

عقوم ىلإ عقوم نم IKEv2 IPv6 ق فن نيوكت ASA و FTD نيب

تايوت حمل

[عمدق م](#)

[ةيساس الابلط م](#)

[تابلط م](#)

[عمدخت س م تانوك م](#)

[نيوك ت](#)

[ةكبش ل ل يطيطخت ل م س ر](#)

[ASA نيوك ت](#)

[FTD نيوك ت](#)

[يبناج ل ل و ص و ل اب م ك ح ت](#)

[NAT اناثت س ا نيوك ت](#)

[ةحص ل ل نم ق ق ح ت](#)

[اهج الص او ا ط خ ال ا ف اش ك ت س](#)

[عج ا ر م](#)

عمدق م

ASA لوكوتورب نيب عقوم ىلإ IPv6 عقوم ق فن دادع ل نيوك ت ل ل الاثم دنن س م ل اذه مدقي مادخت س اب (Firepower ديدهت دض ع ا ف د ل) FTD لوكوتورب و (فيك ت ل ل ل ا ق ل ل نام ال ا زا ه ج) IPv6 ةكبش ل ل اص ت ا دادع ل ل نم ض ت ي و . (IKEv2) 2 رادص ل ا ت ن ر ت ن ل ا ح ا ت ف م ل د ا ب ت لوكوتورب VPN ا ه ا ن ا ة ز ه ا ك ASA و FTD مادخت س اب ي ف ر ط ل ا

ةيساس الابلط م

تابلط م

ةيلات ل ل ع ي ض ا و م ل اب ة ف ر ع م ك ي د ل نو ك ت ن ا ب Cisco ي ص و ت :

- ASA CLI نيوك ت ب ةيساس ا ة ف ر ع م
- IPSec و IKEv2 تالوكوتورب ب ةيساس ا ة ف ر ع م
- ه ي ج و ت ل ل او IPv6 ة ن و ن ع م ه ف
- FMC ر ب ع FTD نيوك ت ل ي س ا س ال م ه ف ل ا

عمدخت س م تانوك م

ة ز ه ا ل ا نم ا ه و ا ش ن ا م ت ، ة ي ض ا ر ت ف ا ة ي ب ي ل ا دنن س م ل ا اذه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا دنن س ت نيوك ت ب دنن س م ل ا اذه ي ف عم د خ ت س م ل ا ة ز ه ا ل ا ع ي م ج ت ا د ب . د د ح م ي ل م ع م دادع ا ي ف ة د و ج و م ل ا ي ال ل م ت ح م ل ا ر ي ث ا ت ل ل ك م ه ف نم د ك ا ت ف ، ج ا ت ن ا ل ا د ي ق ك ت ك ب ش ت ن ا ك ا ذ ا . (ي ض ا ر ت ف ا) ح و س م م ر م ا


```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 14
prf sha256
lifetime seconds 86400
```

```
crypto ikev2 enable outside
```

ق. افنألة ومجم نيوكتب مق 4. ةوطخال

```
tunnel-group 2001:cccc::1 type ipsec-l2l
tunnel-group 2001:cccc::1 ipsec-attributes
ikev2 remote-authentication pre-shared-key cisco123
ikev2 local-authentication pre-shared-key cisco123
```

رورملا ةكرح ةقباطم ل (ACL) لوصولا يف مكحتل ةمئاقو تانئالكلا ءاشناب مق 5. ةوطخال
ةديفملا

```
object-group network local-network
network-object 2001:aaaa::/64
```

```
object-group network remote-network
network-object 2001:dddd::/64
```

```
access-list CRYPTO_ACL extended permit ip object-group local-network object-group remote-network
```

مامتهالل اريثم رورم ةكرحل ةدعاق (NAT) ةمچرت ناو نع ةكبش ةيوهلا تللكش 6. ةوطخال

```
nat (inside,outside) source static local-network local-network destination static remote-network
remote-network no-proxy-arp route-lookup
```

ةوطخال IKEv2 IPsec حرتقم نيوكتب 7. ةوطخال

```
crypto ipsec ikev2 ipsec-proposal ikev2_aes256
protocol esp encryption aes-256
protocol esp integrity sha-1
```

