

نم راسم الیلا ةدنتسم ال VPN ةكبش نیوكت FTD و ASA نیب عقوم الیلا عقوم

تایوتحمل

[ةمدقم](#)

[ةیساس الیلا تابلطتم](#)

[تابلطتم](#)

[ةمدختسم الیلا تانوكم](#)

[ةیساس ا تامولعم](#)

[نیوكت الیلا](#)

[ةكبش لیللی طیطخت الیلا مسر](#)

[تانیوكت الیلا](#)

[FMC مادختساب الیلا FTD یلع IPSec VPN نیوكت](#)

[FMC مادختساب الیلا FTD یلع عاچرتس الیلا ةهچاو نیوكت](#)

[ASA یلع IPSec VPN نیوكت](#)

[ASA یلع عاچرتس الیلا ةهچاو نیوكت](#)

[FMC مادختساب الیلا FTD یلع یطخت الیلا BGP نیوكت](#)

[ASA یلع یطخت الیلا BGP نیوكت](#)

[ةحصل الیلا نم ققحت الیلا](#)

[ةعرس الیلا قیاف لیسر الیلا چمانرب راطا یف چتاوون الیلا](#)

[دجوم الیلا عادالار شؤمب ةقلعت الیلا چتاوون الیلا](#)

[اهجالص او عاطح الیلا فاشكتس الیلا](#)

ةمدقم

نیب عقوم الیلا عقوم نم راسم الیلا دننسم VPN قفن نیوكت ةیفیك دننسم الیلا اذه فصی
ةیشغتك یكیمانی دلا هیچوتلل BGP عم FMC ةطساوب FTD و ASA.

ةیساس الیلا تابلطتم

تابلطتم

ةیلالات الیلا عیضاوم لابل ةفرعم كیدل نوكت ناب Cisco یصوت:

- IPsec عقوم الیلا عقوم نم VPN ةكبش لیسر الیلا مهفال
- FirePOWER دیدت دض عافدلا چمانرب یلع (BGP) ةیدودحلا ةرابعلا لوكوتورب تانیوكت (ASA) ةلدعما نامال ةزهچاو (FTD)
- FirePOWER (FMC) ةرادا زكرم ةبرجت

ةمدختسم الیلا تانوكم

- Cisco ASAv رادصل الیلا 9.20(2)2

- Cisco FMC، رادصلإل 7.4.1
- Cisco FTD، رادصلإل 7.4.1

ةصاخ ةي لمعم ةئي ب ي ف ةدوجومل ةزهجال نم دنتسمل اذه ي ف ةدراول تامولعمل عاشنإ مت تناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسمل اذه ي ف ةمدختسمل ةزهجال عيمج تأدب رما يأل لمتمحمل ريثأتلل كمهف نم دكأتف ،ليغشتل دي قكتكبش

ةيساسأ تامولعم

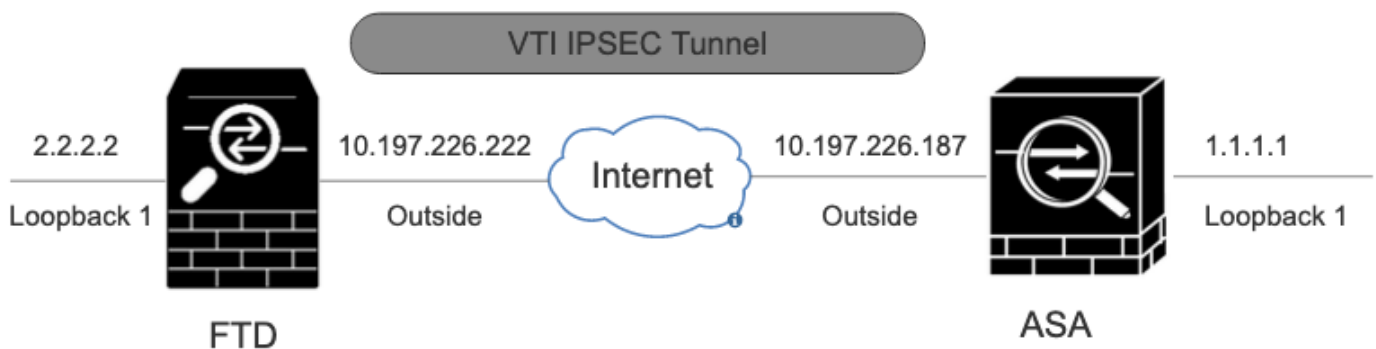
رورم ةكرح ديدحت ريفشتب راسمل إلى ةدنتسمل (VPN) ةيرهاظلا ةصاخلا ةكبشل حمست نم ادب رورملا ةكرح هي جوت مدختستو ،VPN قفن ربع اهلا سلا وأ مامت هلال ةريثمل تانايبلا وأ ريفشتلا ةطيرخ إلى ةدنتسمل VPN ةكبش ي ف لالحا وه امك ةسايسلا/لوصولا ةمئاق قفن لخدت رورم ةكرح ي أب حامسلل ريفشتلا لاجم نييغت مت .ةسايسلا إلى ةدنتسمل IPsec ل ةديعبلاو ةيلحمل تانايبلا رورم ةكرح تاددحم نييغت مت .IPsec 0.0.0.0/0.0.0.0 إلى ةعرفلا ةكبشل نع رظنلا ضغب IPsec قفن إلى اههيجوت متي رورم ةكرح ي ريفشت متي ةهوجل/ردصملل

