

ةس اي س لـا ئـلـا ةـدـنـتـسـمـلـا ةـكـبـشـ نـيـوـكـتـ وـمـيـاـقـ وـمـيـاـقـ Microsoft Azure

تـايـوـتـحـمـلـا

[ةـمـدـقـمـلـا](#)

[مـيـهـاـفـمـلـا](#)

[رـيـفـشـتـ لـاجـمـ](#)

[ةـيـسـاسـأـلـاـتـابـلـطـتـمـلـا](#)

[تـابـلـطـتـمـلـا](#)

[ةـمـدـخـتـسـمـلـاـتـانـوـكـمـلـا](#)

[نـيـوـكـتـلـا](#)

[ةـيـلـعـ آـنـيـوـكـتـ ASA](#)

[ثـدـحـأـرـادـصـاـ وـأـ \(1\)ـ زـمـرـلـعـ ASA 9.8ـ عـمـ رـاسـمـلـاـ ئـلـاـ دـنـتـسـمـ](#)

[IKEv1ـ ئـلـعـ FTDـ IKEv2ـ](#)

[ةـسـايـسـلـاـ ئـلـاـ ةـدـنـتـسـمـلـاـ رـوـرـمـلـاـ ةـكـرـحـ تـادـدـحـمـ عـمـ رـاسـمـلـاـ ئـلـاـ دـنـتـسـمـ](#)

[قـحـصـلـاـ نـمـ قـقـحـتـلـا](#)

[ئـلـوـأـلـاـ ةـلـحـرـمـلـا](#)

[ةـيـنـاثـلـاـ ةـلـحـرـمـلـا](#)

[اهـالـصـ اوـعـاطـخـأـلـاـ فـاشـكـتـسـاـ](#)

[IKEv1](#)

[IKEv2](#)

ةـمـدـقـمـلـا

وـةـيـامـحـ رـادـجـ نـمـأـيـ ciscoـ ASAـ نـيـبـ VPNـ لـ نـيـوـكـتـلـاـ وـمـيـهـاـفـمـلـاـ ـةـقـيـثـوـاـذـهـ فـصـيـ Microsoftـ Azureـ.

مـيـهـاـفـمـلـا

رـيـفـشـتـ لـاجـمـ

رـيـفـشـتـلـاـ لـاجـمـ دـيـدـحـتـ مـتـيـ. VPNـ قـفـنـ يـفـ ةـكـرـاشـمـلـاـبـ IPـ IPSecـ نـيـوانـعـ قـاطـنـ حـمـسـيـ تـاقـاطـنـ دـيـدـحـتـلـ دـعـبـ نـعـ تـانـاـيـبـلـاـ رـوـرـمـ ةـكـرـحـ يـقـتـنـمـوـ يـلـحـمـ رـوـرـمـ ةـكـرـحـ دـدـحـمـ مـاـدـخـتـسـاـبـ كـانـهـ IPSecـ. ةـطـسـاـوـبـ اـهـرـيـفـشـتـ وـاهـطـاـقـتـلـاـ مـتـيـ يـتـلـاـ ةـدـيـعـبـلـاـوـ ةـيـلـحـمـلـاـ ةـيـعـرـفـلـاـ تـاـكـبـشـلـاـ وـأـ رـاسـمـلـاـ ئـلـاـ ةـدـنـتـسـمـلـاـ رـوـرـمـلـاـ ةـكـرـحـ تـادـدـحـمـ: VPNـ رـيـفـشـتـ تـاـلـاـجـمـ دـيـدـحـتـلـ نـاـبـوـلـسـأـ ةـسـايـسـلـاـ ئـلـاـ ةـدـنـتـسـمـلـاـ.

رـاسـمـلـاـ ئـلـاـ دـنـتـسـمـ:

ةـكـرـحـ تـادـدـحـمـ نـيـيـعـتـ مـتـ. IPSecـ قـفـنـ لـخـدـتـ رـوـرـمـ ةـكـرـحـ يـأـبـ حـامـسـلـلـ رـيـفـشـتـلـاـ لـاجـمـ نـيـيـعـتـ مـتـ ةـكـرـحـ يـأـنـأـ يـنـعـيـ اـذـهـوـ. 0.0.0.0ـ نـمـ ةـدـيـعـبـلـاـوـ ةـيـلـحـمـلـاـ تـانـاـيـبـلـاـ رـوـرـمـ ـةـهـجـوـلـاـ/ـرـدـصـمـلـلـ ةـيـعـرـفـلـاـ ةـكـبـشـلـاـ نـعـ رـظـنـلـاـ ضـغـبـ اـهـرـيـفـشـتـ مـتـيـ IPSecـ قـفـنـ ئـلـاـ اـهـهـيـجـوـتـ.

راسملاء دنتسملاء VPN ئەكپش Cisco نم (ASA) فىكتلل لباقلما نامالا زاچ معدي ثدحألا تارادصلالا او 9.8 تارادصلالا يف (VTIs) ئەرەاظلما قفنلما تاچ او مادختساب.

لبق نم ئارادملاء Cisco نم (FTD) ئەرەاظلما دض ئىامحلما وأ نمآلما ئەيامحلما رادج معدي مادختساب هىجوتلما دلۇع ۋەمىئاقدا (VPN) ئەرەاظلما ئەكپش (Firepower) ئەرادىزكىرم (FMC) ثدحألا تارادصلالا او 6.7 تارادصلالا يف VTI تاكپش.

ةسايسلاء دنتسملاء:

ردصملاء نم لكل طقق ئەنېيۇم IP تاقاطن رېفشتىلما لاجم نېيىعت مت نع رورملما ئەکرەت ددھم و ئاسايسلاء دنتسملاء دنلە ئەنلە ئەنلە رورملما ئەرەاظلما ددھم ددھي .ةھجولالا رباع اھرىفشت بجى يېتلما رورملما ئەکرەت ددھب.

8.2 رادصلالا يف رېفشتىلما طئارخ عم ئاسايسلاء دنلسملاء VPN ئەكپش ASA معدي ثدحألا تارادصلالا او

وا ئاسايسلاء دلۇع ۋەمىئاقلما وأ راسملاء ئەکرەت دادھم Microsoft Azure معدي مت يېتلما ئاسايسلاء دنلسملاء رورملما ئەکرەت تاددھم مادختساب راسملاء دلۇع ۋەمىئاقلما ھنىوكت كنكمى يذلا Internet Key Exchange (IKE) رادصلما دىيىقتب ايلاح Azure موقىي .اهتاكاھم يناثللا رادصلالا راسملاء دنلسملاء بولسالا دنلە ادانتسا لوكوتورب نم لۋالا رادصلالا ئاسايسلاء دنلسملاء دنلە دنلسملاء بولطتى امك، IKEv1، IKEv2، لوكوتورب نم بجىو Azure يف راسملاء دنلسملاء دىدھت بجىف، IKEv2 مادختسى مت اذا هنأ يىنعمى اذھو بجىف، زىمرلارادصلما بېبسې طقق رېفشتىلما طئارخ معدي ASA ناك اذا نكلى، ASA VTI، مادختسى راسملاء دنلسملاء ئاسايسلاء دنلسملاء رورملما ئەکرەت دىدھت تافلملل Azure نىوكت رايىخ ذىفنتل PowerShell ل ئېىصىنلارىپىلار شىن ربع لخدم يف كىلذ قىيقىحت مەتىي وانھ حضوم وھ امك Microsoft UsePolicyBasedTrafficSelectors:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-multiple-policybased-arm-ps>.

نېوكت روظنم نم صىخلىتلىل ASA و FTD:

- ل Azure نېوكت بجى ، رېفشت ئەطىرخ مادختساب ھنىوكت مت يذلا ASA/FTD ل ئەبسنلاب مادختساب راسملاء دنلسملاء دنلە ئاسايسلاء دنلسملاء دنلە UsePolicyBasedTrafficSelectors.
 - ل ئەبسنلاب ئەكپشل VPN نېوكت بجى ، مادختساب ھنىوكت مت يذلا ASA ل ئەبسنلاب راسملاء دنلسملاء دنلە.
 - انھ VTIs نېوكت ئېفېك لوح تامولۇملا نم دىزم دلۇع روٹىلما نكىمىي ، FTD ل ئەبسنلاب.
- 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

ةيىسالا تابلطتملا

تابلطتملا

ةيىلاتلما عيضاوملاب ئەفرۇم كىدل نوكت نأب Cisco يىصوت:

- زمر ASA: دلۇع VTI مادختسىت يېتلما IKEv2 راسملاء دنلسملاء VPN ئەكپشل ئەبسنلاب دنلە ئەنلە ئەنلە Azure نېوكت بجى). ثدحأ رادصلما وأ (1) 9.8 رادصلالا (.) راسملاء
- رېفشتىلما ئەطىرخ مادختسىت يېتلما IKEv1 ئاسايسلاء دنلسملاء VPN ئەكپشل ئەبسنلاب دلۇع نېوكت بجى). ثدحأ رادصلما وأ 6.2.0 FTD و ثدحأ رادصلما وأ 8.2 رادصلالا زمر ASA و FTD:

.) ئاسىسلا ىلى ۋە دەنەتسەملا VPN ۋە كېشل Azure

- رىفشتىلا ۋە طېيرخ مەدختىسىت يىتلە IKEv2 راسىملا ىلى ۋە دەنەتسەملا VPN ۋە كېشل ۋە بىسنىلاب زىمر ئاسىسلا ىلى ۋە دەنەتسەملا رورملا ۋە كەرەت تادىحەم ھەممىز ASA ىلىع رادصا و 8.2 نىيوكىت بجى). رىفشت ۋە طېيرخ مەدختىساب ھەنئىيوكىت مەت ۋە دەنەتسەملا (UsePolicyBasedTrafficSelectors.)
- ھەنئىيوكىت و FMC ۋە FTD ۋە دەنەتسەملا ىلى ۋە فەرۇم.

ۋە دەنەتسەملا تانووكىملا

ئەيلاتلا ۋە داملا تانووكىملار جەنمەرپەلا تارادصا ىلى دەنەتسەملا اذە يەن ۋە دراولە تامولۇغىمىلا دەنەتسەت:

- ASA نىم Cisco
- Microsoft Azure
- Cisco FTD
- Cisco FMC

ۋە صاخ ۋە لەمعەم ئەئىب يەن ۋە دەنەتسەملا اذە يەن ۋە دراولە تامولۇغىمىلا ئاشنە مەت تەنەك اذا. (يەپارتفا) حەوسىم نىيوكىت بى دەنەتسەملا اذە يەن ۋە دەنەتسەملا ۋە زەھەجەلە عەيمەج تادىب رەمما يەل لەمەتەجەل كەمەف نىم دەكتەن، لېغشەتىلا دېق كەتكېش.

نىيوكىتلا

مەدختىساب راسىملا ىلى اداھىتسا IKEv2 و IKEv1 راسىم نىيوكىت اما رەت خەلەپىشلىك شەتلىك steps. (ۋە طېيرخ) ئاسىسلا ىلى ۋە دەنەتسەملا رورملا ۋە كەرەت تادىحەم مەدختىساب ىلى اداھىتسا IKEv2 راسىم و VTI ىلىع رىفشتىلا ASA).

ۋە دەنەتسەملا IKEv1 نىيوكىت

نىيوكىت عېتىلا ASA نىم IKEv1 عەقۇم ىلى عەقۇم نىم VPN ۋە كېشل Azure، ئەلەخەنەدەم يەن ۋە دەنەتسەملا IKEv1 مەتىي لەخەنەدەم يەن ۋە دەنەتسەملا IKEv1 قەنن نىيوكىت نىم دەكتەن. يەيلاتلا لەڭەنلا اذەل ASA ىلىع رىفشتىلا.

نىيوكىت تامولۇغىمىلا لەڭەنلا اذە دەنەتسەم Cisco عەچار.

ۋە دەنەتسەملا IKEv1 نىيكمەت بى مۇق 1. ۋە طەخىللا.

```
Cisco-ASA(config)#crypto ikev1 enable outside
```

اھمەدختىساب مەتىي سەپەتلىك قەرطىلەتلىك زەراوخلە دەدھەت يەتلىك IKEv1 ئاسىس ئاشنە 2. ۋە طەخىللا رىفشتىلاو، ئايىھىللا ۋە روودو، دیفیھەلمن، ۋە قەداصىملار، ۋە ئىزجەتلىل.

حەتمەللا اذە Microsoft دەنەتسەم نىم دەھەج لەضفأ ۋە جەرمەللا IKEv1 1 ۋە جەرمەللا تامىس مەدقەت: ئەظەحالىم Microsoft Azure. مەع لەكشىپ

```
Cisco-ASA(config)#crypto ikev1 policy 1
Cisco-ASA(config-ikev1-policy)#authentication pre-share
Cisco-ASA(config-ikev1-policy)#encryption aes
Cisco-ASA(config-ikev1-policy)#hash sha
```

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

حاتفم وريظنلل IP ناونع نيوكتب مق وIPsec تامس تحت قفن ئومجم ئاشناب مق. 3. ئوطخلاراقبسم كرتشملا قفنلارا.

```
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)#ikev1 pre-shared-key cisco
```

تاونق عاشن او اهري فشت متيس يتلا رورملأا ةكرح ددحت لوصو ٰممئاق عاشناب مق. 4. ٰوطخلأ هيلع لوصحلأا مت ييذلأا قفنلأا نم رورملأا ةكرح يه ٰحلصلملأا رورم ةكرح، لاثملأا اذه يف. اهل تناك اذا ٰددعتم تالاخدا ٰيلع ٰوتتحي نأ نكمي و 10.1.1.0 ىلإ 10.2.2.0 ٰيعرفلا ةكبشلا نم عقاوملأا نيب ٰكرتشم ٰددعتم ٰعرف تاكبشكانه.

```
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
```

بجي. IKEv1. ئاس ألا ۋە ئەملىكلا نەمىزىت نأ بجي يىتلار، (TS) لىيوحىلىا ۋە مۇجمۇن يىوكتى. 5. ۋە طخلىا اپىأ دىعېبلا فرطلا ئىلۇق باطم TS ئاشنى.

حاتملا اذه Microsoft دنتسم نم دهج لضفأ ٖ ئىردىملا 2 ٖ لىحرملا تامس مدقق ئەظحالىم معىدلب لىستا، حىپوتلار نم دىزىملىك Microsoft Azure.

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

يوجتحت ييتلاو، ةيجراخلا ٥٥ج اولالا ىلع اهقيبطتو ريفشتلا ةطيرخ نيوكتب مق. ٦. ةوطخلالا
ةيلاتللا تانوكملا ىلع:

ریظن لـ IP ناونع

ةدىافل رورم ئىلە يوتحت يەتلا ئەدەھملا لوصول ئەمىاقد.

ب قوچوملا يس اس الما ئاظنلار

Azure قیائموں نال ارظن (PFS) ڈیل اسکی معاون ہیجوتلا ڈادا ڈیرس نیکی عتب نیوکتلا موقی اے PFS دادا نیکمٹ نکمی Azure. یف IKEv1 PFS لی طمعت لیلے صنٹ **ماع لکش ب ڈرفوت ملنا** اهم ادھت سا متی یتلا Diffie-Hellman حیتافم نم دی دج جوز عاشنے یلے ی دؤی ی ذلوا، ی رایت خا مادھت سا لالخ نم، (2 ڈل حرملا روہظ لباق PFS نم نی بن اجل اک نیکمٹ بجی) تانای بل اے امحل crypto map outside map 20 set pfs .

ديزمـل روـهـمـجـلـلـ قـحـاتـمـلـا Azure قـئـاثـوـ إـلـاـ ةـدـدـحـمـلـا IPSec لـمـعـ تـارـتـفـ نـمـ 2 ةـلـحـرـمـلـا دـنـتـسـتـ . معـدـبـ لـصـتـاـ، حـيـضـ وـتـلـاـ نـمـ Microsoft Azure.

```
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 ikev1 transform-set myset
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime seconds 3600
Cisco-ASA(config)#crypto map outside_map 20 set security-association lifetime kilobytes
102400000
Cisco-ASA(config)#crypto map outside_map interface outside

```

عانثتسا ٽدعاق عاشنإ . ٽدعاق nat رخآ ىلإ رورم ٽكرح VPN لـ ا عضخي ال نأ تنمض . 7 ٽوطخل 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

```

تانياك تاعومجم عاشنإ كيلع بجي ، ٽدعتم ٽيعرف تاكتبش مادختسإ دنع : ٽحالم ٽدعاق يف اهلامعتس او ٽهجهول او ردصملل ٽيعرفلاتاكتبشلا عيمج مادختساب NAT.

```

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

```

ٽدحأ رادصا وا (1) ASA 9.8 (1) دنتسم زمرىلع VTI ع راسملاء لـ

عابتا زمرىلع عقوم ىلإ عقوم نم راسملاء VPN ٽكبشل ٽبسنلاب نـيـوكـتـبـ مـوقـتـ الـ وـ رـاسـمـلـاـ ىـلـاـ ٽـدـنـتـسـمـلـاـ Azure ٽكبشل VPN نـيـوكـتـ نـمـ دـكـأـتـ . نـيـوكـتـلـاـ اـذـهـ UsePolicyBasedTrafficSelectors لـ خـدمـ يـفـ Azure . لـ اـلـ ASA .

لمـاـكـلـاـبـ ASAـ نـيـوكـتـ تـامـوـلـعـ مـىـلـعـ لـوـصـحـلـلـ [Cisco دنتسم](#) عـجـرمـ .

ٽـيـجـراـخـلـاـ ٽـهـجـاـوـلـاـ ىـلـعـ 1ـ نـيـكـمـتـ . ٽـوـطـخـلـاـ :

```

Cisco-ASA(config)#crypto ikev2 enable outside

```

نـمـ ىـلـوـأـلـاـ ٽـلـحـرـمـلـاـ جـهـنـ ٽـفـاضـاـ . 2ـ ٽـوـطـخـلـاـ .

ٽـلـحـرـمـلـاـ ٽـصـاخـلـاـ ٽـرـيـفـشـتـلـاـ ٽـزـيـمـ عـمـ ضـرـاعـتـتـ تـامـوـلـعـ رـشـنـبـ تـمـاـقـ : ٽـحالـمـ تـامـسـلـاـ رـيـفـوتـ مـتـيـ Azure . لـبـقـ نـمـ ٽـمـدـخـتـسـمـلـاـ رـمـعـلـاـ تـامـسـ وـ ٽـهـاـزـنـلـاوـ ٽـK~E~v~2~ نـمـ ىـلـوـأـلـاـ يـتـلـاـ تـامـوـلـعـمـلـاـ . [مـاعـلـكـشـبـ رـفـوتـمـلـاـ اـذـهـ Microsoft دنتسم](#) نـمـ دـهـجـ لـضـفـأـبـ ٽـجـرـدـمـلـاـ معـدـبـ لـصـتـاـ ، حـيـضـوـتـلـاـ نـمـ دـيـزـمـلـ . [اـنـهـ ٽـيـئـرـمـ Microsoft](#) نـمـ ٽـK~E~v~2~ Microsoft نـمـ ضـرـاعـتـتـ Microsoft Azure .

```

Cisco-ASA(config)#crypto ikev2 policy 1
Cisco-ASA(config-ikev2-policy)#encryption aes

```

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

يـف نـامـأـلا تـامـلـعـم دـيـدـحـتـ IKEv2ـ نـمـ 2ـ ةـلـحـرـمـلـلـ IPsecـ حـرـتـقـمـ ةـفـاضـاـ 3ـ ةـوـطـخـلـاـ:ـ نـيـوـكـتـلـاـ عـضـوـاـ ikev2 ipsec-proposalـ رـيـفـشـتـلـلـ:

AES-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 } زـارـطـلـاـ لـوـكـوـتـوـرـبـلـلـ ESPـ غـرـافـ { des | 3des | AES | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 } aes-192 | aes-256 | sha-1 | SHA-256 | SHA-384 | SHA-512 | aes-192 | aes-256 | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 } esp { md5 | sha-1 | SHA-256 | SHA-384 | SHA-512 | aes-192 | aes-256 | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 } غـرـافـ لـوـكـوـتـوـرـبـ لـمـاـكـتـ:

IPSecـ رـيـفـشـتـوـلـمـاـكـتـ تـامـسـعـ ضـرـاعـتـ تـامـوـلـعـمـ رـشـنـبـ تـمـاـقـ:ـ ظـاحـالـمـ
 ةـجـرـدـمـلـاـ تـامـسـلـاـ رـيـفـوـتـ مـتـيـ Azureـ اـهـمـدـخـتـسـتـ يـتـلـاـ ةـيـنـاـثـلـاـ ةـلـحـرـمـلـابـ ةـصـاخـلـاـ
 عـمـ ضـرـاعـتـ يـتـلـاـ تـامـوـلـعـمـلـاـ مـاعـ لـكـشـبـ رـفـوـتـمـلـاـ اـذـهـ Microsoftـ دـنـتـسـمـ نـمـ دـهـجـ لـضـفـأـبـ
 معـدـبـ لـصـتـاـ حـيـضـوـتـلـاـ نـمـ دـيـزـمـلـ .ـ اـنـهـ قـيـئـرـمـ Microsoftـ نـمـ 2ـ ةـلـحـرـمـلـلـ IPSecـ ةـمـسـ
 Microsoftـ Azureـ.

```
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
```

دـدـحـيـ يـذـلـاـ IPSecـ فـيـرـعـتـ فـلـمـ ةـفـاضـاـ 4ـ ةـوـطـخـلـاـ:

- 2ـ ةـلـحـرـمـلـاـ IVE2ـ لـ اـقـبـسـمـ هـنـيـوـكـتـ مـتـ يـذـلـاـ IPSecـ لـوـكـوـتـوـرـبـ حـرـتـقـمـ
- تـيـاـبـولـيـكـ وـأـوـيـنـاـوـثـلـاـبـ (ـيـرـايـتـخـ)ـ لـ 2ـ ةـلـحـرـمـلـلـ يـضـارـتـفـالـاـ رـمـعـلـاـ
- (ـيـرـايـتـخـ)ـ ةـعـوـمـجـمـ PFSـ

ةـلـحـرـمـلـلـ يـضـارـتـفـالـاـ رـمـعـلـاـ عـمـ ضـرـاعـتـ تـامـوـلـعـمـ رـشـنـبـ تـمـاـقـ:ـ ظـاحـالـمـ
 ةـجـرـدـمـلـاـ تـامـسـلـاـ رـيـفـوـتـ مـتـيـ Azureـ لـبـقـ نـمـ ـمـدـخـتـسـمـلـاـ PFSـ تـامـسـوـ IPSecـ نـمـ ةـيـنـاـثـلـاـ
 عـمـ ضـرـاعـتـ يـتـلـاـ تـامـوـلـعـمـلـاـ مـاعـ لـكـشـبـ رـفـوـتـمـلـاـ اـذـهـ Microsoftـ دـنـتـسـمـ نـمـ دـهـجـ لـضـفـأـبـ
 معـدـبـ لـصـتـاـ حـيـضـوـتـلـاـ نـمـ دـيـزـمـلـ .ـ اـنـهـ قـيـئـرـمـ Microsoftـ نـمـ 2ـ ةـلـحـرـمـلـلـ IPSecـ ةـمـسـ
 Microsoftـ Azureـ.

```
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
```

رـيـظـنـلـلـ IPـ نـاـونـعـ نـيـوـكـتـبـ مـقـ وـ IPSecـ تـامـسـ تـحـتـ قـافـنـأـ ةـعـوـمـجـمـ عـاـشـنـاـبـ مـقـ 5ـ ةـوـطـخـلـاـ:
 قـافـنـأـ ةـعـوـمـجـمـ كـرـتـشـمـلـاـ دـيـعـبـلـاـوـيـلـحـمـلـاـ قـفـنـلـاـ حـاتـفـمـ وـ:

```
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
```

نـيـعـيـ نـأـ VTIـ تـقـلـخـ 6ـ ةـوـطـخـلـاـ:

- [number] ۋەچاولى قىن دىدج قىن ۋەچاولى [number]
- name[name] دىدج قىن ۋەچاولى مىسا
- [ip] ناونع IP ناونع: قىنلا ۋەچاولى دوجوم رىغ IP ناونع
- قىنلا ردصم ۋەچاولى: اىلچىم VPN يەتنىت ثىچ قىنلا ردصم ۋەچاولى
- قىنلا Azure: [Azure Public IP] ۋەچاولى IP ناونع
- IPSec IPv4 ل قىنلا عضو: IPSec IPv4
- صاخلا IPsec فىرعت فلم: اذه VTI فىرعت فلممل ھمادختسا بولطملا IPsec فىرعت فلم قىنلا [profile-name] ۋەچاولى

```
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
```

نکاس راسم ۋەفاصلە. قىنلا لخاد رورملا ۋەكىحىلى ۋەرشىلل تباث راسم عاشناب مۇق. 7. ۋەطخلە رەمأىلا اذه لخدا، يېكىتاتسالا:

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

لەڭمەلە لېبسىلىق ۋەچاولى IP ناونع وە dest_ip و mask رەمأىلا ضرعى ۋەيعرفىلە ۋەكىشلىق (دوجوم رىغ وە دوجوم) IP ناونع يىأ نوكى نأ بىجى. ۋەچاولى رورملا ۋەكىحىجىوت وە gateway_ip اذه نەم ضرغىلا 169.254.0.2. 169.254.0.2 لىم، قىنلا ۋەچاولى ۋەچاولى اتسىل اھسەن ip ۋەصاخلا ۋە باوبىلا نكىلۇ، قىنلا.

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

ىلع IKEv1 نىيوكىت

زاحىج لىجىست كەمىزلى، Azure ىلى VPN IKEv1 نەم عقۇم ىلى عقۇم نەم ىنەن ئەتكەنلەپ FTD ىلى اقىبىسىم FTD.

1. ۋەطخلە اۇرىنىڭدىن، FMC dashboard > Devices > VPN > Site to Site.



2. ۋەطخلە Add VPN قۇف رقنى. دىدج جىن عاشناب مۇق. Firepower Threat Defense device رەتىخ او ۋەلدىسىنم ۋەمىئاقدا.



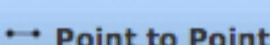
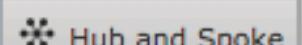
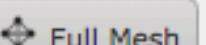
3. ۋەطخلە Create new VPN Topology Name، نىيىعىت بىرىق، ۋەذفانلىق ىلع IKEV1 نەم قىقىختى.

حیتافملا مادختس ا متی ، لاثمل ا اذه ضارغأ . بیوبت ةمالع IKE قوف رقنا او لوكوتوربلا رایتخا . ةقاداصم ةقيرطک اقبسم اهطبض مت يتلا

يوديل ا حاتفملا بتکا . ئەلسنم ئەمىئاق Authentication Type Pre-shared manual key . قوف رقنا صنلا لوقح Key و Confirm Key كرتشمل ا.

Create New VPN Topology

Topology Name: * Policy-Based-to-Azure 

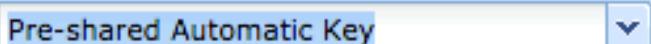
Network Topology:   

IKE Version: *  IKEv1 IKEv2 

IKE **Endpoints** **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 

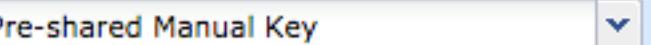
Authentication Type: Pre-shared Automatic Key 

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

Endpoints **IKE** **IPsec** **Advanced**

IKEv1 Settings

Policy: * preshared_sha_aes256_dh5_5 

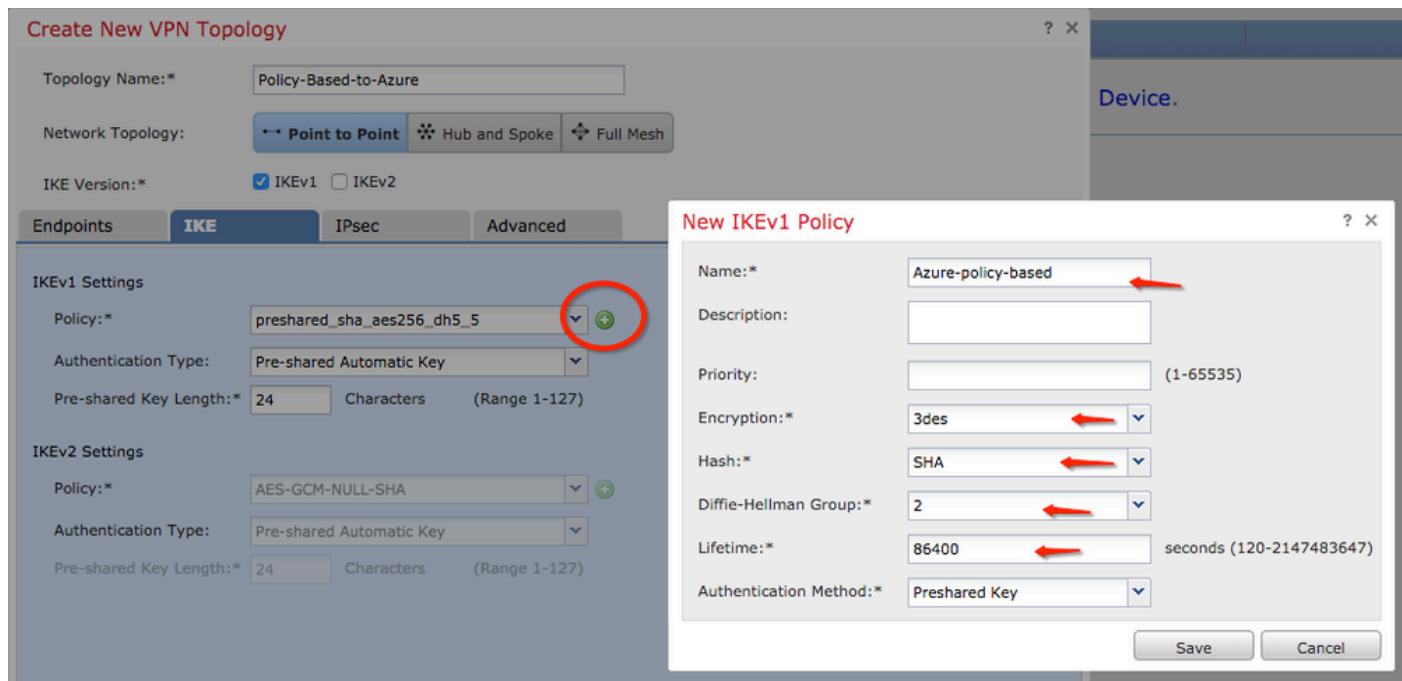
Authentication Type: Pre-shared Manual Key 

Key: * 

Confirm Key: * 

ي. ئەدىج ئەس ايىس عاشناب 1 ئەلحرملا تاملىع و ئاساكىپ نىوكتب مق. 4 ئەوطخلان

رتخ او جهـنـلـا مـسـا دـدـحـ . ةـدـيـدـجـ ISA~KMPـ ئـسـاـيـسـ ئـفـاضـالـ ئـلـعـ رـقـنـاـ ، رـاطـالـاـ سـفـنـ . رـقـنـاـوـ ، ئـقـدـاصـمـلـاـوـ رـمـعـلـاـ ئـقـيـرـطـوـ Diffie-hellmanـ ئـعـوـمـجـمـوـ ئـزـجـتـلـاـوـ بـوـلـطـمـلـاـ رـيـفـشـتـلـاـ . Saveـ .



ىـلـعـ رـايـتـخـ ، ئـلـوـدـجـ IPsecـ ئـلـاـ لـقـتـنـاـ . 2ـ ئـلـحـرـمـلـاـ تـامـلـعـمـ وـأـ IPsecـ ئـلـاـ لـقـتـنـاـ . 5ـ ئـوـطـخـلـاـ . رـايـخـ ئـفـ Staticـ Crypto Map Typeـ Transform Setsـ IKEV1 IPsec Proposalsـ edit pencilـ قـوـفـ رـقـنـاـ . رـايـتـخـ ئـنـاخـ .

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**

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals* 

tunnel_aes256_sha

IKEv2 IPsec Proposals 

AES-GCM

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

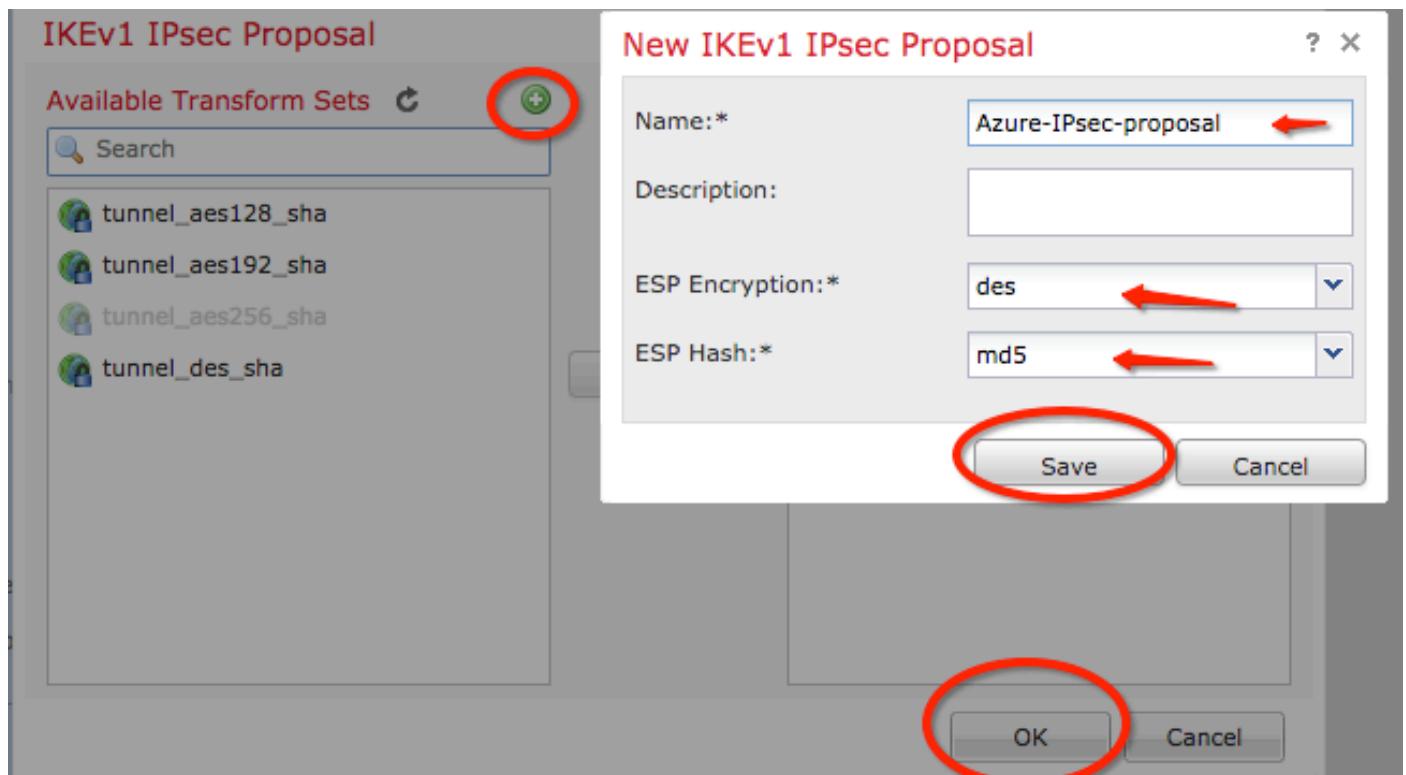
Modulus Group: 2

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

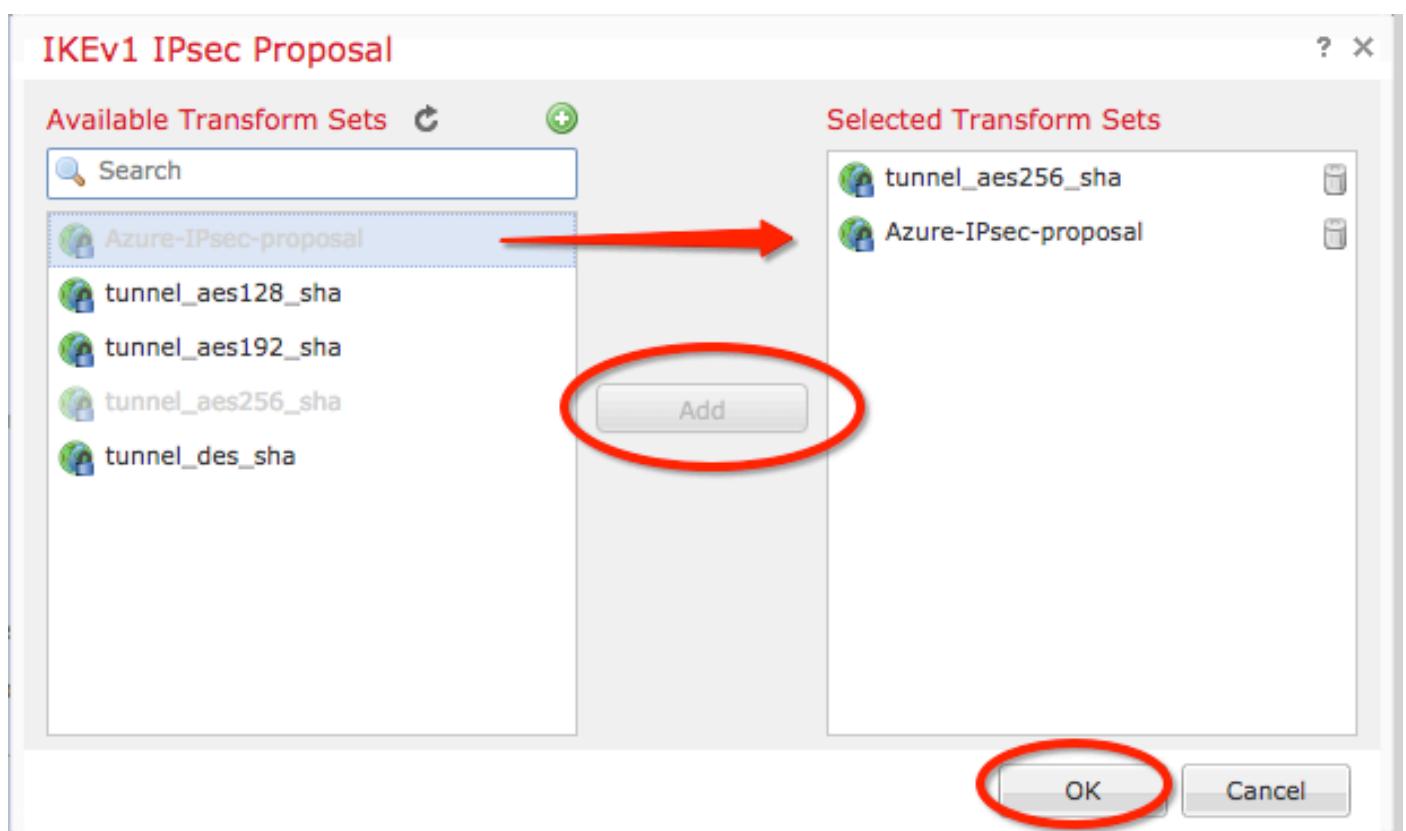
Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

—  **ESPv3 Settings**

6. ۋەتەخلى قوف رقنا، راطى IKEv1 IPSec Proposal ىلىع. دىدج حىرتقىم عاشنإ. قىچىت تايىمىزراو خە و ESP رېفشتىل ۋە بولطملى تامىلۇ جەنلەم مىسالا دىدج مىسا ئەفاضىل قوف رقنا او ESP Save .



عطقم Selected Transform Sets ىلى ديجلا IPsec جهن فضا، راطا IKEv1 IPsec Proposal ىل عطق طق طقا و OK .



مجموح يضر ارتفالا رمعلا ةدم نيوكتب مق ،بيوبتلاءماع IPSec ىلإ ةدعو 8. ةوطخلانـيـبـولـطـمـلـاـ

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* <input type="text" value="tunnel_aes256_sha, Azure-IPsec-proposal"/>	IKEv2 IPsec Proposals <input type="text" value="AES-GCM"/>
---	--

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

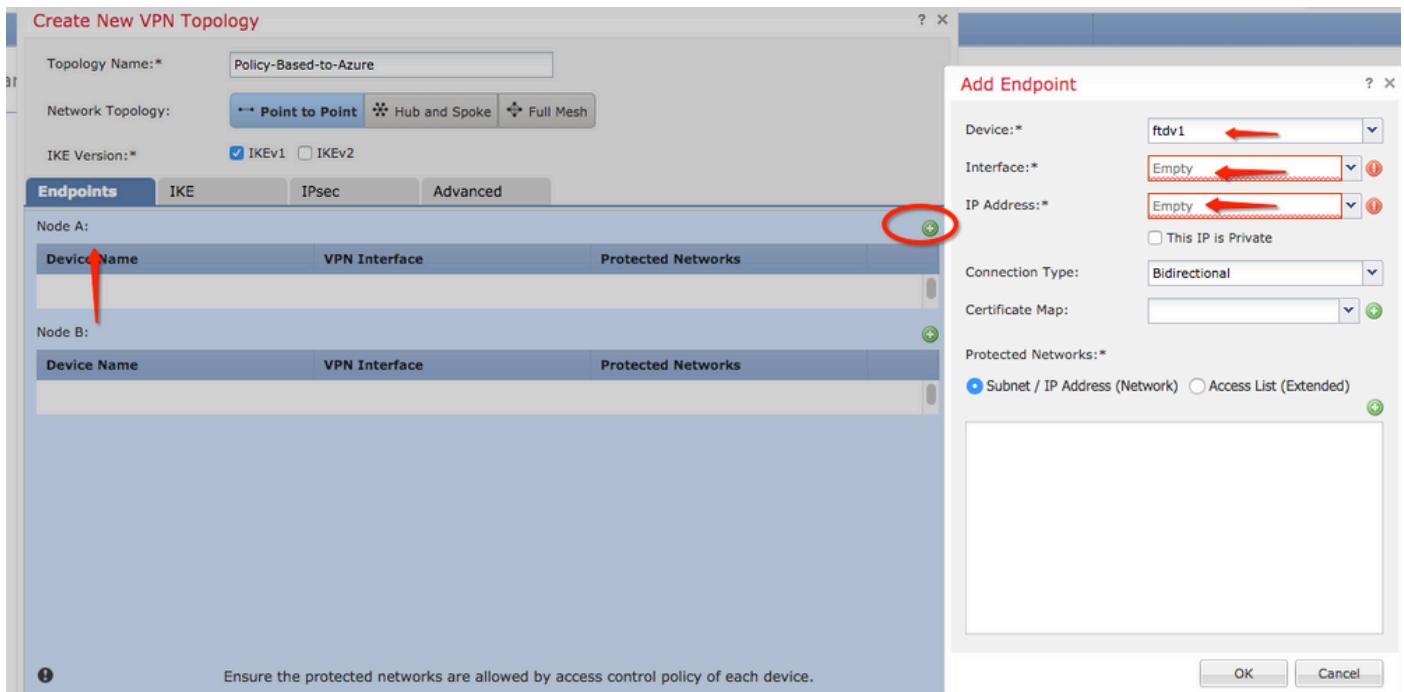
Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

ESPv3 Settings

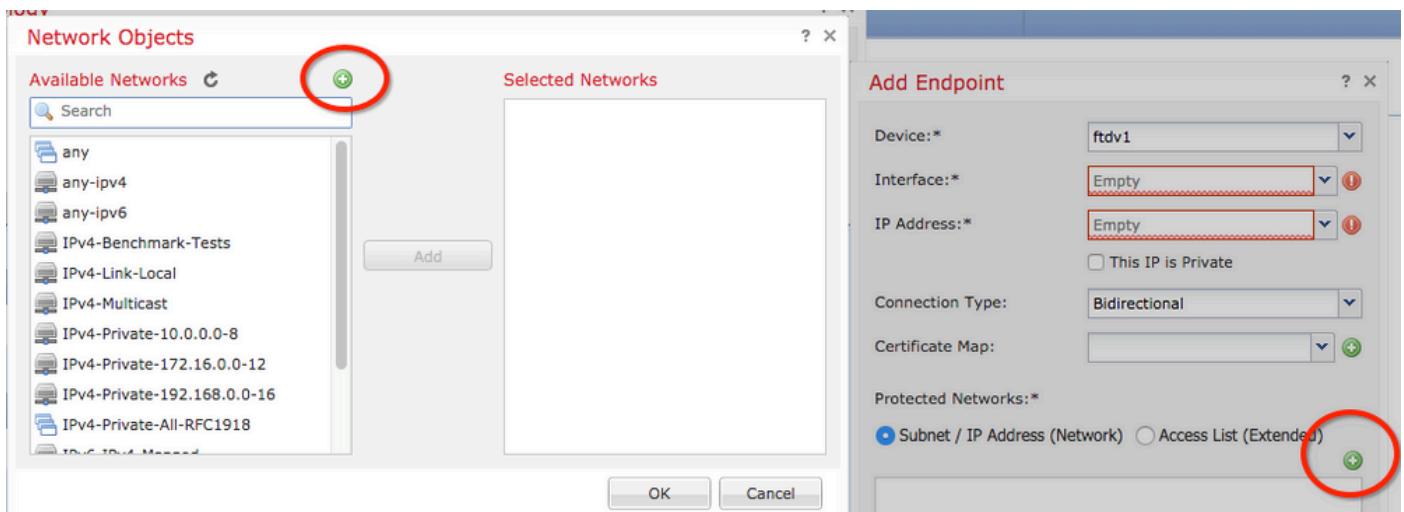
يلى لقتنا. ئى محملا تاكبىشل اتانا يى بىلا رورم ئى كىچ تاددحەم/رىفشتىلا لاجم رت خا 9. ئو طخلا يىف . دى دج مسا ئە فااضىل green plus button ع طقىمىلا قوف رقنى Node A ىلىع . بى ووبت ئە مالع Endpoints ل ئى لىحەم ئې عىرف تاكبىش ك A ئە دقىع لامادختىسا متىي ، لاثمىلما اذە FTD.



ئي داملا ۋەجىءە ئەم لەسەنم Device ىلىڭ دەدەن، راتاً مادختىسى ئەل دەدەن، 10. ۋەطخىلما مادختىسى ئەل IP ناونۇ وە.

ئى داملا ۋەجىءە ئەم لەسەنم Protected Networks ىلىڭ دەدەن، ۋەزىئە ئەل دەدەن، 11. ۋەطخىلما قوف رقنا مىت green plus button دەدەن، دى دەن ئەك ئاشنال.

ئى داملا ۋەجىءە ئەم Available Networks ىلىڭ دەدەن، ۋەزىئە ئەل دەدەن، 12. ۋەطخىلما green plus button Available Networks ىلىڭ دەدەن، دى دەن ئەك ئاشنال.



كەلذل اق فورتىخا مىت، نى ئاكىلا مسا نى يىعتب مۇق ىلىڭ New Network Object ىلىڭ دەدەن، ۋەزىئە ئەل دەدەن، 13. ۋەطخىلما FQDN/قاطىنلار/ةكبشىلار/فېضمەلار قوف رقنا مىت Save .

New Network Object

Name: local-ftd

Description:

Network:

- Host
- Range
- Network
- FQDN

192.168.20.0/24

Allow Overrides:

Save Cancel

رقنـا . OK رقـنـو ةـذـفـان Selected Networks نـع مـسـق Network Objects ئـلـا نـئـاـكـلـا ةـفـاضـاـ . 14 ةـوـطـخـلـا ةـذـفـان Add Endpoint ئـلـعـ.

Network Objects

Available Networks

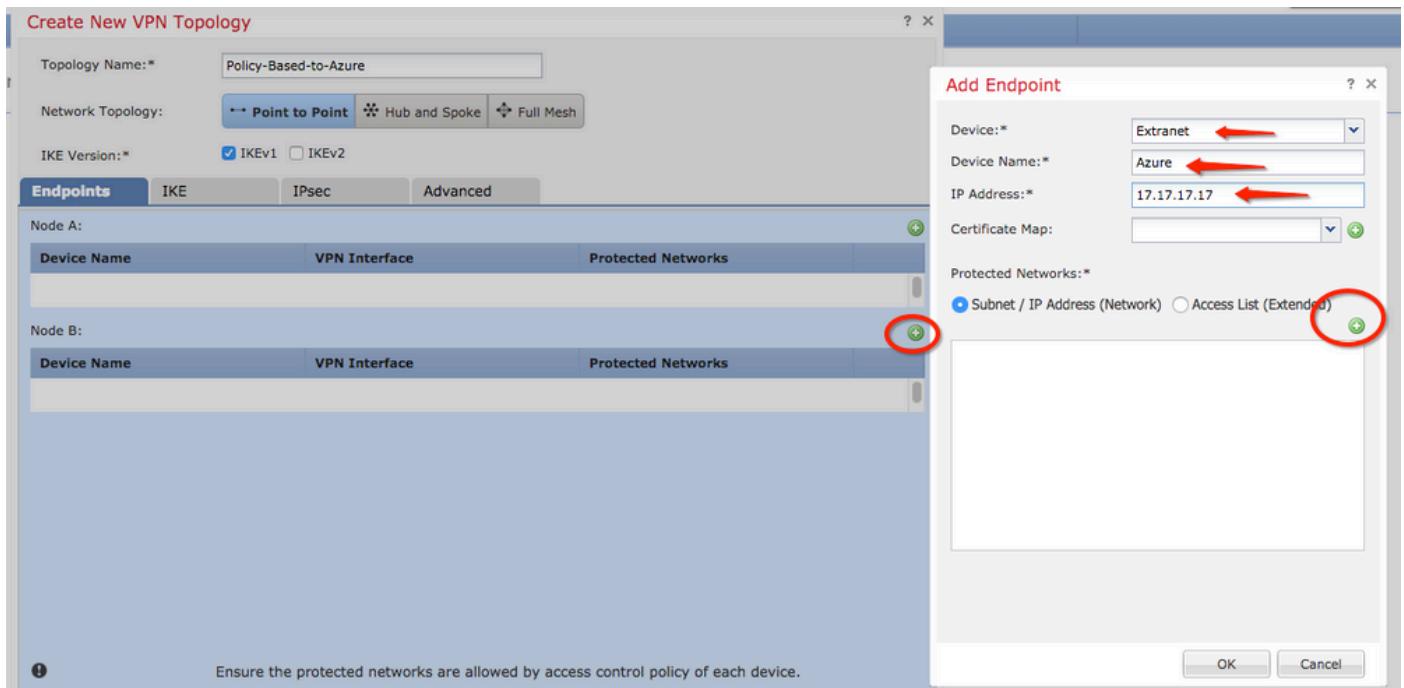
Selected Networks

local-ftd

Add

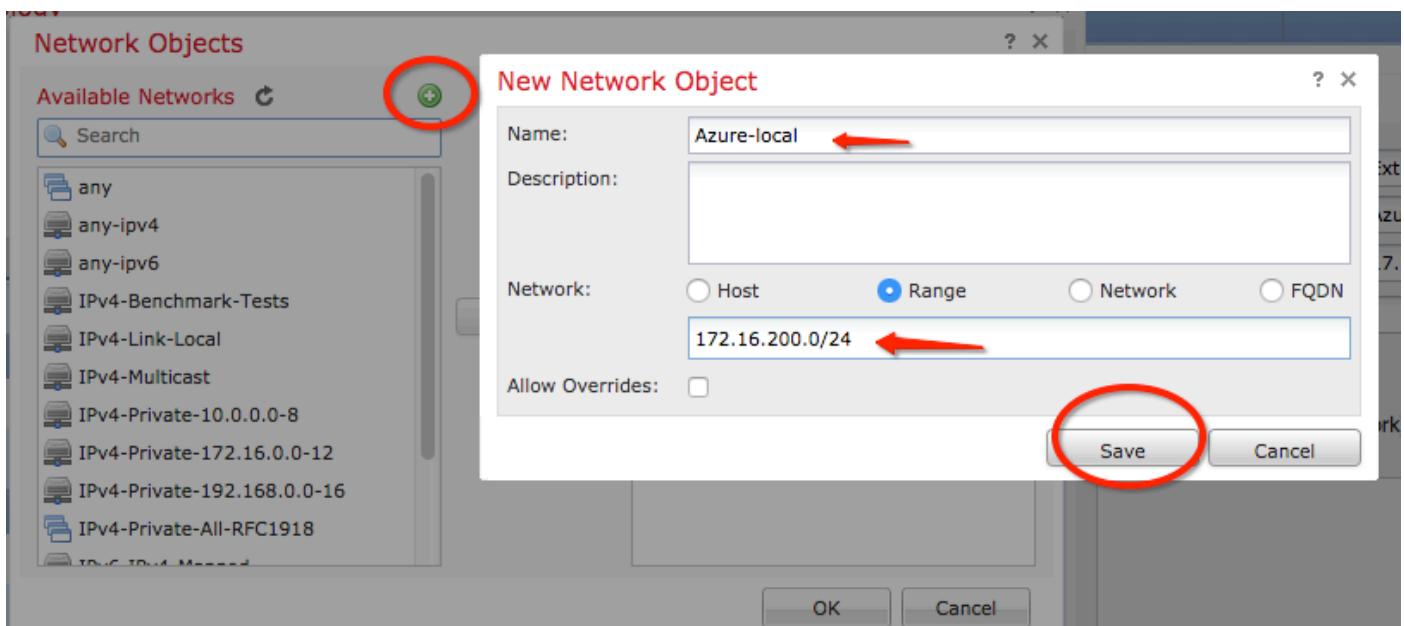
OK Cancel

ةـيـاهـنـ ةـطـقـنـ ، لـاثـمـلـا اـذـهـ يـفـ يـهـ يـتـلـاوـ ، B ةـدـقـعـلـا ةـيـاهـنـ ةـطـقـنـ فـيـرـعـتـبـ مـقـ . 15 ةـوـطـخـلـا دـدـحـمـ ةـفـاضـاـلـ green plus button قـوـفـ رـقـنـا مـثـ Node B ئـلـا لـقـتـنـا ، ةـذـفـانـ Create New VPN Topology ئـلـعـ ةـرـيـظـنـلـا ةـيـاهـنـلـا طـاقـنـ عـيـمـجـلـ ةـبـسـنـلـابـ Extranet دـيـدـحـتـ . ةـدـيـعـبـلـا ةـيـاهـنـلـا ةـطـقـنـ رـورـمـ ةـكـرـحـ اـهـسـفـنـ (FMC) ةـيـسـاسـأـلـا ةـرـادـإـلـا يـفـ مـكـحـتـلـا ةـدـحـوـ ةـطـسـاـوـبـ اـهـتـرـادـاـ مـتـتـ الـ يـتـلـاـ VPN ةـكـبـشـلـ بـصـاـخـلـا IP نـاـوـنـعـوـ (طـقـفـ اـيـلـجـمـ مـهـمـلـا) زـاـجـلـاـ مـسـاـ بـتـكـاـ A ةـدـقـعـلـاـ بـصـاـخـلـاـ .

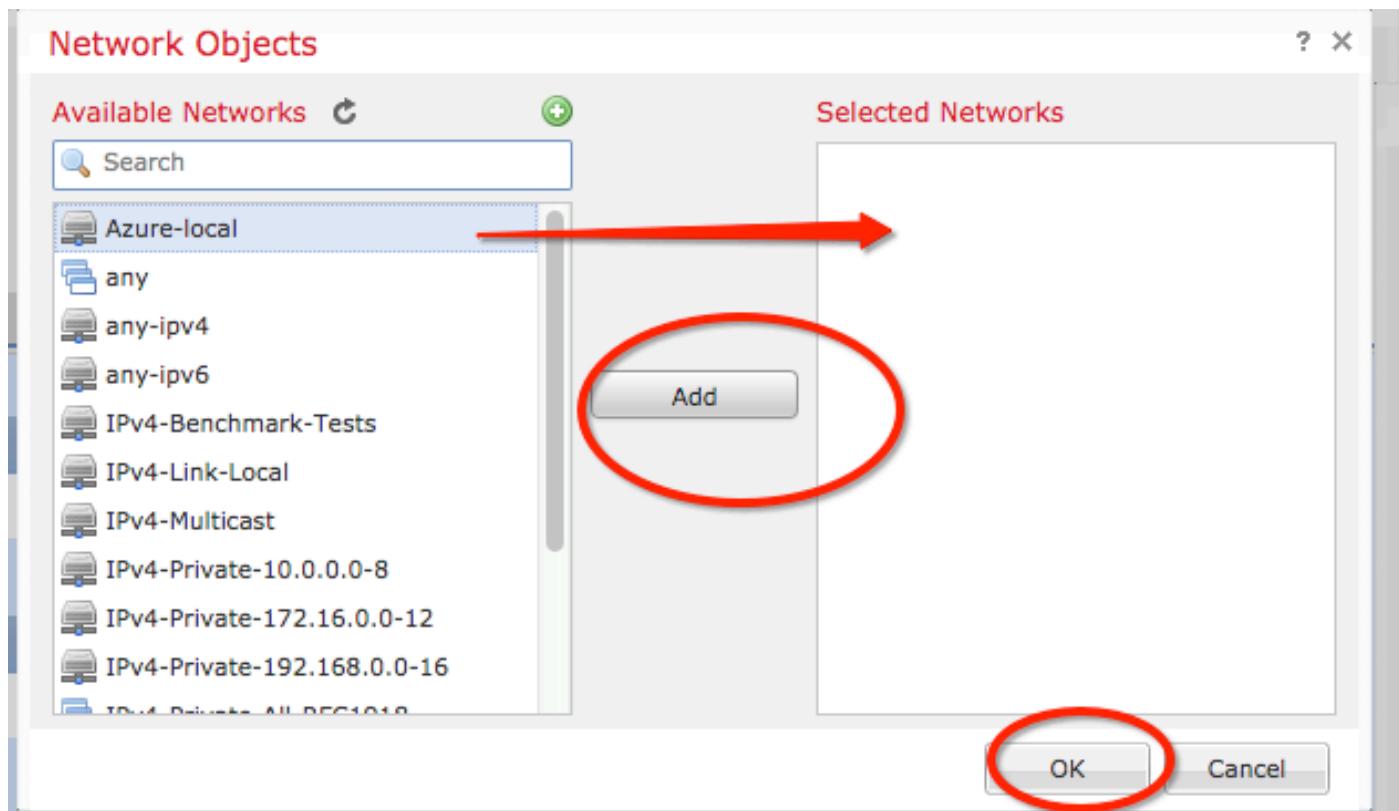


رقنا مث ىلإ لقتنا. دعب نع رورملأا ةكرح ددجم نئاك عاشناب مق. 16. ٥وطخلإا ديدج نئاك ةفاضل قوف green plus button.

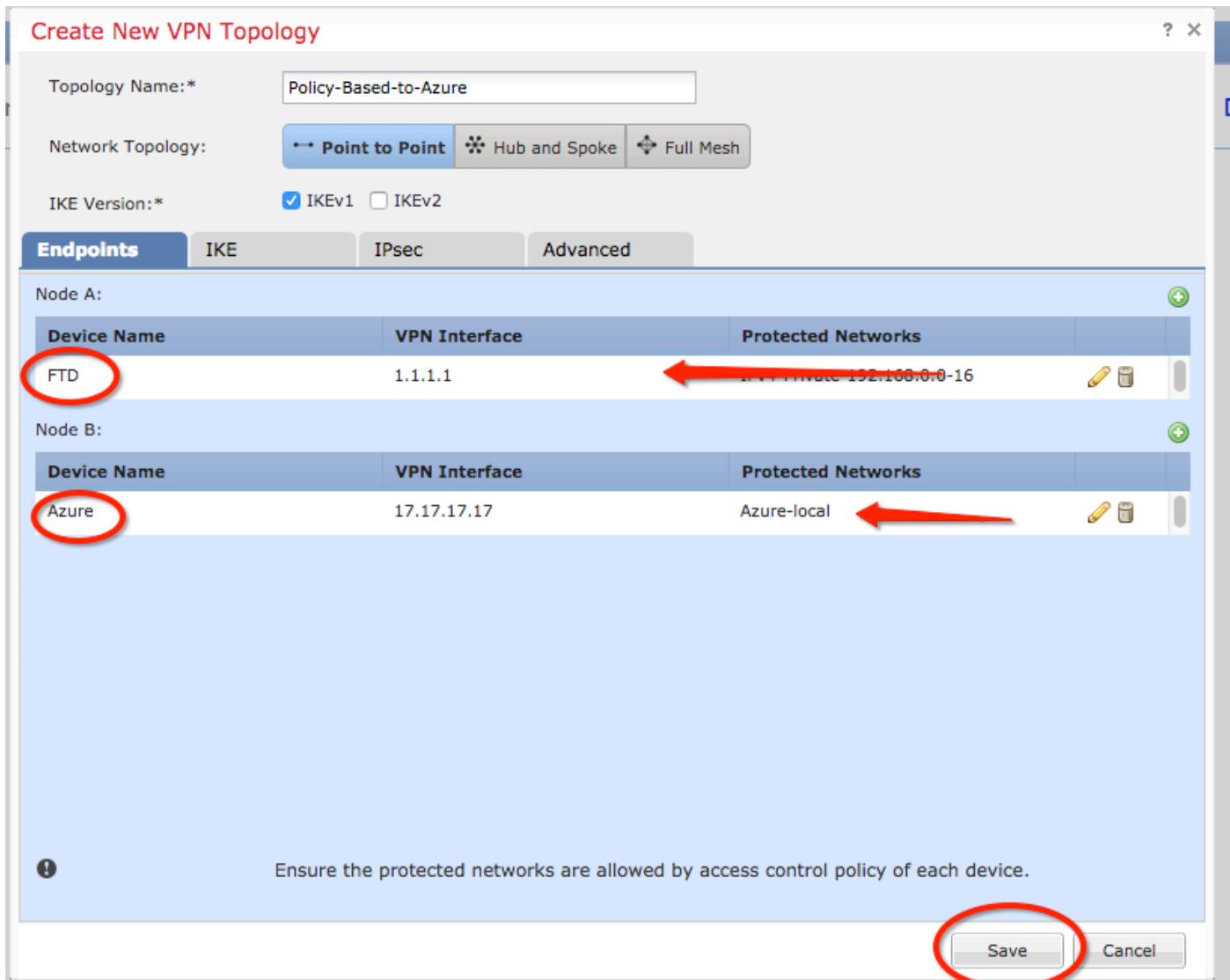
صنن اقفورتختا مث، نئاكلا مسا نيعتب مق New Network Object ىلع. ديدج نئاك عاشناب رقنا او FQDN/ةكبشلأا/قاطنلأا/فيضمملأا Save .



رقنا ىلإ ديدجلا ديعبلا نئاكلا فضاً، ةذفان Network Objects ىلإ ٥دوع. 18. ٥وطخلإا ٤٠٣ طقق طوع طقمم رقنا Add Endpoint ىلع OK .



ةكوح تاددح م عم دقعلا الک نآلا هتيؤر كنكمي يذلا راطإلا Create New VPN Topology ىلع 19. ووطخلا رقنا اهب ۆصاخلا ۆحیحصلا ۆيەحملاتاکبشلارورملا Save .



زاهج رتخا، رسیألا يولعلا عزجل ايف Deploy FMC، رقنا، تامولعم ٰحول يف 20 ٰوطخل FTD، رقناو Deploy .

زههجأب ٰبسنلاب لاحلا وه امك هسفن VPN نيوكت ودب، رمألا رطس ٰهجاوىل 21 ٰوطخل ASA.

ةسأيسلا ىلإ ٰدنتسملا رورملأا ٰكرح تاددحم عم راسملأا ىلإ دنتسم

اده عبتا، ريفشتلا طئارخ عم ASA ىلع عقوم ىلإ عقوب نم IKEv2 VPN نيوكت بجي هنأو راسملأا ىلإ ٰدنتسملا Azure VPN ٰكبسنلاب لامتكا نودب. راسملأا ىلإ دنتسملا Azure VPN مادختسا لالخ نم PowerShell UsePolicyBasedTrafficSelectors يف.

عوضوم نارتقالاب Microsoft UsePolicyBasedTrafficSelectors نيوكت فصي ريفشتلا طئارخ عم ASA لشفي، ٰوطخل اذه لامتكا نودب. راسملأا ىلإ دنتسملا Azure VPN نم اهلابقتسا مت يتلا رورملأا ٰكرح تاددحم يف قباطت مدع ببس لاصتا اعاشنا يف Azure.

ريفشتلا ٰطييرخ نيوكت تامولعم مادختساب لمالاب IKEv2 Cisco دنتسم عجار.

ٰيجراخل ٰهجاول ىلع IKEv2 نيكمت 1. ٰوطخل:

```
Cisco-ASA(config)#crypto ikev2 enable outside  
|IKEv2 نم ىلولأا ٩لحرمل جهـن ٩فاضـا 2. ٩وطخلـا
```

٩لحرملاب ٩صاخـلا ريفـشـتـلا ٩ـزـيمـعـمـ ضـرـاعـتـتـ تـامـوـلـعـمـ رـشـنـبـ Microsoftـ تـامـسـلـاـ رـيـفـوتـ مـتـيـ Azureـ لـبـقـ نـمـ ٩ـمـ دـخـتـسـمـلـاـ رـمـعـلـاـ تـامـسـ وـ ٩ـهـاـزـنـلـاـوـ IKEv2ـ نـمـ ىـلـوـلـاـ IKEv2ـ ٩ـمـسـ تـامـوـلـعـمـ .مـاعـ لـكـشـبـ رـفـوتـمـلـاـ اـذـهـ Microsoftـ دـنـتـسـمـ نـمـ دـهـجـ لـضـفـأـبـ ٩ـجـرـدـمـلـاـ Microsoftـ معـدـبـ لـصـتـاـ،ـ حـيـضـوـتـلـاـ نـمـ دـيـزـمـلـ .اـنـهـ تـاصـرـاعـتـلـاـ رـهـظـتــ يـتـلـاـ Microsoftـ Azureـ.

```
Cisco-ASA(config)#crypto ikev2 policy 1  
Cisco-ASA(config-ikev2-policy)#encryption aes  
Cisco-ASA(config-ikev2-policy)#integrity sha  
Cisco-ASA(config-ikev2-policy)#group 2  
Cisco-ASA(config-ikev2-policy)#lifetime seconds 28800
```

ريـظـنـلـلـ IPـ نـاـونـعـ نـيـوـكـتـبـ مـقـ وـ IPsecـ تـامـسـ تـحـتـ قـافـنـأـ ٩ـعـوـمـجـمـ عـاـشـنـإـبـ مـقـ 3. ٩ـوطـخـلـاـ

تـاـوـنـقـ عـاـشـنـإـاـوـ اـهـرـيـفـشـتـ مـتـيـسـ يـتـلـاـ رـوـرـمـلـاـ ٩ـكـرـحـ دـدـحـتـ لـوـصـ لـوـصـ ٩ـمـئـاـقـ عـاـشـنـإـبـ مـقـ 4. ٩ـوطـخـلـاـ
هـيـلـعـ لـوـصـحـلـاـ مـتـيـ يـذـلـاـ قـفـنـلـاـ نـمـ رـوـرـمـلـاـ ٩ـكـرـحـ يـهـ ٩ـحـلـصـمـلـاـ رـوـرـمـ ٩ـكـرـحـ،ـ لـاـثـمـلـاـ اـذـهـ يـفـ .ـاـهـلـ
تـنـاـكـ اـذـ ٩ـدـدـعـتـمـ تـالـاـخـداـ ٩ـلـعـ يـوـتـحـيـ نـأـ نـكـمـيـوـ 10.2.2.0ـ ٩ـلـعـ 10.1.1.0ـ ٩ـعـرـفـلـاـ ٩ـكـبـشـلـاـ نـمـ
عـقـاـوـمـلـاـ نـيـبـ ٩ـكـرـشـمـ ٩ـدـدـعـتـمـ ٩ـعـرـفـ تـاـكـبـشـ كـاـنـهـ.

تـاـيـواـحـكـ لـمـعـتـ تـاـنـيـاـكـ تـاـعـوـمـجـمـ وـأـ تـاـنـيـاـكـ عـاـشـنـإـاـكـ ،ـثـدـحـأـلـاـ تـاـرـادـصـإـاـوـ 8.4ـ تـاـرـادـصـإـاـيـفـ
عـاـشـنـإـبـ مـقـ .ـ٩ـدـدـعـتـمـ تـاـنـيـاـكـ وـأـ فـيـضـمـلـلـ IPـ نـيـوـانـعـ وـأـ ٩ـيـعـرـفـلـاـ تـاـكـبـشـلـاـ وـأـ تـاـكـبـشـلـلـ
مـئـاـوـقـ نـمـ لـكـلـ اـمـهـاـدـخـتـسـاـوـ ٩ـدـيـعـبـلـاـوـ ٩ـيـلـحـمـلـاـ ٩ـيـعـرـفـلـاـ تـاـكـبـشـلـاـ ٩ـلـعـ نـاـيـوـتـحـيـ نـيـنـيـاـكـ
تـاـرـابـعـوـرـيـفـشـتـلـلـ (ACL)ـ لـوـصـوـلـاـ يـفـ مـكـحـتـلـاـ NATـ .ـ

```
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
```

نـيـوـكـتـ عـضـوـيـفـ نـاـمـأـلـاـ تـاـمـلـعـمـ دـدـحـ |IKEv2ـ نـمـ 2ـ ٩ـلـحـرـمـلـلـ IPsecـ حـرـتـقـمـ ٩ـفـاضـاـ 5. ٩ـوطـخـلـاـ
رـيـفـشـتـ ٩ـلـعـ يـوـتـحـيـ الـ يـذـلـاـ IPsecـ لـ تـنـرـتـنـإـاـ لـوـكـوـتـوـرـبـ حـرـتـقـمـ:

AES-256 | aes-gcm | AES | 3des | des | ZARTEL | ZARTEL AES-192 | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | esp {md5 | sha-1 | SHA-256 | SHA-384 | SHA-512 | غراف}

ةصالخا ريفشتلا او لماكتلا تامس عم ضراعت تامولع رشنب Microsoft تماق: **ظحالم**
 ئجردملا تامسلا ريفوت متى لبقي نم ۆمەختسملا Azure نم ئيناثلا ۆلحرملاب
 ۆمس تامولع 2 ۆلحرملار **ماع لكشب رفوتمل اذه Microsoft دنتسم** نم دەج لصفاپ
 IPSec Microsoft نم Microsoft Azure نم ديزمل **انه تاضراعتلارهظت** يتللا معدب لصتا، حيضوتلا نم 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
```

ىلع يوتحت يتللاو، ئيجراخلا ۆھجاولا ىلع اھقيبطتو ريفشت ۆطيرخ نيوكتب مق. 6. ۆوطخلالا:

ريظنلل IP ناونع.

ةدىافلا رورم ۆكرح ىلع يوتحت يتللا ۆددحملار لوصولالا ۆمىاپ:

2 ۆلحرملار IKEv2 IPSec حرتقىم:

ين اوثلاب IPSec نم 2 ۆلحرملاءاقب ۆدم.

حيتافم نم ديدج جوز ئاشنالا يدؤي امم، (PFS) ئيلاتملار ھيچوتلا ۆداعا ئيرسل يرايتخا دادعى Diffie-Hellman PFS نم نىبناجلا الك نىكمت بجي) تانايبلار ئاماحل اهمادختسالا متي يتللا 2 ۆلحرملاروهظ لبقي

PFS تامسو IPSec ب ئصالخا 2 ۆلحرملاءاقب ۆدم عم ضراعت تامولع رشنب Microsoft تماق.

ماع لكشب رفوتمل اذه Microsoft دنتسم

حىضوتلا نم ديزمل **انه تاضراعتلارهظت** يتللا IPSec نم Microsoft تامولع 2 ۆلحرملار Microsoft Azure.

```
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
```

ئانىتتسا ۆدعاق ئاشنالا. ۆدعاق nat رخآ يألى رورم ۆكرح VPN لار عضخي ال نأتنمض. 8. ۆوطخلالا 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
```

تانىاك تاعومجم ئاشنالا كيلىع بجي، ۆددعتم ۆيعرف تاكبىش مادختسالا دنۇع: **ظحالم**
 ۆدعاق يف اهلامعتسا او ۆھجولار دىصملل ۆيعرفلا تاكبىشلا عيمج مادختساب NAT.

```
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
```

ةحصـلـا نـم قـقـحتـلـا

قفـن ةـئـيـهـتـبـ اـوـبـوـ اـوـسـ دـحـ لـيـكـشـتـلـاـ تـنـأـ مـتـيـ بـقـعـ
VPNـ:ـ رـمـأـ اـذـ عـمـ حـيـحـصـ لـكـشـبـ يـنـبـيـ قـفـنـلـاـ نـأـ تـقـقـدـ عـيـطـتـسـيـ تـنـأـ.

ىـلـوـأـلـا ـقـلـحـرـمـلـا

ىـلـوـأـلـا ـقـلـحـرـمـلـاـ نـامـاـ نـارـتـقـاـ ءـاشـنـاـ نـمـ قـقـحتـ:

IKEv2

اـيـلـحـمـلـاـ ةـيـجـرـاخـلـاـ ةـهـجـاـوـلـاـ نـمـ هـؤـاشـنـاـ مـتـ يـذـلـاـ IKEv2 SAـ ضـرـعـ مـتـيـ ،ـ كـلـذـ دـعـبـ
لـ تـيـنـبـ حـيـحـصـ SAـ عـرـفـ اـضـيـأـ كـانـهـ 192.168.2.2ـ IPـ 500ـ UDPـ ڈـيـعـبـلـاـ ةـهـجـوـلـاـ ىـلـاـ رـبـعـ ـقـفـدـتـيـ نـأـ رـوـرـمـ ةـكـرـحـ رـفـشـيـ.

```
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	

عـمـ رـيـظـنـلـ ئـدـابـكـ ASAـ مـادـخـتـسـابـ هـؤـاشـنـاـ مـتـ يـذـلـاـ IKEv1 SAـ ضـرـعـ مـتـيـ ،ـ اـنـهـ ئـيـنـاـثـ 86388ـ نـمـ ئـاقـبـ ةـرـتـفـ.

```
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
```

ةـيـنـاـثـلـاـ ـقـلـحـرـمـلـاـ

IPSec مادختساپ هواشنا مت دق 2 ةلحرملل نامأ نارتقا نأ نم ققحتل [peer-ip] .

```
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 0x00000001F

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
```

ظقون تيبيثت مت .عاطخأ نود IPSec SA رباع مزح عبأ مالتسا متى و مزح عبأ لاسرا متى عقوتم وه امك SA SPI 0x8E7A2E12 ع SPI 0x9B60EDC5 ع م دراو ةدحاو لوصو .

Cisco-ASA#show vpn-sessiondb 121

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

رابع ۋە مەلۇتىسىملاو ۋە لىسرمىلا تانايىبلا تادادع راھ ئەنلا و Tx: Bytes Rx: تىابلا تادادع.

اھالىچىسىملاو ۋە مەلۇتىسىملا

صاخ Azure لى دىم يىلخاد نراقلى ىلۇغ ASA ب روئىم ۋە كەرەت تەملىتسا نأ تىققىد. 1. ۋە طۆخلى طاقىتلار ئىۋەتكەرلىكىمەتلىرىنىڭ ئەپتەخانى ئەپتەخانىنىڭ كەنگەمىي، راپاتخالىل. ۋە كېش ئەپتەخانىنىڭ قىقەتلىل ASA ىلۇغدا ئەپتەخانىنىڭ قىقەتلىل:

show capture [cap-name] [if-name] [capture-type] [src-ip] [src-mask] [dest-ip] [dest-mask]
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

ۋە كەرەت تەملىتسىي/لىسرىي و تىپنىڭ حىچىسىملا لى كەلذ دىعە، Azure نم روئىم ۋە كەرەت تىأر نا روئىم.

ىلۇغدا حىچىسىملا لىسرمىلا ھىجوت نم قىقەتلىق، ۋە دوجوم رىغ روئىم ۋە كەرەت تەملىتسىي ASA.

قىقەتلىق عباىف، Azure نم درىلا روئىم ۋە كەرەت دوجوم مەتى مل نكىلۇردىمىلما روئىم ۋە كەرەت ضرع مەت اذىم بېسىلە نام.

2. ۋە طۆخلى طاقىتلار ئىلۇغدا ASA ىلۇغدا حىچىسىملا لىسرمىلا روئىم ۋە كەرەت تەملىتسىي ASA لى VPN:

ىدىص بىلەت ئەكاحىملە:

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

انە مۆزىلە عېتتىل ئەلماكىلا مادختىسىلا تاداشىرا ىلۇغ روئىتەلە ئەن كەنگەمىي:

<https://community.cisco.com/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 لـ NAT نـم اـم تـقـقـدـ (ـمـجـرـتـ يـأـ قـبـطـ اـلـ) رـوـرـمـاـ ةـكـرـحـ يـفـعـيـ NAT نـأـ ظـحـاـ رـوـرـمـ ةـكـرـحـ.

قىبلىت مەتى ئىچىرىنىڭ داملا ئەھجىلاردا نۇكىت نا بىچى - حىيەنلىك output-interface نىم اپتىأ قىقىت ئەپرەتلىق فەنلاردا ئەھجىلاردا رېفېشتلە ئەطىپلە.

لوصول اقتصاد روهظ مدع نم دکأت

لعلاب قفنلا عاشن ام ، **ENCRYPT: ALLOW** (VPN) ةيرهاظلا ةصاخلا ةكبشلا ةلحرم ترهظ اذا نيمضتلات ايالمع عم اتبثم IPSec SA ئيور كنكمي و.

2.1. اذى **ALLOW** رهظت يف قيّبطة، **Packet-tracer** ووطخلا.

show crypto ipsec sa .

نم ۋەرۋىشىملا مۇھىلە لاسرا نم قىقىحتىلىل ئېجراخىلا ئەجىملا ئىلە طاقىتلا ئارچا كىنكمىي ASA نم ۋەرۋىشىملا تاباچىتسالا لابقىتسا او Azure.

2.2. ةوطخل اذى ENCRYPT:DROP رهظت يف قىبطة Packet-tracer.

قفنلا بـلـجـتـ اـمـ دـنـ عـ عـ قـ وـ تـ مـ ظـ لـ اـ حـ هـ ذـهـ .ضـ وـ اـ فـ تـ لـاـ دـيـ قـ هـنـ كـلـ وـ دـعـ بـ VPNـ قـ فـ نـ عـ اـشـ نـ اـ مـ تـ يـ مـ ثـ وـ دـحـ نـ اـكـمـ دـيـ دـحـ تـ وـ قـ فـنـ لـاـ ضـ وـ اـ فـ تـ ةـ يـ لـمـ عـ ضـ رـ عـ لـ اـ طـ اـخـ الـاـ حـيـ حـصـتـ لـ يـ غـ شـ تـ بـ مـ قـ .ةـ رـمـ لـ وـ اـلـ كـلـ ذـ ثـ دـحـ اـذـ اـمـ وـ لـ شـ فـ

ةيلمعلا ءانثأ ةلص تاذ عاطخأ روھظ مدع نم و KE نم حيحصل رادصإا ليغشت نم ققحت ،الوا ةعئاشلا:

```
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.

ةكرح طاقس اينعي اذهف، VPN رورم ةكرح عدب دنع عئاش ءاطخأ حي حصت جارخا يأ رهظي مل اذا ئلع crypto ikev1/ikev2 نيكمت مدع وأ ريفشتلا ةيملمع ليل ا لصت نأ لبقب تانايبلرا رورم مزحللا طاقس ات ايملعم وري فشتلا نويوكت نم نويترم ققحت. عبرملا

IKEv1

انه هلیلحت و KEV1 ل مکلا ااطخألا حیحصت ءارجا یلع روش علا نكمی

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

IKEv2

انه هلیحت و ۷۰ ل لمکلا اطخالا حی حصت عارجا یل ع روتعلا نکمی.

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

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

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