ةيچراخال ةهجالو لىل عاهقبيبطتو ريفشلتل ةطيرخ نييعيتب مق 8. ةوطخال

```
crypto map VPN 1 match address CRYPTO_ACL
crypto map VPN 1 set peer 2001:cccc::1
crypto map VPN 1 set ikev2 ipsec-proposal ikev2_aes256
crypto map VPN 1 set reverse-route
```

```
crypto map VPN interface outside
```

FTD نيوكتب

FMC مادختساب FTD نيوكتب تاداشرامسقلال اذه ريفوي

(VPN) ةيرهاطلال ةصاخلال ةكبشلال ططخم ديدحت

عقوم لىل عقوم > VPN > ةزهجالو لىل لقتنا 1. ةوطخال

فوصولل هذه يف حضورم وه امك، 'FirePOWER' ديدحت دض عافندلا زايج' رتخاو 'add VPN' ديدحت

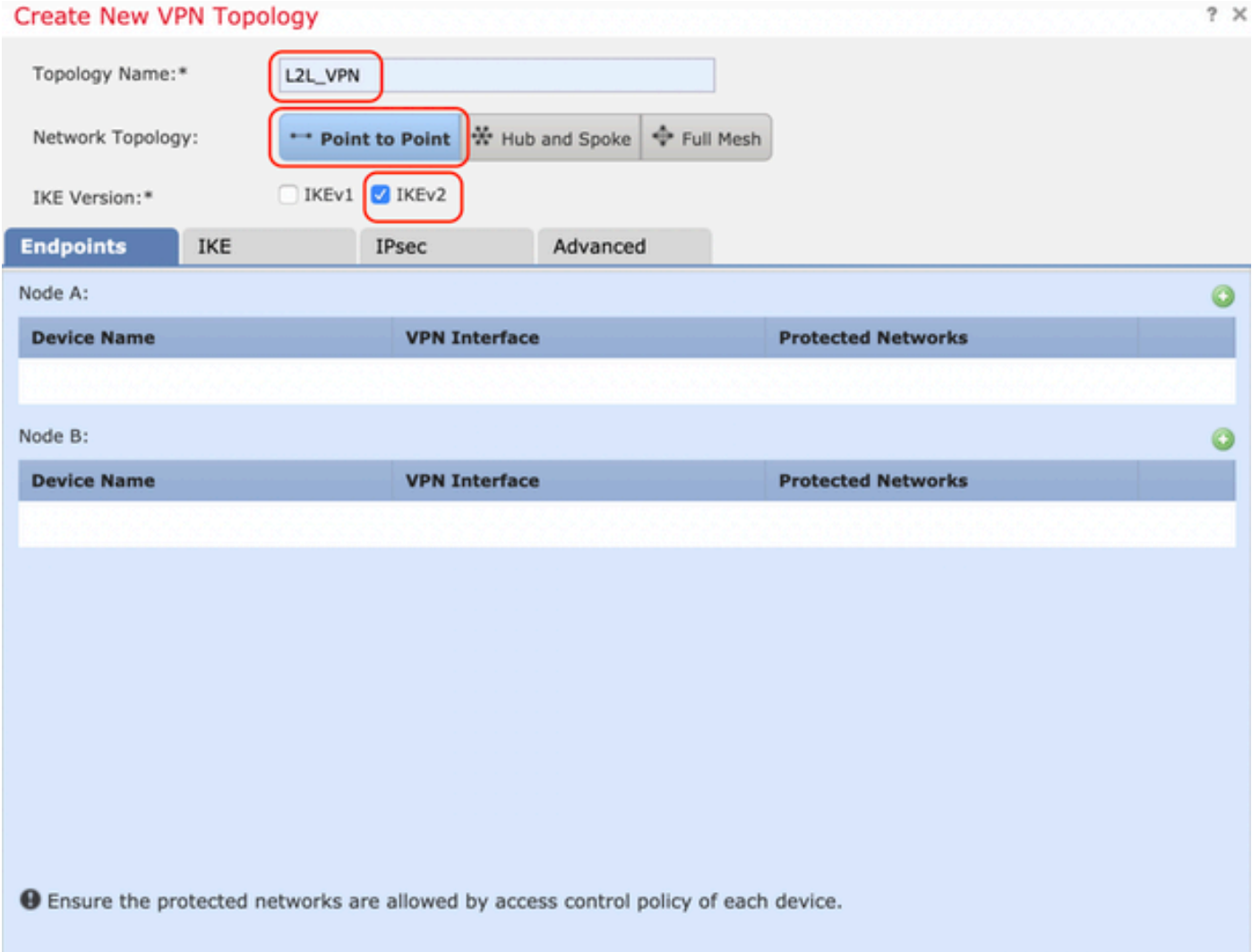


ةلوه سب هيلع فرع تل نكمي امسا (VPN) ةيره اظلا ةصاخلا ةكبشلا حنم ا. "ديج VPN طلخم ءاشن"ا ع برم ره طي. 2 ةوطخل

