConnect Premium

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384

Bytes Tx : 15470 Bytes Rx : 2147

Group Policy : RAVPN Tunnel Group : RAVPN

Login Time : 03:04:27 UTC Fri Jun 28 2024

Duration : 0h:14m:08s

Inactivity : 0h:00m:00s

VLAN Mapping : N/A VLAN : none

Audt Sess ID : 0a6a3468016ed000667e283b

Security Grp : none Tunnel Zone : 0

2. IKEv2 لاصتا نم ققحتلل:

<#root>

firepower# show crypto ikev2 sa

IKEv2 SAs:

Session-id:2443, Status:UP-ACTIVE

, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role

3363898555

10.106.52.104/500 10.106.52.127/500 READY INITIATOR

Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK

Life/Active Time: 86400/259 sec

Child sa: local selector 2.2.2.0/0 - 2.2.2.255/65535

remote selector 10.106.54.0/0 - 10.106.54.255/65535

ESP spi in/out: 0x4588dc5b/0x284a685

3. IPsec لاصتا نم ققحتلل:

<#root>

firepower# show crypto ipsec sa peer 10.106.52.127

peer address: 10.106.52.127

Crypto map tag: CSM_outside1_map

,

seq num: 2, local addr: 10.106.52.104

access-list CSM_IPSEC_ACL_1 extended permit ip 2.2.2.0 255.255.255.0 10.106.54.0 255.255.255.0

local ident (addr/mask/prot/port): (2.2.2.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (10.106.54.0/255.255.255.0/0/0)

current_peer: 10.106.52.127

#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3

#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 3, #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.: 10.106.52.104/500, remote crypto endpt.: 10.106.52.127/500

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: 0284A685

current inbound spi : 4588DC5B

i

inbound esp sas:

spi: 0x4588DC5B (1166597211)

SA State: active

transform: esp-aes-256 esp-sha-512-hmac no compression

in use settings ={L2L, Tunnel, IKEv2, }

slot: 0, conn_id: 5882, crypto-map: CSM_outside1_map

sa timing: remaining key lifetime (kB/sec): (3962879/28734)

IV size: 16 bytes

replay detection support: Y

Anti replay bitmap:

0x00000000 0x0000000F

outbound esp sas:

spi: 0x0284A685 (42247813)

SA State: active

transform: esp-aes-256 esp-sha-512-hmac no compression

in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 5882, crypto-map: CSM_outside1_map
sa timing: remaining key lifetime (kB/sec): (4285439/28734)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

اهحال صإو ءاطخأل فاشك تسال

1. نيكمت وأ تانايبل ةمزح عمجب مق ،اهحال صإو AnyConnect لاصتا ءاطخأل فاشك تسال .
AnyConnect ءاطخأل حيحصت
2. ةيالاتل ءاطخأل حيحصت تاي لمع مدختسأ ،اهحال صإو IKEv2 ق فن ءاطخأل فاشك تسال .

```
debug crypto condition peer <peer IP address>  
debug crypto ikev2 platform 255  
debug crypto ikev2 protocol 255  
debug crypto ipsec 255
```

3. نم ققحتل ءومزحل طاقتل ذخاب مق ، FTD لعل ءاهحال صإو رورملا ةكرح ءاطخأل فاشك تسال .
نيوكتل .

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل م عد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا