

ةساي سلا ىلإ ةدنن سملل VPN ةكبش نيوكت ىلإ FTD و ASA نم راسملا ىلع ةمئاقو Microsoft Azure

تايوت حمللا

[ةمدقملا](#)

[ميهافملا](#)

[VPN ريفشت لاجم](#)

[ةسس اسألا تابلطت ملا](#)

[تابلطت ملا](#)

[ةمدخت سملل تانوكملا](#)

[نيوكتللا](#)

[ASA ىلع IKEv1 نيوكت](#)

[ثدحأ رادصلا وأ \(1\) ASA 9.8 زمر ىلع VTI عم راسملا ىللا دننن سملل IKEv2](#)

[FTD ىلع IKEv1 نيوكت](#)

[ةساي سلا ىللا ةدنن سملل رورملا ةكرح تاددحم عم راسملا ىللا دننن سملل IKEv2](#)

[ةحصلا نم ققحتلا](#)

[ىلوالا ةلحرملا](#)

[ةيناثلا ةلحرملا](#)

[اهجالص او ءاطخألا فاشكتسا](#)

[IKEv1](#)

[IKEv2](#)

ةمدقملا

و ةيامح راج نم أي cisco ASA و cisco VPN ل نيوكتللا او ميهافملا ةقيثو اذه فص ي تامدخ ةباحس Microsoft Azure.

ميهافملا

VPN ريفشت لاجم

ريفشتلا لاجم ديدحت متي. VPN قفن ي ف ةكراشم لاب IPsec IP نيوانع قاطن حمسي تاقاطن ديدحتل دعب نع تانايبلا رورم ةكرح ي قننمو يلحم رورم ةكرح ددحم مادختساب IPsec. ةطساوب اهريفشتو اهطاقتللا متي يتلا ةديعبلا او ةيلحملا ةي عرفلا تاكلبشلا وأ راسملا ىللا ةدنن سملل رورملا ةكرح تاددحم: VPN ريفشت تالاجم ديدحتل نابولسأ ةساي سلا ىللا ةدنن سملل.

راسملا ىللا دننن سملل:

ةكرح تاددحم نييعت مت IPsec قفن لخدت رورم ةكرح ي أب حامسلل ريفشتلا لاجم نييعت مت متي رورم ةكرح ي أن ينع ي اذهو. 0.0.0.0 ىلع IPsec نم ةديعبلا او ةيلحملا تانايبلا رورم ةهوجل/ردصم لل ةي عرفلا ةكبشلا نع رظنلا ضغب اهريفشت متي IPsec قفن ىللا اهيهجوت.

راسم اليا لى ءءنئسم اليا VPN ءكبش Cisco نم (ASA) فى كئلل لباقل اليا نام اليا زاا مءءى ءءال اليا ءاراء اليا 9.8 ءاراء اليا فى (VTIs) ءىره اظلال قفنل اليا ءااوا مااءءءسا ب

لبق نم ءراءم اليا Cisco نم (FTD) ءىرانل اليا ءقائل ءىءء ءى ءىامءل اليا نم اليا ءىامءل اليا راء مءءى مااءءءسا ب ءىءءل اليا ءىء ءمءاق (VPN) ءىره اظلال ءصاا ءكبش (Firepower ءراءل زكرم) FMC ءءال اليا ءاراء اليا 6.7 ءاراء اليا فى VTIs ءاكبش

ءسايس اليا لى ءنئسم:

ءصم اليا نم ل كل طقف ءنى عم IP ءاقاطن رىفشء لىء رىفشءل اليا لاءم نىءىء مء نع رورم اليا ءكرا وءءم وءسايس اليا لى ءنئسم اليا ءىءءم اليا رورم اليا ءكرا ن وءءم ءءى. ءهءول اليا و IPSec ربع اءرىفشء بءى ءىءل رورم اليا ءكرا ءب

8.2 راء اليا فى رىفشءل اليا طءاء عم ءسايس اليا لى ءنئسم اليا VPN ءكبش ASA مءءى ءءال اليا ءاراء اليا

و ءسايس اليا لى ءمءاق اليا و راسم اليا لى ءنئسم اليا رورم اليا ءكرا ءاءءم Microsoft Azure مءءى مء ءىءل اليا ءسايس اليا لى ءنئسم اليا رورم اليا ءكرا ءاءءم مااءءءسا ب راسم اليا لى ءمءاق اليا نىءوكء كنىمى ءىءل اليا Internet Key Exchange (IKE) راء اليا ءىءىءب اليا لاء Azure موقى. اءءاكءم نىءل اليا راء اليا راسم اليا لى ءنئسم اليا ب ل طءى. VPN ءكبش ل ءءم اليا بولس اليا لى ءانءسا IKEv1 لوكوءورب نم لوال راء اليا ءسايس اليا لى ءنئسم اليا ب ل طءى امك، IKEv2 لوكوءورب نم نأ بءى و Azure فى راسم اليا لى ءنئسم ءىءء بءى فى، IKEv2 مااءءءسا ب مء اءل هنىءى اءو بءى فى، زمرل راء اليا ب بسب طقف رىفشءل اليا طءاء مءءى ASA ناك اءل نكلو، ASA VTIs مءءءسى راسم اليا لى ءنئسم اليا ءسايس اليا لى ءنئسم اليا رورم اليا ءكرا ءىءء ءافل ل Azure نىءوكء راء ءىءفنءل PowerShell ل ءىصنل اليا راء اليا رشن ربع Azure لءءم فى كل ءقءىء مءى و انه ءضوم وه امك UsePolicyBasedTrafficSelectors ءىءءءسا ب Microsoft موقت

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policy-based-rm-ps>.

FTD و ASA نىءوكء روظنم نم صىءلءل

- ل Azure نىءوكء بءى، رىفشء ءطىء مااءءءسا ب هنىءوكء مء ءىءل اليا ASA/FTD ل ءبس نل اب مااءءءسا ب راسم اليا لى ءنئسم اليا و ءسايس اليا لى ءنئسم اليا VPN UsePolicyBasedTrafficSelectors.
- VPN ءكبش ل Azure نىءوكء بءى، VTIs مااءءءسا ب هنىءوكء مء ءىءل اليا ASA ل ءبس نل اب راسم اليا لى ءنئسم اليا.
- انه VTIs نىءوكء ءىءفىء ل وءءامول عم اليا نم ءىزم لىء روءءل نكمى، FTD ل ءبس نل اب، https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/firepower_threat_defense_site_to_site_vpns.html#concept_ccj_p4r_cmb

ءىسايس اليا ءابل طءم اليا

ءابل طءم اليا

ءىءل اليا ءىءءم ل اب ءفر عم كىءل نوكء نأ Cisco ءىءءم:

- زمر: ASA لىء VTIs مءءءءسء ءىءل اليا IKEv2 راسم اليا لى ءنئسم اليا VPN ءكبش ل ءبس نل اب لى ءنئسم اليا VPN ءكبش ل Azure نىءوكء بءى). ءءال راء اليا (1) 9.8 راء اليا (راسم اليا).
- رىفشءل اليا ءطىء مءءءسء ءىءل اليا IKEv1 ءسايس اليا لى ءنئسم اليا VPN ءكبش ل ءبس نل اب نىءوكء بءى). ءءال راء اليا و 6.2.0 FTD و ءءال راء اليا 8.2 راء اليا ASA زمر: ASA و FTD لىء


```
Cisco-ASA(config-ikev1-policy)#group 2
Cisco-ASA(config-ikev1-policy)#lifetime 28800
```

حاجات فم وريظن لل IP ناوع نيوكتب مقو IPsec تامس تحت قفن ةومجم عاشن اب مق 3. ةوطخل اقبسم كرتشم القف لل

```
Cisco-ASA(config)#tunnel-group 192.168.1.1 type ipsec-l2l
Cisco-ASA(config)#tunnel-group 192.168.1.1 ipsec-attributes
Cisco-ASA(config-tunnel-ipsec)#ikev1 pre-shared-key cisco
```

تاونق عاشن او اهرى فشت متيس يتل رورم الة كرح ددحت لوصو ةمئاق عاشن اب مق 4. ةوطخل هيلع لوصحل متي يذلقف لل نم رورم الة كرح يه ةحلصم ل رورم ة كرح، لاثم ل اذه يف اهل تناك اذا ةددعتم تالخد اىل ع يوتحي نأ نكمي و 10.1.1.0 اىل 10.2.2.0 ةي عرف الة كبش ل نم عقاوم ل ني ب ة كرتشم ةددعتم ةي عرف تالكبش كانه

تاىواك لمعت تانئاك تاعومجم و تانئاك عاشن نكمي، ثدح ال اارادصل او 8.4 تارادصل اىل عاشن اب مق. ةددعتم تانئاك و اىل فم ل IP نيوانع و اىل عرف ال تالكبش ل و تالكبش ل ةمئاق تارابع نم لكل امه اذختسا و ةديعبو ةي لجم ةي عرف تالكبش ل ع ناىوتحي نيئاك (NAT) ةكبش ل ناوع ةمچرتو ريفش لل (ACL) لوصول اىل فم كحتل

```
Cisco-ASA(config)#object network 10.2.2.0_24
Cisco-ASA(config-network-object)#subnet 10.2.2.0 255.255.255.0
Cisco-ASA(config)#object network 10.1.1.0_24
Cisco-ASA(config-network-object)#subnet 10.1.1.0 255.255.255.0
```

```
Cisco-ASA(config)#access-list 100 extended permit ip object 10.2.2.0_24 object 10.1.1.0_24
```

بجى IKEv1 ةي ساس الة م لك ل نمضتت نأ بجى يتل او، (TS) لىوتحت الة ةومجم نيوكت 5. ةوطخل اىل اىل ةي عرف ال فم ل ع قباطم TS عاشن اب

[حاجاتم ل اذه Microsoft دن تسم](#) نم دهج لصف اءج ردم ل IKEv1 2 ةلجرم ل تامس مدقت: [ءظحال ماع لكشب](#) Microsoft Azure م ع دب لصتا، حىضوتل نم ديزم.

```
Cisco-ASA(config)#crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac
```

يوتحت يتل او، ةي جراخل الة جاول اىل ع اوقى ببطتو ريفش الة ةطيرخ نيوكتب مق 6. ةوطخل الة: رىظن لل IP ناوع: ةئاق ل رورم ة كرح اىل ع يوتحت يتل ةددح ل لوصول ةمئاق: ب قوئوم ل ساس ال ماظن ل: [Azure قئاثو](#) نأل ارظن (PFS) ةي لاثم ل هىجوتل ةداع ةيرس نييعبت نيوكت موقى ال PFS دادع نيكمت نكمي. Azure يف IKEv1 ل PFS لىطعت اىل صنت [ماع لكشب ةرفوتم ل](#) اهم اذختسا متي يتل ال Diffie-Hellman حىتافم نم دىج جوز عاشن اىل اىل دوى يذلاو، رىراىخ اذختسا لال نم، (2 ةلجرم ل روهظ لبق PFS نم نيبنال الة نيكمت بجى) تاناب الة ةي حل اذختسا لال نم، [روهم ل ع حاجاتم ل Azure قئاثو](#) اىل ةددح ل ال IPsec لمع تارتف نم 2 ةلجرم ل دن تست: [ماع لكشب](#) Microsoft Azure م ع دب لصتا، حىضوتل نم

```
Cisco-ASA(config)#crypto map outside_map 20 match address 100
Cisco-ASA(config)#crypto map outside_map 20 set peer 192.168.1.1
```



```
Cisco-ASA(config-ikev2-policy)#integrity sha
Cisco-ASA(config-ikev2-policy)#group 2
Cisco-ASA(config-ikev2-policy)#lifetime seconds 28800
```

IPsec في نامألا تاملعم ديدحت. IKEv2 نم 2 ةلحرم لل IPsec حرتقم ةفاضإ. 3 ةوطخلا نيوكتلل عضو `ikev2 ipsec-proposal` ريفشتلل:

ايسر ةفشت {des | 3des | AES | AES-192 | AES-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | ايسر }
ايسر {md5 | sha-1 | SHA-256 | SHA-384 | SHA-512 | ايسر } ةفشت لوكوتورب لمك

IPSec ريفشتو لمك تامس عم ضراعتت تامولعم رشنب Microsoft تماق: **ةظحال** ةجردملا تامسلا ريفوت متي. Azure اهمدختست يتلا ةيناثلا ةلحرم لابة صاخلا عم ضراعتت يتلا تامولعملا. [معال لكش ب ريفوت مالا اذه Microsoft دن تسيم](#) نم دهج لصفاب معدب لصتا، حيصوتلا نم ديزمل. [انه ةيئرم](#) Microsoft نم 2 ةلحرم لل IPSec ةمس Microsoft Azure.

```
Cisco-ASA(config)#crypto ipsec ikev2 ipsec-proposal SET1
Cisco-ASA(config-ipsec-proposal)#protocol esp encryption aes
Cisco-ASA(config-ipsec-proposal)#protocol esp integrity sha-1
```

ددحي يذلا IPSec فيرعت فلم ةفاضإ. 4 ةوطخلا:

- ةلحرم لاي 2 ل اقبسم هنيوكت مت يذلا IPSec لوكوتورب حرتقم
- تيابوليك و/ويناوثلل اب (يرايخا) ل IPSec ةلحرم لل يضايرت فالارمعال
- ةومجم (يرايخا) PFS ةومجم

ةلحرم لل يضايرت فالارمعال عم ضراعتت تامولعم رشنب Microsoft تماق: **ةظحال** ةجردملا تامسلا ريفوت متي. Azure لبق نم ةمدختست مالا PFS تامسو IPSec نم ةيناثلا عم ضراعتت يتلا تامولعملا. [معال لكش ب ريفوت مالا اذه Microsoft دن تسيم](#) نم دهج لصفاب معدب لصتا، حيصوتلا نم ديزمل. [انه ةيئرم](#) Microsoft نم 2 ةلحرم لل IPSec ةمس Microsoft Azure.

```
Cisco-ASA(config)#crypto ipsec profile PROFILE1
Cisco-ASA(config-ipsec-profile)#set ikev2 ipsec-proposal SET1
Cisco-ASA(config-ipsec-profile)#set security-association lifetime seconds 27000
Cisco-ASA(config-ipsec-profile)#set security-association lifetime kilobytes unlimited
Cisco-ASA(config-ipsec-profile)#set pfs none
```

ريظنل ل IP ناوع نيوكتب مقو IPSec تامس تحت قافنأ ةومجم عاشناب مق. 5 ةوطخلا IKEv2 ل اقبسم كرتشملا ديعبل او يلحرملا قفنلا حاتفمو:

```
Cisco-ASA(config)#tunnel-group 192.168.1.1 type ipsec-121
Cisco-ASA(config)#tunnel-group 192.168.1.1 ipsec-attributes
Cisco-ASA(config-tunnel-ipsec)#ikev2 local-authentication pre-shared-key cisco
Cisco-ASA(config-tunnel-ipsec)#ikev2 remote-authentication pre-shared-key cisco
```

نيعي نأ VTI تقلخ. 6 ةوطخلا:

- [number] ةهجاو ل ق فن: دي دج ق فن ةهجاو م قر
- [name]: دي دج ق فن ةهجاو م سا
- [ع انق] [ip ناو نع]: ق فن ل ةهجاو ل ع دو جوم ري غ IP ناو نع
- [int-name]: ق فن ل ر دص م ةهجاو: اي ل حم VPN يه ت ن ت شي ح ق فن ل ر دص م ةهجاو
- [Azure Public IP]: ق فن ل ةهجاو: ة ر ا ب ع IP ناو نع
- IPv4 ل ق فن ل ع ضو: IPsec IPv4 ع ضو
- ص ا خ ل IPsec في ر ع ت ف ل م: ا ذ ه VTI في ر ع ت ف ل م ل ه م ا د خ ت س ا ب و ل ط م ل IPsec في ر ع ت ف ل م ب [profile-name] ق فن ل ة ه ا م ح ب

```
Cisco-ASA(config)#interface tunnel 100
Cisco-ASA(config-if)#nameif vti
Cisco-ASA(config-if)#ip address 169.254.0.1 255.255.255.252
Cisco-ASA(config-if)#tunnel source interface outside
Cisco-ASA(config-if)#tunnel destination [Azure Public IP]
Cisco-ASA(config-if)#tunnel mode ipsec ipv4
Cisco-ASA(config-if)#tunnel protection ipsec profile PROFILE1
```

نكاس راسم ةفاضل. ق فن ل ل خاد رورم ل ة ك ر ح ل ة ر ا ش ل ل ت ب ا ت ر ا س م ة ا ش ن ا ب م ق 7. ة و ط خ ل ا ر م ا ل ا ذ ه ل خ د ا ، ي ك ي ت ا ت س ا

```
route if_name dest_ip mask gateway_ip [distance]
```

ل ا ث م ل ل ي ب س ل ع ، Azure ة ب ا ح س ي ف ة ه ج و ل ا ة ك ب ش ل IP ناو نع و ه mask و dest_ip ر م ا ل ا ض ر ع ي ة ر ف ل ل ة ك ب ش ل ل ع (دو جوم ري غ و دو جوم) IP ناو نع ي gateway_ip نو ك ي ن ا ب ج ي . 10.0.0.0/24 ة ه ج ا و ل ا رورم ل ة ك ر ح ه ي ج و ت و ه gateway_ip ا ذ ه ن م ض ر ع ل . 169.254.0.2 ل ث م ، ق فن ل ة ه ج ا و ل ة م ه م ت س ي ل ا ه س ف ن ip ة ص ا خ ل ل ة ب ا و ب ل ن ك ل و ، ق فن ل ا

```
Cisco-ASA(config)#route vti 10.0.0.0 255.255.255.0 169.254.0.2
```

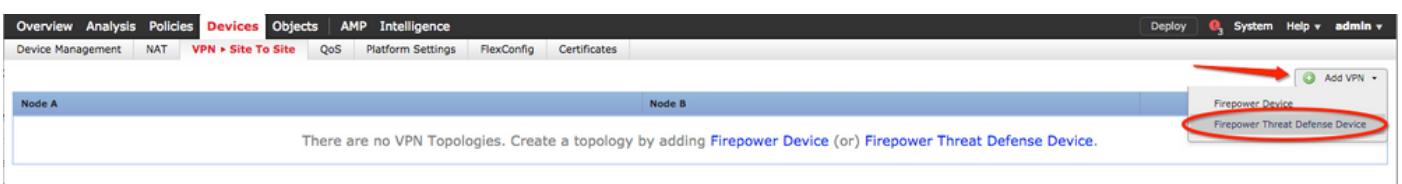
FTD ل ع IKEv1 ني و ك ت

ز ا ه ج ل ي ج س ت ك م ز ل ي ، Azure ل ا ل FTD ن م ع ق و م ل ا ع ق و م ن م VPN IKEv1 ة ك ب ش ل ا ة ب س ن ل ا ب FTD ل ا ا ق ب س م FTD.

ل ا ط و خ ل ا FMC dashboard > Devices > VPN > Site to Site. ل ا ل ق ت ن ا . ع ق و م ل ا ع ق و م ن م ج ه ن ة ا ش ن ا ب م ق 1. ة و ط خ ل ا



Firepower Threat Defense device ر ت خ ا و ة ل د س ن م ة م ا ق Add VPN ق و ف ر ق ن ا . دي دج ج ه ن ة ا ش ن ا . 2. ة و ط خ ل ا



ة ن ا خ IKEv1 ن م ق ق ح ت ، Topology Name ني ي ع ت ب م ق ، ة ذ ف ا ن ل a Create new VPN Topology ل ع 3. ة و ط خ ل ا

حيت افملا مادختسا متي ، لاثملا اذه ضارغل . بيوت عمال IKE قوف رقناو لوكوتوربلا رايتخا
ةقداصم ةقيرطك اقبسما هطبس مت يتلا .

يوديلا حاتفملا بتكا . Pre-shared manual key رتخاو ، ةلدسنم ةمئاق Authentication Type قوف رقنا
صنلا لوقح Key و Confirm Key لىع اقبسما كرتشملا .

Create New VPN Topology

Topology Name:* Policy-Based-to-Azure

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh5_5

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:* Pre-shared Automatic Key
Pre-shared Manual Key
Certificate

IKEv2 Settings

Policy:* AES-GCM-NULL-SHA

Authentication Type: Pre-shared Automatic Key

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

Endpoints IKE IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh5_5

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

ف . ةديج ةسايس عاشناب 1 ةلحرمل تاملعم و ISAKMP ةسايس نيوكتب مق . 4 ةوطخل

رتخاو جهنلا مسادح .ةديج ISAKMP ةسايس ةفاضلا green plus button لىل رقنا ،راطلا سفن . Save رقناو ،ةقداصل او رمل او ةقيرطو Diffie-hellman ةومجمو ةئجتلاو بولطملا ريفشتلا

The image shows the configuration interface for a new VPN topology. The main window is titled "Create New VPN Topology" and has several tabs: "Endpoints", "IKE", "IPsec", and "Advanced". The "IKE" tab is selected, and the "IKEv1 Settings" section is visible. A red circle highlights a green plus icon next to the "Policy" dropdown menu. A "New IKEv1 Policy" dialog box is open, showing the following fields and values:

- Name: Azure-policy-based
- Description: (empty)
- Priority: (empty) (1-65535)
- Encryption: 3des
- Hash: SHA
- Diffie-Hellman Group: 2
- Lifetime: 86400 seconds (120-2147483647)
- Authentication Method: Preshared Key

Red arrows point to the values in the Name, Encryption, Hash, Diffie-Hellman Group, Lifetime, and Authentication Method fields.

لىل Static رايخا ،ةلودج IPsec لىل لقتنا .2 ةلحرمل تاملعم وأ IPsec جهن نيوكت .5 ةوطخلا رايخ Transform Sets في IKEv1 IPsec Proposals نم زمر edit pencil قوف رقنا .رايخا Crypto Map Type

Create New 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

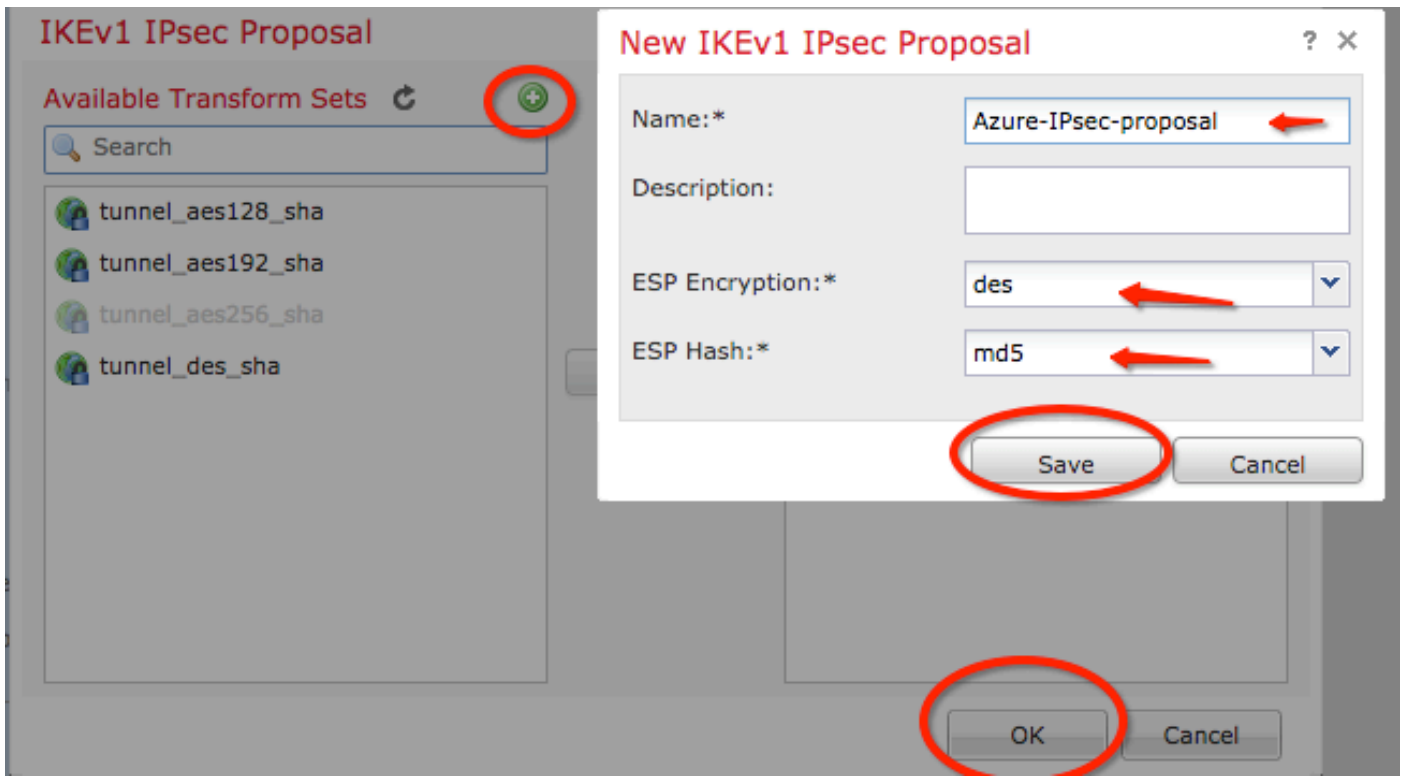
Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

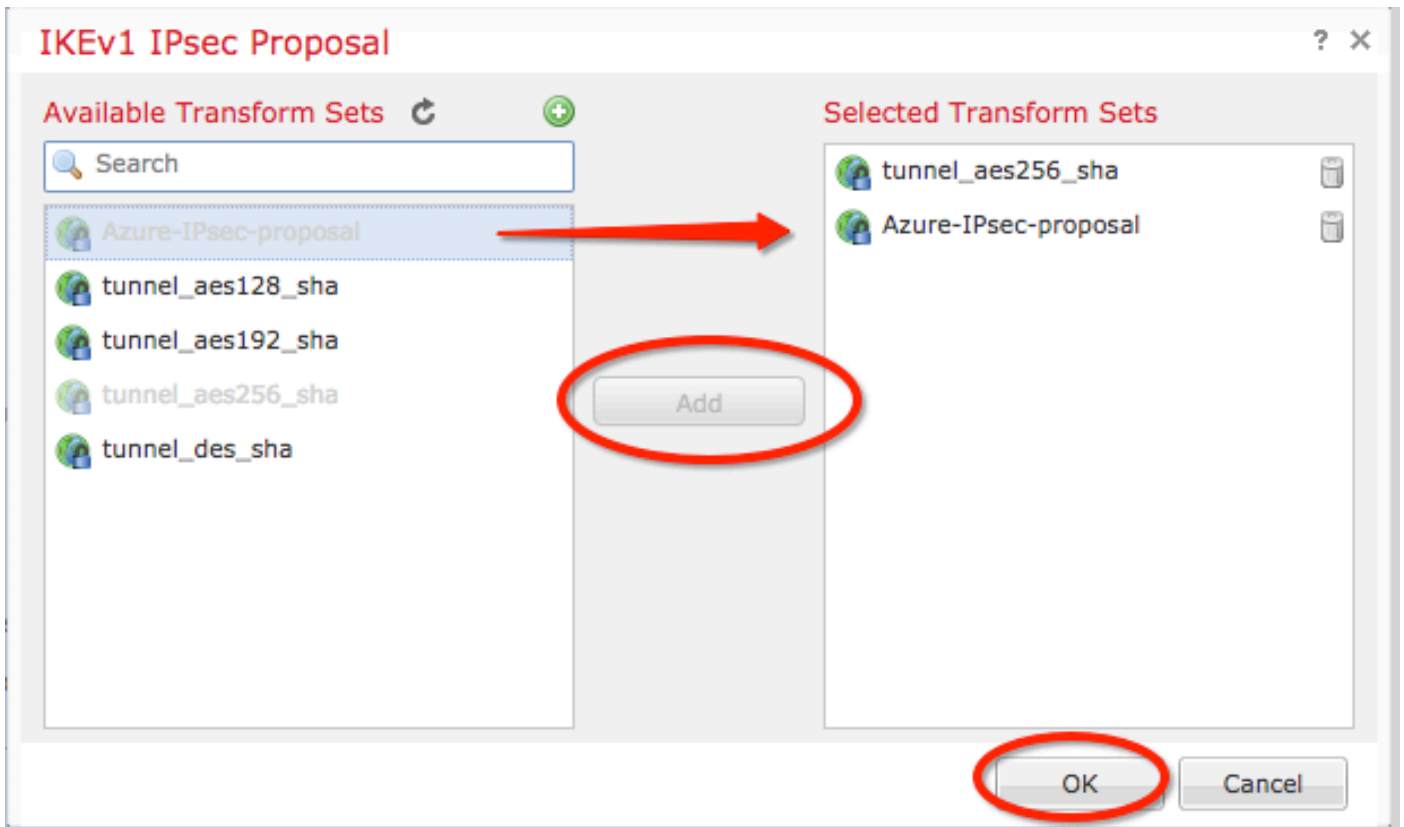
Lifetime Size: Kbytes (Range 10-2147483647)

ESPv3 Settings

6. قوف رونا، راطا IKEv1 IPsec Proposal لى لى. دىج IPsec حرتقم عاشن ا 6. ة وطلال
ةئجت تايمزراوخو ESP ريفش لة بولطم ل تامل عمل او جهن ل م سا دح. دىج م سا ة اضا ل
Save. قوف رونا و ESP



ع طقم Selected Transform Sets إلى دي دجال IPsec جهن فضا، راطا IKEV1 IPsec Proposal إلى ع 7. ة واطخل
OK . ة ق ط ق و



ه م ح و ي ض ا ر ت ف ا ل ا ر م ع ل ا ة د م ن ي و ك ت ب م ق ، ب ي و ب ت ل ا ة م ا ل ع I P S e c ل ا ة د و ع 8 ة و ط خ ل ا ن ي ب و ل ط م ل ا .

Create New 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

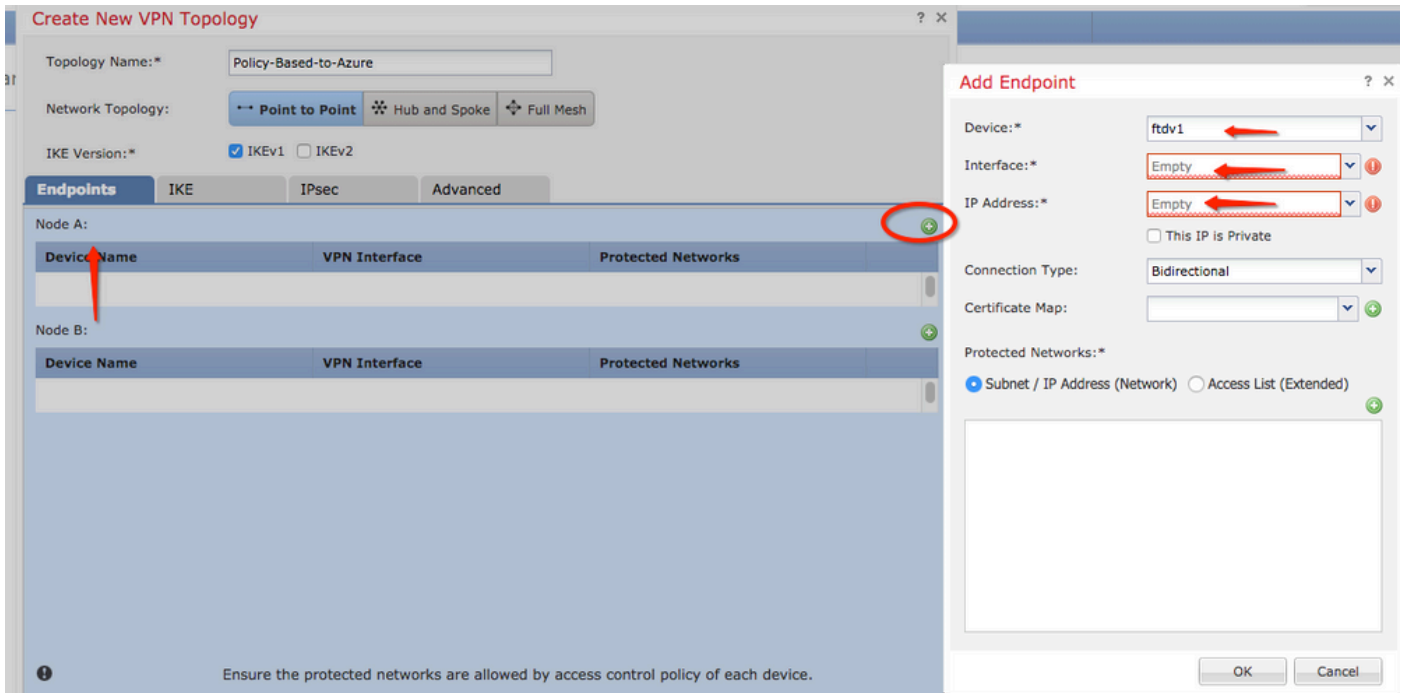
Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

— ESPv3 Settings

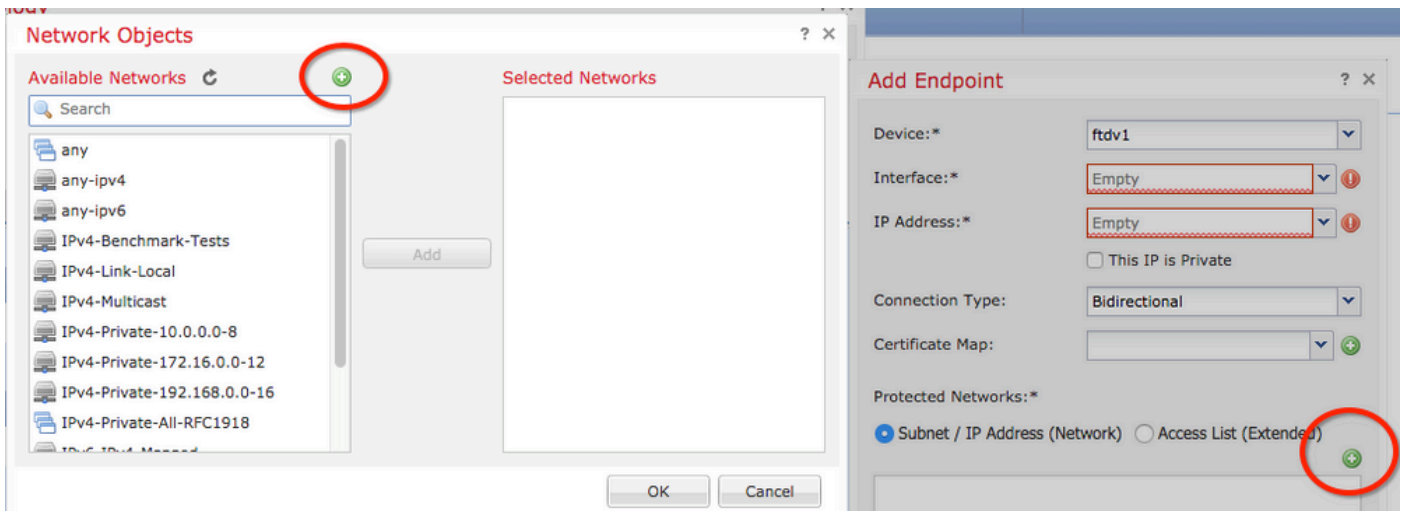
ل ا ل ق ت ن ا . ة ي م ح م ل ا ت ا ك ب ش ل ا / ت ا ن ا ي ب ل ا ر و ر م ة ك ر ح ت ا د د ح م / ر ي ف ش ت ل ا ل ا ح م ر ت خ ا . 9 ة و ط خ ل ا ي ف . د ي د ج م س ا ة ف ا ض ا ل ا g r e e n p l u s b u t t o n ع ط ق م ل ا ق و ف ر ق ن ا N o d e A ل ع . ب ي و ب ت ة م ا ل ع E n d p o i n t s ل F T D . ل ة ي ل ح م ة ي ع ر ف ت ا ك ب ش ك A ة د ق ع ل ا م ا د خ ت س ا م ت ي ، ل ا ث م ل ا ا ذ ه



ةي داملا ةه جاولا عم لدسنم Device لىل عمادختس ال FTD دح ، راطا Add Endpoint لىل عم 10 ةوطخلال م ادختس ال ل IP ناو نعو .

ال 11 ةوطخلال green قوف رقنا م Protected Networks لىل لقتنا ، ةي ل حمل رورملا ة كرح ددحم دي دحتل . 11 ةوطخلال plus button لىل ءاشن ل .

ال 12 ةوطخلال Available Networks بنجاب green plus button لىل رقنا ، ةذفان Network Objects لىل عم 12 ةوطخلال دي دج ي حمل رورم ة كرح ددحم لىل ءاشن ل .



ال 13 ةوطخلال لذل اق فورتحا م ، نىل م سا نىي عتب مق New Network Object لىل عم 13 ةوطخلال Save قوف رقنا م . FQDN/ق اطنل/ة ك ب ش ل /ل في ضملا .

New Network Object

? X

Name: local-ftd

Description:

Network: Host Range Network FQDN

192.168.20.0/24



Allow Overrides:

Save Cancel

OK رونا . OK رقنو ةذفان Network Objects ن ع مسق Selected Networks لى لى نئلكلا ةفاضل . 14 ةوطخل
ةذفان Add Endpoint لى ع .

Network Objects

? X

Available Networks  

Search

local-ftd

any

any-ipv4

any-ipv6

IPv4-Benchmark-Tests

IPv4-Link-Local

IPv4-Multicast

IPv4-Private-10.0.0.0-8

IPv4-Private-172.16.0.0-12

IPv4-Private-192.168.0.0-16

IPv4-Private-All-RFC1918

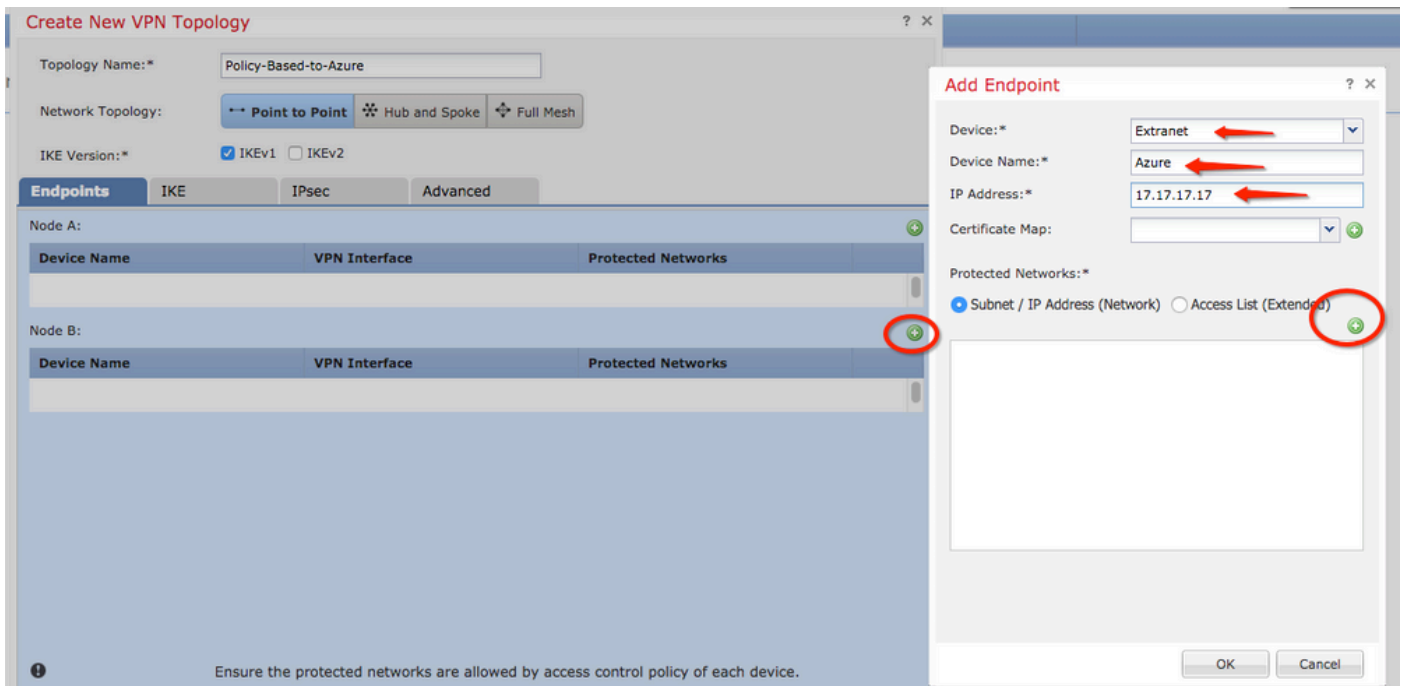
Selected Networks

local-ftd

Add

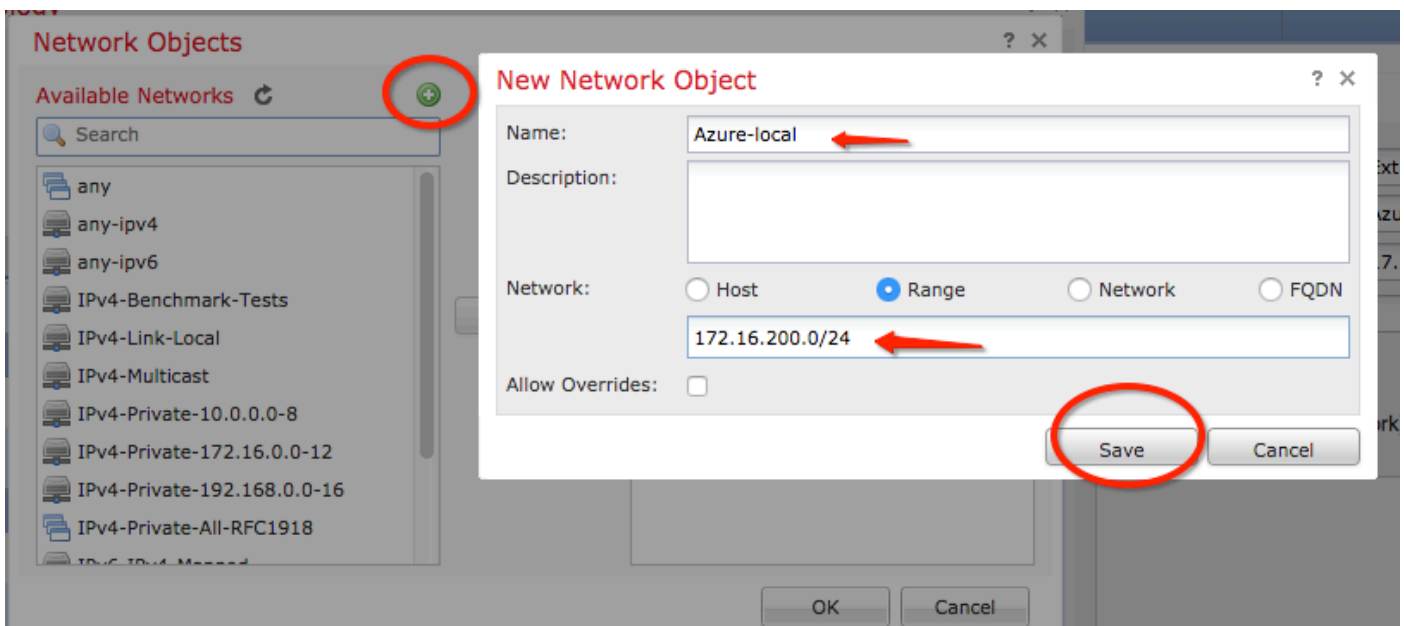
OK Cancel

Azure ةياهن ةطقن ، لاثملا اذه يف يه يتلاو ، B ةدقعلا ةياهن ةطقن فيرعتب مق . 15 ةوطخل
ددحم ةفاضل **green plus button** قوف رونا م **Node B** لى لى لى لى ، ةذفان **Create New VPN Topology** لى ع
ةرظنلا ةياهنلا طاقن عيمجل ةبسنلاب Extranet ديدحت . ةديعبلا ةياهنلا ةطقن رورم ةكرح
اهسفن (FMC) ةيساسال ةرادال يف مكحتلا ةدحو ةطساوب اهترادإ متت ال يتلا VPN ةكبشل
هب صاخلا IP ناونعو (طقف ايلحم مهملا) زاهجلا مسابتك . A ةدقعلا ةصاخلا

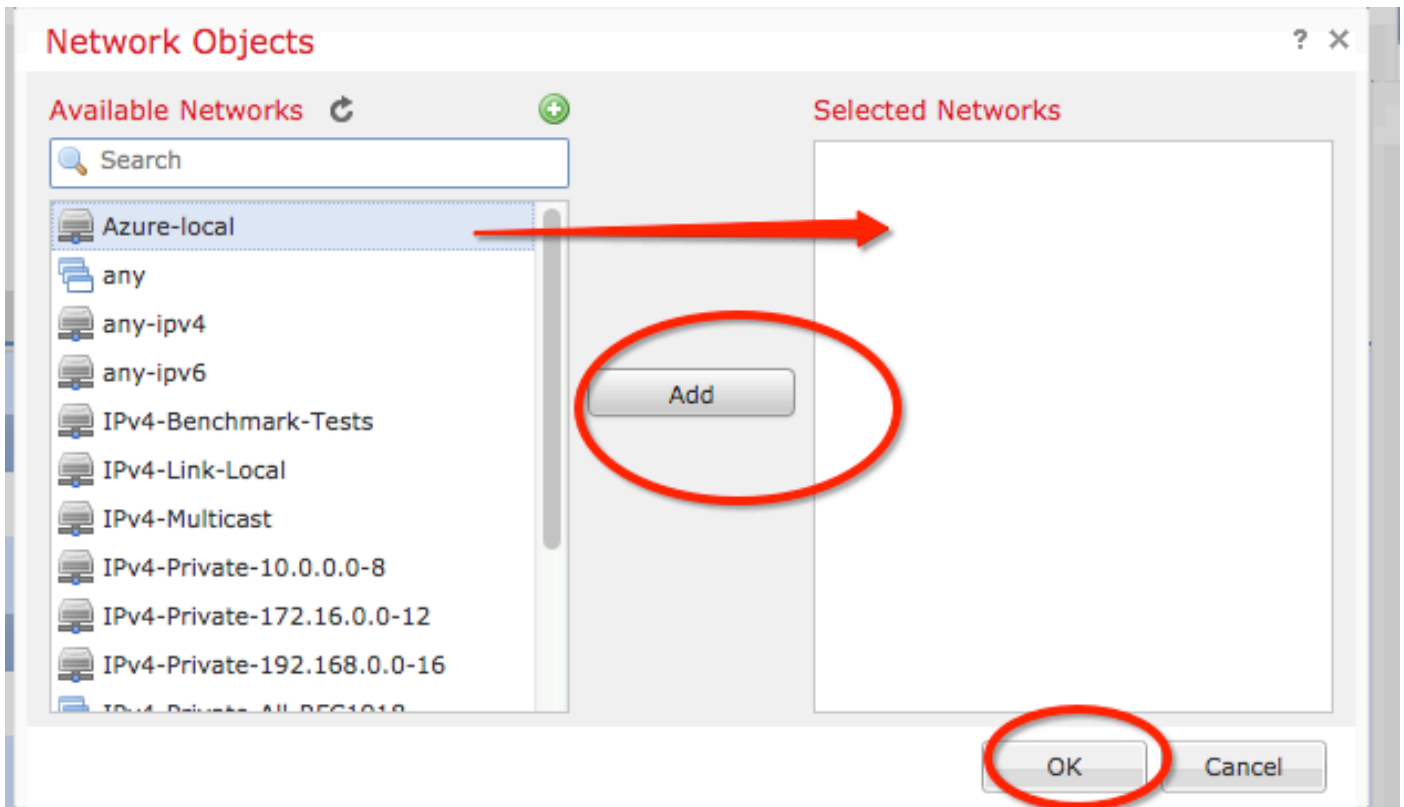


رقنا مٹ Protected Networks ىل لقتنا .دعب نع رورملا ةكرح ددحم نئاك عاشناب مق 16. ةوطخلا
 ديدج نئاك ةفاضل green plus button قوف .

صن Available Networks بنجاب green plus button ىل رع رقنا ،ةذفان Network Objects ىل رع 17. ةوطخلا
 كلذل اقفور تخأ مٹ ،نئاكلا مسا نبيعتب مق New Network Object ىل رع .ديج نئاك عاشناب
 Save .رقنا و FQDN/ةكبشلال/اقاطنلال/افيضملا



Selected Networks ىل ديدجلال ديبعل نئاكلا فضا ،ةذفان Network Objects ىل رع 18. ةوطخلا
 ةذفان Add Endpoint ىل رع Ok .رقنا . OK ةق قوطوع طقم



ة كرح تاددحم عم دقعلا الك نآلا هتيؤر كنكمي يذلا راطإلا Create New VPN Topology لىع 19. ةوطخلا
ة صاخلا ةحيحصلا ةيحمملا تاكبشلا/رورملا Save . رقنا .

Create New VPN Topology

Topology Name:* Policy-Based-to-Azure

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Node A:

Device Name	VPN Interface	Protected Networks
FTD	1.1.1.1	1.1.1.1 Private 192.168.0.0-16

Node B:

Device Name	VPN Interface	Protected Networks
Azure	17.17.17.17	Azure-local

Ensure the protected networks are allowed by access control policy of each device.

Save Cancel

FTD، رسي ألي يولع ال اعزل الي في Deploy رقنا، FMC تامولعم ةحول في 20. ةوطخلال
Deploy رقناو .

ةزهجال ةبس نلاب لال ال وه امك هس فن VPN نيوكت ودي، رم اوألا رطس ةهجاو لىل ع 21. ةوطخلال
ASA.

ةسايسلا لىل ةدنتسملا رورملا ةكرح تاددحم عم راسملا لىل دننتسم IKEv2

اذه عبتا، ريفشلال طئارخ عم ASA لىل ع قوم لىل ع قوم نم IKEv2 VPN لىل ع لوصحلل
نيوكت بجي هنأو راسملا لىل ةدنتسملا VPN ةكبش ل Azure نيوكت نم دكأت. نيوكتل
PowerShell مادختسا لال ل Azure لخدم في UsePolicyBasedTrafficSelectors

عضو عم نارقتال اب UsePolicyBasedTrafficSelectors نيوكت Microsoft نم [دنتسملا اذه](#) فصي
ريفشلال طئارخ عم ASA لشف في، ةوطخلال هذه لامتك نودب. راسملا لىل دننتسملا Azure VPN
نم اهلابقتسا مت يتل رورملا ةكرح تاددحم في قباطت مدع ب بسب لاصتال اعاشن في
Azure.

ريفشلال ةطيرخ نيوكت تامولعم مادختساب لملاب ل ASA IKEv2 ل [اذه Cisco دننتسم](#) عجار.

ةجراخلال ةهجاو لىل ع IKEv2 نيوكت 1. ةوطخلال

صاخلا ريفش تالاولم اكلتلا تامس عم ضراعتت تامولعم رشنب Microsoft تم اق: **ةظحال** ةجر دمل تامس لاريفوت متي. Azure لقب نم ةمدختسم ل IPsec نم ةيناثلا ةلجرمل باب ةمس تامولعم 2 ةلجرم ل. [ملاع لكشب رفوتم ل اذه Microsoft دن تسم](#) نم دهج لضفأب م ع دب لصتا، حيصوتلا نم ديزمل. [إنه](#) تا ضراعتلا [رهظت](#) يتلا Microsoft ل Azure. Microsoft

```
Cisco-ASA(config)#crypto ipsec ikev2 ipsec-proposal SET1
Cisco-ASA(config-ipsec-proposal)#protocol esp encryption aes
Cisco-ASA(config-ipsec-proposal)#protocol esp integrity sha-1
```

يلع يوتحت يتلاو، ةيجراخلا ةهجاو ليلع اهق يبطتو ريفشت ةطيخ نيوكتب مق. 6 ةوطخلا ةيلاتلا تانوكمل:

• ريفظن ل IP ناو نع

• ةدئافل رورم ةكرح يلع يوتحت يتلا ةدجرم ل لوصول ةمئاق:

• IPsec 2 ةلجرم ل IKEv2 حرتقم

• ي ناو ثلاب IPsec نم 2 ةلجرم ل عاقب ةدم

• حيتافم نم ديدج جوز عاشن ل يلدوي امم، (PFS) ةيلاثم ل هي جوتلا ةداع ةيرسل يراي تخ | دادع | PFS نم نيبنجال الك نيكم تبجي) تانا يبل ةيامل امدختس | متي يتلا Diffie-Hellman (2 ةلجرم ل روهظ لقب

PFS تامسو IPsec ب صاخلا 2 ةلجرم ل عاقب ةدم عم ضراعتت تامولعم رشنب Microsoft تم اق ل Azure لقب نم ةمدختسم ل.

[ملاع لكشب رفوتم ل اذه Microsoft دن تسم](#) نم دهج لضفأك ةجر دمل تامس لاريفوت متي

حيصوتلا نم ديزمل. [إنه](#) تا ضراعتلا [رهظت](#) يتلا Microsoft نم IPsec ةمس تامولعم 2 ةلجرم ل Microsoft Azure م ع دب لصتا

```
Cisco-ASA(config)#crypto map outside_map 20 match address 100
Cisco-ASA(config)#crypto map outside_map 20 set peer 192.168.1.1
Cisco-ASA(config)#crypto map outside_map 20 set ikev2 ipsec-proposal myset
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime seconds 27000
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime kilobytes unlimited
Cisco-ASA(config)#crypto map outside_map 20 set pfs none
Cisco-ASA(config)#crypto map outside_map interface outside
```

ءانثتس | ةدعاق عاشن |. ةدعاق nat رخآ ي ل رورم ةكرح VPN ل عضيخ ال نأ تنمض. 8 ةوطخلا NAT:

```
Cisco-ASA(config)#nat (inside,outside) 1 source static 10.2.2.0_24 10.2.2.0_24 destination static 10.1.1.0_24 10.1.1.0_24 no-proxy-arp route-lookup
```

تانئاك تاعومجم عاشن ل يلع بجي، ةددعتم ةي عرف تاكبش م ادختس | دن ع: **ةظحال** NAT. ةدعاق ي ف اهل م عتساو ةهوجل او ردصم ل ةي عرف ل تاكبش ل عي م ادختس اب

```
Cisco-ASA(config)#object-group network 10.x.x.x_SOURCE
Cisco-ASA(config-network-object-group)#network-object 10.4.4.0 255.255.255.0
Cisco-ASA(config-network-object-group)#network-object 10.2.2.0 255.255.255.0
```

```
Cisco-ASA(config)#object network 10.x.x.x_DESTINATION
Cisco-ASA(config-network-object-group)#network-object 10.3.3.0 255.255.255.0
Cisco-ASA(config-network-object-group)#network-object 10.1.1.0 255.255.255.0

Cisco-ASA(config)#nat (inside,outside) 1 source static 10.x.x.x_SOURCE 10.x.x.x_SOURCE
destination static 10.x.x.x_DESTINATION 10.x.x.x_DESTINATION no-proxy-arp route-lookup
```

تحصيل نم ققحتلا

قفن ةئيه تب Azure موقوي، ةباوبو ASA ءاوس دح ىلع لىكشتلا تنأ متي بقع
رمأ اذه عم ححص لكشب ينبي ققحتلا نأ تقود عيطتسي تنأ VPN.

ىلوالا ةلحرمل

(SA) ىلوالا ةلحرمل نامأ نارتقا ءاشنإ نم ققحت

IKEv2

ب ةي لحرمل ةي جراخلا ةهجاو لا نم هؤاشنإ مت يذلا SA IKEv2 ضرع متي، كلذ دعب
ل تي نب ححص SA عرف اضيأ كانه. IP 192.168.2.2 ةديعبلا ةهجاو لا ىلإ، UDP 500 ذفنم ىلع
ربع ققحتي نأ رورم ةكرح رفش ي.

```
Cisco-ASA# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:44615, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
Status Role
3208253 192.168.1.2/500 192.168.2.2/500
READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/142 sec
*-->Child sa: local selector 192.168.0.0/0 - 192.168.0.255/65535
remote selector 192.168.3.0/0 - 192.168.3.255/65535
ESP spi in/out: 0x9b60edc5/0x8e7a2e12
```

عم IP 192.168.2.2 ريظنل ئدابك ASA مادختساب هؤاشنإ مت يذلا SA IKEv1 ضرع متي، انه
ةيناث 86388 نم ءاقب ةرتف.

```
Cisco-ASA# sh crypto ikev1 sa detail
```

IKEv1 SAs:

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 192.168.2.2
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
Encrypt : aes Hash : SHA
Auth : preshared Lifetime: 86400
Lifetime Remaining: 86388
```

ةيناثلا ةلحرمل

show crypto ipsec sa peer [peer-ip] نام ا نارتقا نأ نم ققحتلا

```
Cisco-ASA# show crypto ipsec sa peer 192.168.2.2
peer address: 192.168.2.2
Crypto map tag: outside, seq num: 10, local addr: 192.168.1.2

access-list VPN extended permit ip 192.168.0.0 255.255.255.0 192.168.3.0 255.255.255.0
local ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer: 192.168.2.2

#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.1.2/500, remote crypto endpt.: 192.168.2.2/500
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 8E7A2E12
current inbound spi : 9B60EDC5
```

```
inbound esp sas:
spi: 0x9B60EDC5 (2606820805)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 182743040, crypto-map: outside
sa timing: remaining key lifetime (kB/sec): (4193279/28522)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x0000001F
```

```
outbound esp sas:
spi: 0x8E7A2E12 (2390371858)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 182743040, crypto-map: outside
sa timing: remaining key lifetime (kB/sec): (3962879/28522)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

ةطقن تيبتت مت .ءاطخأ نود IPsec SA ربع مزح عبرأ مالتسا متي و مزح عبرأ لاسرا متي .
عقوتم وه امك SPI 0x8E7A2E12 عم SA ةرداص ةدحاو و SPI 0x9B60EDC5 عم ةدراو ةدحاو لوصو

vpn-sessiondb l2l نم ققحتلا لالخ نم ققحتلا ربع تانايب لارورم نم ققحتلا اضيأ كنكمي
تالخدإ:

```
Cisco-ASA#show vpn-sessiondb l2l
```

Session Type: LAN-to-LAN

Connection : 192.168.2.2
Index : 44615 IP Addr : 192.168.2.2
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 400 Bytes Rx : 400
Login Time : 18:32:54 UTC Tue Mar 13 2018
Duration : 0h:05m:22s

IPSec SA ربع ةملتسملاو ةلسرمللا تانايبلا تادادع راهظا: Bytes Rx و Tx تايابلا تادحو

اهحالص او عاطخال فاشكتسا

صاخ Azure ل ل دعم يلخاد نراقلا لىل ع ASA ب VPN ل رورم ةكرح تملتس | نأ ةتقود 1. ةوطخال طاقتل نيوكتو يلخاد ليمع نم رمتسم لاصتا رابتخا نيوكت كنكمي، رابتخالل. ةكبش همالتس | نم ققحتلل ASA لىل ةمزح

[cap-name] [if-name] [src-ip] [src-mask] [dest-ip] [dest-mask] [لوكوتورب] قباطت [cap-name] ةهجاو طاقتل

show capture [cap-name]

```
Cisco-ASA#capture inside interface inside match ip host [local-host] host [remote-host]  
Cisco-ASA#show capture inside
```

2 packets captured

```
1: 18:50:42.835863      192.168.0.2 > 192.168.3.2: icmp: echo request  
2: 18:50:42.839128      192.168.3.2 > 192.168.0.2: icmp: echo reply
```

2 packets shown

ةكرح ملتسي/لسري و تي ن ب حي حص لكش ب VPN ل كلذ دع ب، Azure نم رورم ةكرح در تي ارن رورم.

ASA لىل حي حص لكش ب لسرمللا هي جوت نم ققحتت ف، ةدوجوم ريغ ردصملا رورم ةكرح تناك اذا

ققحتلل عبات ف، Azure نم درلا رورم ةكرح دوجو متي مل نكلو ردصملا رورم ةكرح ضرع مت اذا ب بسلا نم.

ASA ب ةجالع ام حي حص لكش ب نراق لخاد ASA لىل ملتسي رورم ةكرحلا نأ ةتقود 2. ةوطخال VPN لىل هجومو

ICMP لىل ةاكاجمل

Packet-tracer [inside-interface-name] ICMP [inside-host-ip] 8 0 [azure-host-ip]

انه مزحلل عبتتل ةلماكل مادختسالا تاداشرا لىل روثلل نكمي

<https://community.cisco.com:443/t5/security-knowledge-base/troubleshooting-access-problems-using-packet-tracer/ta-p/3114976>

```
Cisco-ASA# packet-tracer input inside icmp 192.168.0.2 8 0 192.168.3.2 detail
```

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x7f6c19afb0a0, priority=13, domain=capture, deny=false
hits=3, user_data=0x7f6c19afb9b0, cs_id=0x0, l3_type=0x0
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0000.0000.0000
input_ifc=inside, output_ifc=any

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

Forward Flow based lookup yields rule:

in id=0x7f6c195971f0, priority=1, domain=permit, deny=false
hits=32, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0100.0000.0000
input_ifc=inside, output_ifc=any

Phase: 3

Type: **ROUTE-LOOKUP**

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop 192.168.1.1 **using egress ifc outside**

Phase: 4

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x7f6c19250290, priority=0, domain=nat-per-session, deny=true
hits=41, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 5

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x7f6c1987c120, priority=0, domain=inspect-ip-options, deny=true
hits=26, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside, output_ifc=any

Phase: 6

Type: QOS

Subtype:

Result: ALLOW

Config:

Additional Information:

```
Forward Flow based lookup yields rule:
in id=0x7f6c19a60280, priority=70, domain=qos-per-class, deny=false
    hits=30, user_data=0x7f6c19a5c030, cs_id=0x0, reverse, use_real_addr, flags=0x0,
protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
    input_ifc=any, output_ifc=any
```

```
Phase: 7
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
```

Additional Information:

```
Forward Flow based lookup yields rule:
in id=0x7f6c1983ab50, priority=66, domain=inspect-icmp-error, deny=false
    hits=27, user_data=0x7f6c1987afc0, cs_id=0x0, use_real_addr, flags=0x0, protocol=1
    src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0, tag=any
    dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, tag=any, dscp=0x0
    input_ifc=inside, output_ifc=any
```

```
Phase: 8
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
```

Additional Information:

```
Forward Flow based lookup yields rule:
out id=0x7f6c19afela0, priority=70, domain=encrypt, deny=false
    hits=2, user_data=0x13134, cs_id=0x7f6c19349670, reverse, flags=0x0, protocol=0
    src ip/id=192.168.0.0, mask=255.255.255.0, port=0, tag=any
    dst ip/id=192.168.3.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
    input_ifc=any, output_ifc=outside
```

```
Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
```

Additional Information:

```
New flow created with id 43, packet dispatched to next module
Module information for forward flow ...
```

```
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_inspect_icmp
snp_fp_adjacency
snp_fp_encrypt
snp_fp_fragment
snp_ifc_stat
```

Module information for reverse flow ...

```
Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

VPN لا ىلع عقي ةمجرت nat نم ام تققود. (ةمجرت ياً قبطت ال) رورملا ةكرح يف عي NAT نأ طحال رورم ةكرح.

قېبېت مېتې شېح ەيەداملا ەجاولا ام نوكت نا بچې - چې حص output-interface نىم اضي ققحت ەيەراظلال قفنلا ەجاولا و ريفشلال ەطيخ.

لوصول ەمئاق طاقس تالاح روهظ مدع نىم دكأت

لعللاب قفنلا عاشن م ، ENCRYPT: ALLOW (VPN) ەيەراظلال ەصاخلال ەكبشلال ەلحرم ترهظ اذلا نىمضتلال تايلىم عم اتبثم IPsec SA ەيەور كنكنميو.

Packet-tracer قېبېت مېتې رهظت ENCRYPT: ALLOW اذلا 2.1. ەوطخللا

show crypto ipsec sa مادختساب رورملا ەكره ريفشلا و IPsec دعاسم تېبثت نىم ققحت

ASA نىم ەرفشملا مزحلال لاسرا نىم ققحتلال ەيەجراخللا ەجاولا لىل طاقتلال اارجل كنكنميو Azure نىم ەرفشملا تاباختسالا لابقتساب

Packet-tracer قېبېت مېتې رهظت ENCRYPT:DROP اذلا 2.2. ەوطخللا

ققفنلا بلجت ام دنع ەقوت م ەلاح ەذە .ضوافتلال دىق ەنكلو دعب VPN قفنلا عاشن مېم شودح ناكم ديدحتو قفنلا ضوافت ەيەلم عم ضرعل اطاخاللا چېحصت لىغشتب مق . ەرم لوال كلذ ثدح اذلا امولش ف

ەيەلم علل اناثأ ەلص تاذا اطاخاللا روهظ مدع نىم و IKE نىم چېحصلال رادصلالا لىغشت نىم ققحت ،الوا ەيەل ەكئاشلال

```
Cisco-ASA#debug crypto ike-common 255
```

```
Cisco-ASA# Mar 13 18:58:14 [IKE COMMON DEBUG]Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1. Map Tag = outside. Map Sequence Number = 10.
```

ەكره طاقسلا ينعى اذەف ، VPN رورم ەكره ادب دنع ەكئاش اطاخاللا چېحصت جارخلا يا رهظي مل اذلا لىل crypto ikev1/ikev2 نىم م مدع و ريفشلال ەيەلم عم لىل لصت نا لبق تانايىبال رورم مزحلال طاقسلا تايلىم عم و ريفشلال نىم نىم نىم ققحت .عب رمللا

يذلا IKE رادصلالا چېحصت م مقف ، ريفشلال ەيەلم عم لىغشت رهظت IKE-common اطاخاللا تناك اذلا قفنلا عاشن م لىل لشفلا شودح ناكم ديدحتو قفنلا ضوافت لىل لىل ضرعل ەنوكت م ت اب مادختساب Azure.

IKEv1

[لنە](#) ەللىلحت و iKEV1 ل لماكللا اطاخاللا چېحصت اارجل لىل روثللا نىم

```
Cisco-ASA#debug crypto ikev1 127
Cisco-ASA#debug crypto ipsec 127
```

IKEv2

[لنە](#) ەللىلحت و iV2 ل لماكللا اطاخاللا چېحصت اارجل لىل روثللا نىم

```
Cisco-ASA#debug crypto ikev2 platform 127
Cisco-ASA#debug crypto ikev2 protocol 127
Cisco-ASA#debug crypto ipsec 127
```