ةطقن ىل ةطقن :ةكبشلا طلخم

رادصا IKE: IKEv2

طلخم لىل ةزهجأ ةفاضال "دئاز رضخأ" رزلا قوف رونا. ASA هه B ةدق ل. FTD مادختسا م تي. A ةدق ل ةياهن ل ةطقن ديدحت دنع ، لاثم ل اذه في



ىل ةياهن ةطقنك FTD ةفاضل 3. ةوطخل

زاهج ل نيوكت نم ايئاق ل IP ناونع ةئبعت متت نأ بجي. اه ل ع ريفش ل ةطيرخ قي ببطت م تي يتي ال ةهجاو ل رتخأ

ئاك نوك تي ، لاثم ل اذه في. اذه VPN قفن ربع اه ريفش م تي يتي ال ةي عرف ل تاكبش ل ديدحت ل ةي حم ل تاكبش ل نم ص Green Plus زم ر قوف رونا ل ةكبش ل IPv6 '2001:DDDD::/64' ل ةي عرف ل ةكبش ل نم FMC لىل ع "لي لحم ل لىل" ةكبش ل

Edit Endpoint



Device:*

FTDv

Interface:*

OUTSIDE

IP Address:*

2001:CCCC::1

This IP is Private

Connection Type:

Bidirectional

Certificate Map:

Protected Networks:*

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

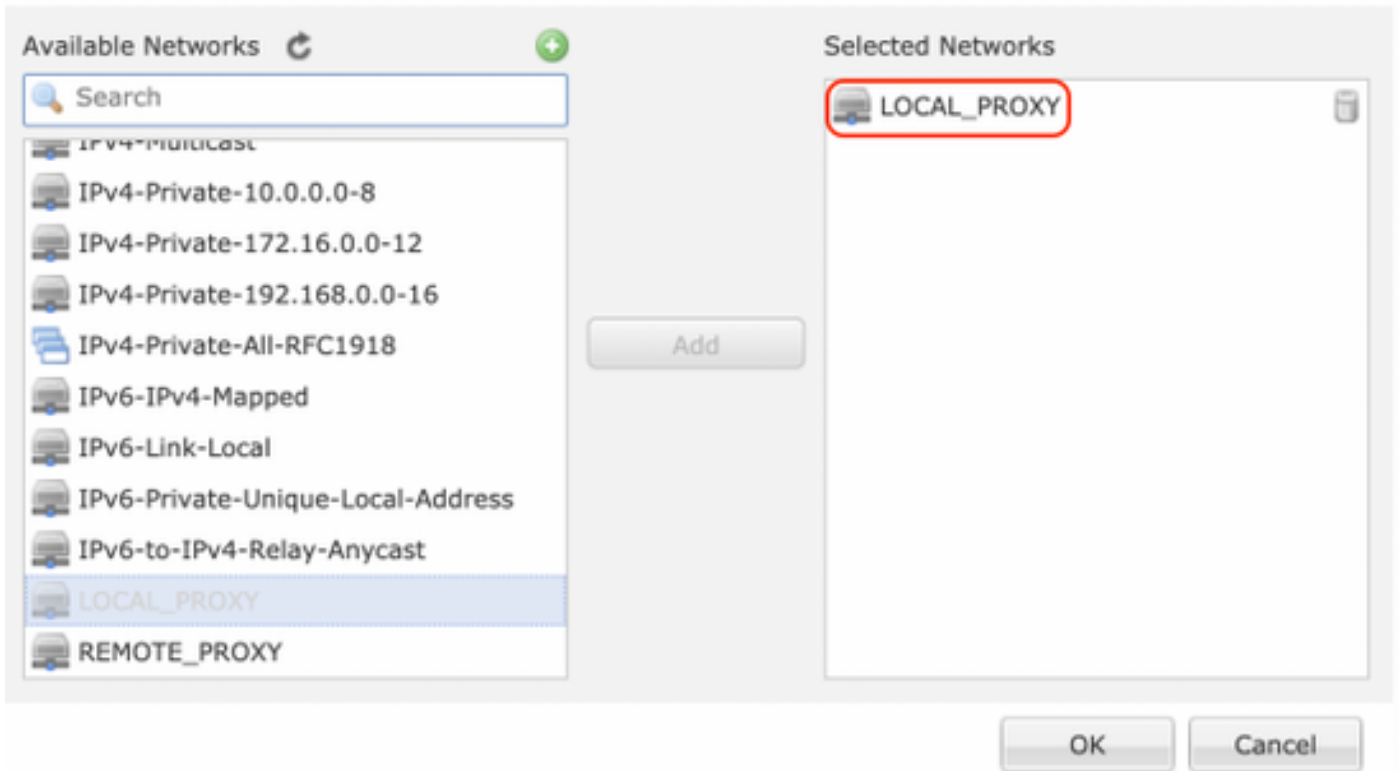


LOCAL_PROXY

OK

Cancel

Network Objects



FTD. فاهن ةطقن نيوكت لمتك، هالعأ ةدراولا ةوطخال عم

ربتعتو. لاثم ليكشال في ASA نوكي ياب ةدقع ل زمر green plus ل تقطقط 4. ةوطخال IP. ناوعو زاهج مسا ةفاض. FMC extranet. ةطساوب اهترادامتت ال يتال ةزهجال

ةمحم تاكبش ةفاضال عارضال عمجال ةمالع ةنوقي أدح 5. ةوطخال

Edit Endpoint



Device:*

Extranet

Device Name:*

ASA

IP Address:*

Static Dynamic

2001:BBBB::1

Certificate Map:

Protected Networks:*

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



REMOTE_PROXY

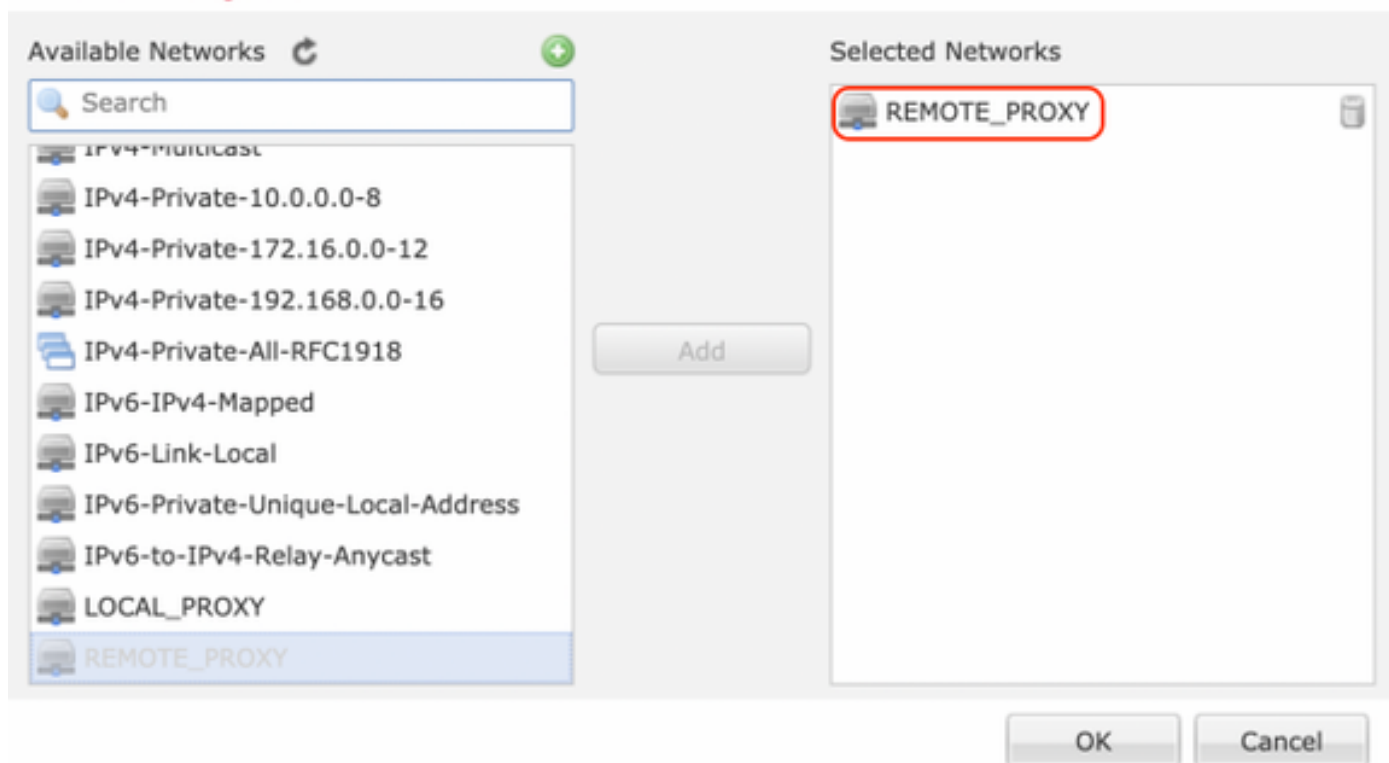
OK

Cancel

ةددحم لآ تاكبش لآ لآ اهتفاضل واهر يفش ت مزلي ي ت لآ ةي عرف لآ ASA تاكبش ددح .6 ةوطخ لآ

لآ لآ اذ ه ي ف '2001:AAA:/64' ةي عرف لآ ASA ةكبش ه 'Remote Proxy'

Network Objects



IKE تاملعم نيوكت

يولوالا لدابتلل اهمادختسا متيس يتلا تاملعملا دح، IKE بيوبتلا عمالعتحت 1. ةوطخلا ديدج IKE جهن عاشنإل عارضخالا ةفاضإلا عمالعت زمروقوف رقنا. IKEv2.

Edit VPN Topology



Topology Name:* L2L_VPN

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh14_3

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:* 24 Characters (Range 1-127)

IKEv2 Settings

Policy:* Ikev2_Policy

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Save Cancel

1 ةلحرمل ةيحلص ةرتف لى ةفاضل اب ةيولوا مقر دح ، ةديدل IKE ةسايس يف 2 ةوطخل
يولوال لدابل لل تاملعمل هذه ليلدل اذ مدختسي . لاصلتال نم
لماكتل (SHA256) ،
رشفشتل (AES-256) ،
و PRF (SHA256) ،
(14 ةومجم) Diffie-Hellman ةومجم

يف دووم وه امع رظنل لضب ديعبل رظنل لى زاهل لى IKE چن ةفاك لاسرا متيس
VPN لاصلتال ديعبل رظنل لى قباطت لول دىحت متيس . ددحل جهنل مسق

1 ةيولوال لاسرا متي . ةيولوال لى قح مادختساب الولا لاسرا متي يذل جهنل رتخا [يرايخا]
الوا .

Edit IKEv2 Policy

Name:*

Ikev2_Policy

Description:

Priority:

(1-65535)

Lifetime:

86400

seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- MD5
- SHA
- SHA512
- SHA256
- SHA384
- NULL

Selected Algorithms

SHA256

Add

Save

Cancel

Edit IKEv2 Policy



Name:*

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- AES
- AES-256
- DES
- 3DES
- AES-192
- AES-GCM
- AES-GCM-192
- AES-GCM-256
- NULL

Add

Selected Algorithms

- AES-256

Save

Cancel

Edit IKEv2 Policy



Name:*

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)

- Integrity Algorithms
- Encryption Algorithms
- PRF Algorithms**
- Diffie-Hellman Group

Available Algorithms

- MD5
- SHA
- SHA512
- SHA256
- SHA384

Add

Selected Algorithms

- SHA256**

Save

Cancel

Edit IKEv2 Policy



Name:* Ikev2_Policy

Description:

Priority: (1-65535)

Lifetime: 86400 seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Groups

- 1
- 2
- 5
- 14
- 15
- 16
- 19
- 20
- 21

Add

Selected Groups

- 14

Save Cancel

عون رتخاو هالعأ انهنيوكت مت يتي لاسايسلا ددح ، تامل عمل افاضل درجم ب. 3 ةوطخل اةقداصل

اقبسم كرتشم حاتفملا تلمعتسا ، دشرم اذه ل . اقبسم كرتشملا يوديلا حاتفملا رايخ ددح 'cisco123'.

Edit VPN Topology

? X

Topology Name:* L2L_VPN

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh14_3

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:* 24 Characters (Range 1-127)

IKEv2 Settings

Policy:* Ikev2_Policy

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Save Cancel

IPsec تاملعم نيوكت

ليوحتلا ةعومجم ريديحتل صاصرلا ملقلا زمر قوف رقتلا قيوط نع ديديج "IPsec حرتقم" ءاشناب مقو IPsec بيوبتلا ةقالع ىلا لقتنا 1. فوطخلا

Edit VPN Topology



Topology Name:*

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:

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*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

— **ESPv3 Settings**

انبدأ حضورم وه امك 2 ةلحرمل تاملعم لالخداو Green Plus ةنوقى أ دىحت لالخ نم دىج IKEv2 IPsec حرتقم عاشنا. 2 ةوطخل

ئىزجت ESP: SHA-1

ئىفش ESP : AES-256

Edit IKEv2 IPsec Proposal



Name:*

Ikev2__IPSec_Proposal

Description:

ESP Hash

ESP Encryption

Available Algorithms

- SHA-512
- SHA-384
- SHA-256
- SHA-1
- MD5
- NULL

Selected Algorithms

SHA-1

Add

Save

Cancel

Edit IKEv2 IPsec Proposal



Name:*

Description:

ESP Hash

ESP Encryption

Available Algorithms

- AES-GCM-256
- AES-256
- AES-GCM-192
- AES-192
- AES-GCM
- AES
- 3DES
- DES
- AES-GMAC-256

Add

Selected Algorithms



- AES-256**

Save **Cancel**

ةددملا ليوحتلا تاومجم ىل هتفاضاب مق ،ديدلج IPsec حرتقم عاشنا درجم ب 3. ةوطخل

IKEv2 IPsec Proposal



Available Transform Sets  

- AES-GCM
- AES-SHA
- DES_SHA-1
- Ikev2__IPSec_Proposal**

Add

Selected Transform Sets

- Ikev2__IPSec_Proposal**

OK **Cancel**

ةوطخل 4. IKEv2 IPsec تا حرتقم نمض نأل ائيدج ددملا IPsec حرتقم جاردا مت

لطعم PFS و يضارفتا هنا على يضارفتا الاعمالم طبض متي، لاثملا اذله. انه PFS تافللمو 2 ولجرملا رمع ريرحت نكمي، رمالا بلطتنا

Edit VPN Topology

Topology Name:*

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:

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*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

— **ESPv3 Settings**

يعرف ال تاك بشلاب حامس لل لوصولو في مكحتلا ةسايس دعاوق عاشنا وأ لوصولو في مكحتلا زواجتلا تاوطخل نيوكت كيلى بچي فTD لال نم (VPN) ةرهاظلا ةصاخلا تاك بشلل

يبناجلا لوصولاب مكحتلا

نيكمت مت اذا فTD زاخ لال نم VPN رورم ةكرحب حامس لل لوصولو في مكحتلا ةسايس عاشنا بچي كلذ دعب *sysopt allowed-vpn* نيكمت متي مل اذا *sysopt allowed-vpn* "في مكحتلا" راخي اذه نيوكتلا لاثم مدختسي. لوصولو في مكحتلا ةسايس عاشنا يطخ *sysopt allowed-vpn*

Advanced > Tunnel. نمض *sysopt allowed-vpn* ةملعمل نيكمت نكمي

ةكرحب صحفل لوصولو في مكحتلا ةسايس مادختسا ةيناكم راخيلا اذه ليزي: ريرحت ميأوق وأ VPN ةيفصت لماموع مادختسا نكمي لازي ال. نيمدختس مل نم ةمداقلا رورملا رمالا اذه. مدختس مل رورم ةكرحب ةيفصتل ليزنتلل ةلباقلا (ACL) لوصولو في مكحتلا هذه راخيلا ةناخ نيكمت مت اذا VPN تاك بشل عيمج على قبطني ماع

Edit VPN Topology



Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints | IKE | IPsec | **Advanced**

IKE
IPsec
Tunnel

NAT Settings

Keepalive Messages Traversal
Interval: Seconds (Range 10 - 3600)

Access Control for VPN Traffic

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

Certificate Map Settings

Use the certificate map configured in the Endpoints to determine the tunnel

Use the certificate OU field to determine the tunnel

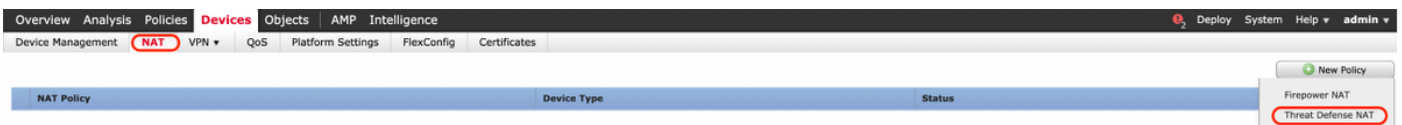
Use the IKE identity to determine the tunnel

Use the peer IP address to determine the tunnel

NAT انثتس | نيوكت

كرك ةمجرت وىرأ NAT ةرابع ةقباطم نم VPN رورم ةكرك عنمل هعضوم في NAT انثتس | نوكتي نأ بجي . رورم ةكرك VPN ل | ل نايب ءافع | NAT تلكش
جحص ريغ لكشب VPN رورم

ديدهت | نع ءافدل | NAT > ةديج ةسايس قوف رونلاب ةديج ةسايس دأ و NAT > ةزهال | ل | ل قنتنا . 1. ةوطخل



New Policy



Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

FTDv

Selected Devices

FTDv

ةدعاق ةفاضل قوف رقنا 2. ةوطخلال

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

NAT_Exempt

Enter Description

Show Warnings Show Add Cancel

Policy Assignments (1)

Filter by Device Add Rule

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
▼ NAT Rules Before											
▼ Auto NAT Rules											
▼ NAT Rules After											

nat ةدعاق يكيتاتسا نكاس ديدج تقلال 3. ةوطخلال

نم رورملا ةكرح يلج دعاوقلا هذه ريثأت عنم لىلا ةهجاوولا تانئاك بيوبتلا ةمالع يف تاهجاوولا ديدجت يدؤي. ةدعاق nat لىلا جراخ نراقو يلخادلا تلحأ جرخال تاهجاوولا.

ةيلصلأا ةهجاوولا/ردصملا تنمض nat ءانثتسا ةدعاق وه اذه نأ امب. ةهجاوولا/ردصملا ةيعرفلا تاكبشلا ددحو "ةمجت" بيوبتلا ةمالع لىلا لقتنا سفن مجرتملا ةهجاوولا/ردصملا او.

Add NAT Rule

? X

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects: **Translation** PAT Pool Advanced

Original Packet

Original Source:* +

Original Destination: +

Original Source Port: +

Original Destination Port: +

Translated Packet

Translated Source: +

Translated Destination: +

Translated Source Port: +

Translated Destination Port: +

راسم لثحب و no-proxy-arp ني كمتب مقو ةمدقتم تاراخي بيوبتال ةمالع قوف رقنا

Add NAT Rule

? X

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects: Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Fallthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

ةمئاق nat ل ي ةلمج nat ةياهنل تذكأو ةدعاق اذه تذقنا

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates Show Warnings Save Cancel

NAT_Exempt
Enter Description Policy Assignments (1)

Rules Add Rule

Filter by Device

#	Direction	Type	Original Packet			Translated Packet			Options
			Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Translated Sources	Translated Destinations	
1		Static	LAN	WAN	LOCAL_PROXY	REMOTE_PROXY	LOCAL_PROXY	REMOTE_PROXY	Dns: false route-lookup no-proxy-arp

FTD لى هرشنب مق م ث نيوكتل لظفح ، نيوكتل لامتكا لدرج م 4 ةوطخل

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Deployment Deployment History

1 device selected
Deploy time: Estimate Deploy

Device	Inspect Interruption	Type	Group	Last Modified Time	Preview	Status
> FTDv		FTD		11/04/2020, 17:15:59		Pending

ةحصل ال نم ققحت ال

ASA على packet-tracer هاندا رمالا لي غشت كنكمي و اة لجم ال ةكبش ال زاغ نم مامته ال ةريثم رورم ةكر اءبا

```
packet-tracer input inside icmp 2001:aaaa::23 128 0 2001:dddd::33 detail
مظاح ال "ىءص بلط" =0 زم رل او 128 = انه عون ال لثم ي: ةظاح ال
```

و ASA ل (CLI) رما و ال رطس ةه جا و لى لع اهل ي غشت كنكمي ي ال رما و ال ي ال ال مسق ال فص ي
IKEv2 ق فن ةلا ح نم ققحت ال ل ل FTD LINA

ال ASA ل نم جات ن نم ل اثم اءه

```
ciscoasa# show crypto ikev2 sa
```

IKEv2 SAs:

```
Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Status Role Remote
6638313 2001:bbbb::1/500
READY INITIATOR 2001:cccc::1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/224 sec
Child sa: local selector 2001:aaaa::/0 - 2001:aaaa::ffff:ffff:ffff:ffff/65535
remote selector 2001:dddd::/0 - 2001:dddd::ffff:ffff:ffff:ffff/65535
ESP spi in/out: 0xa0fd3fe6/0xd95ecdb8
```

```
ciscoasa# show crypto ipsec sa detail
```

```
interface: outside
```

```
Crypto map tag: VPN, seq num: 1, local addr: 2001:bbbb::1
```

```
access-list CRYPTO_ACL extended permit ip 2001:aaaa::/64 2001:dddd::/64
local ident (addr/mask/prot/port): (2001:aaaa::/64/0/0)
remote ident (addr/mask/prot/port): (2001:dddd::/64/0/0)
current_peer: 2001:cccc::1
```

```
#pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 11
#pkts decaps: 11, #pkts decrypt: 11, #pkts verify: 11
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #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
#pkts no sa (send): 0, #pkts invalid sa (rcv): 0
#pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
#pkts invalid prot (rcv): 0, #pkts verify failed: 0
#pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
```

#pkts invalid pad (rcv): 0,
#pkts invalid ip version (rcv): 0,
#pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
#pkts replay failed (rcv): 0
#pkts min mtu frag failed (send): 0, #pkts bad frag offset (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv): 0

local crypto endpt.: 2001:bbbb::1/500, remote crypto endpt.: 2001:cccc::1/500
path mtu 1500, ipsec overhead 94(64), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: D95ECDB8
current inbound spi : A0FD3FE6

inbound esp sas:

spi: 0xA0FD3FE6 (2700951526)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 1937408, crypto-map: VP
sa timing: remaining key lifetime (kB/sec): (4055040/28535)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

outbound esp sas:

spi: 0xD95ECDB8 (3646868920)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 1937408, crypto-map: VPN
sa timing: remaining key lifetime (kB/sec): (4193280/28535)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

ciscoasa# **show vpn-sessiondb detail l2l filter name 2001:cccc::1**

Session Type: LAN-to-LAN Detailed

Connection : 2001:cccc::1
Index : 473 IP Addr : 2001:cccc::1
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA256 IPsec: (1)SHA1
Bytes Tx : 352 Bytes Rx : 352
Login Time : 12:27:36 UTC Sun Apr 12 2020
Duration : 0h:06m:40s

IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:

Tunnel ID : 473.1
UDP Src Port : 500 UDP Dst Port : 500
Rem Auth Mode: preSharedKeys
Loc Auth Mode: preSharedKeys
Encryption : AES256 Hashing : SHA256
Rekey Int (T): 86400 Seconds Rekey Left(T): 86000 Seconds
PRF : SHA256 D/H Group : 14
Filter Name :

IPsec:

Tunnel ID : 473.2

Local Addr	: 2001:aaaa::/64/0/0		
Remote Addr	: 2001:dddd::/64/0/0		
Encryption	: AES256	Hashing	: SHA1
Encapsulation	: Tunnel		
Rekey Int (T)	: 28800 Seconds	Rekey Left(T)	: 28400 Seconds
Rekey Int (D)	: 4608000 K-Bytes	Rekey Left(D)	: 4608000 K-Bytes
Idle Time Out	: 30 Minutes	Idle TO Left	: 23 Minutes
Bytes Tx	: 352	Bytes Rx	: 352
Pkts Tx	: 11	Pkts Rx	: 11

اهحال صاوا عااطخاا فاشكسا

ححصت رماوا لىغشتب مق، ASA و FTD لىع اهاال صاوا IKEv2 ق فن عاشن ا عااطخا فاشكسا الة:
ةللا ا عااطخا الة:

```
<peer IP>  
ريفشتلل ا عااطخا الة ا ححصت طرش رىظن  
debug crypto ikev2 protocol 255  
debug crypto ikev2 platform 255
```

اهل ا عوچرلل IKEv2 ا عااطخا ا ححصت لمع ةن عى لى امى:
<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debug.html>

عچارملا

<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/119425-configure-ipsec-00.html>
<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/81824-common-ipsec-trouble.html>
<https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/vpn/asa-95-vpn-config/vpn-site2site.html>

ةمچرتل هذه لوج

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