BGP لوكوتورب عم (SVTI) ةتباثلا ةيرهاظلا قفنلا ةهجاو نيوكتب إلى ةدنتسمل اذه زكري ةيشغت كيكي مانيدلا هي جوتلل

نيوكتلا

SVTI قفن لالح نم BGP براقوت ضرعل FTD و ASA إلى بولطملا نيوكتلا مسقلا اذه فصلي IPsec.

ةكبشلل يطي طختلا مسرلا



ةكبشلل يطي طختلا مسرلا

تانايبلا

FMC مادختساب FTD إلى IPsec VPN نيوكت

Devices > VPN > Site To Site. إلى لقتنا 1. ةوطخل

Site to Site VPN+ قوف رقنا 2. ةوطخل



عقوم ىلإ عقوم نم VPN ةكبش

IKE Version. رتخأ Route Based (VTI). م ساب VPN ةكبش عونTopology Name رتخأ 3. ةوطخل

يحيضوتلا ضرعلا اذه لجأ نم

- ططخملا مسا : ASA-v-ITI
- رادصا IKE : IKEv2

Edit VPN Topology

Topology Name:*

ASA-v-ITI

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

☒ Point to Point ☐ Hub and Spoke ☐ Full Mesh

IKE Version:*

☐ IKEv1 ☒ IKEv2

VPN ايجولوط

رقنا) ةديج يرهاظ قفن ةهجاو ةفاضلا كنكمي .هنوكت مزلي يذلا قفنل Device رتخأ 4. ةوطخل
ةدوجوملا ةمئاقلا نم ةهجاو ديدحت وأ (زمزل+ىلع

Node A

Device:*

FTD|

Virtual Tunnel Interface:*

+

☐ Tunnel Source IP is Private [Edit VTI](#)☐ Send Local Identity to Peers

- + Add Backup VTI (optional)

► **Advanced Settings**

A عيانه لاطقة طقن عطق

Ok. New Virtual Tunnel Interface. تمام لعمل دوح. 5. ةوطخلا

يحيضوت لاضرع لاذه لجأ نم

- يتي ف-اس: مرسال
- ASA تنارتسك: عم VTI قفن: (يرايتخا) فصولا
- VTI-Zone: مألقة قطنملا
- 1: قفنفلا فرعم
- IP: 169.254.2.1/24 ناونع
- (يجراخ) GigabitEthernet0/1: قفنفلا ردصم
- IPsec: IPv4 قفن عضو

Add Virtual Tunnel Interface



General

Path Monitoring

Tunnel Type

☒ Static ☐ Dynamic

Name:*

ASAv-VTI

☒ Enabled

Description:

VTI Tunnel with Extranet ASA

Security Zone:

VTI-Zone

Priority:

0

(0 - 65535)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VT.

Tunnel ID:*

3

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/1 (Outside)

10.197.226.222

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

☒ IPv4 ☐ IPv6

IP Address:*

☒ Configure IP

169.254.2.1/24

☐ Borrow IP (IP unnumbered)

Loopback1 (loopback)



Cancel

OK

هؤاشن ا مت دق ديدجل VTI نأ اى اري شم قث بنم الم قوف رقن 6.0K ةوطخل

Virtual Tunnel Interface Added

VTI has been created successfully.
Please go to the Device > Interfaces
page to delete/update the VTI.

OK

تامول عمل اري فوتب مق Virtual Tunnel Interface تحت VTI وأ VTI newly created ل ترتخأ 7. ةوطخل
(ريظنل زاهج يه يتلوا) ب ةدق لل

يحضوتل ضرعل اذه لجا نم

- تنارتسك ا: لالتل لاثم ل ي ف
- زاهجل مسا: ASAv-Peer
- ةياهنل ةطقنل IP ناونع: 10.197.226.187

Node A

Device:*
 FTD

Virtual Tunnel Interface:*
 ASAv-VTI (IP: 169.254.2.1)

Tunnel Source: Outside (IP: 10.197.226.222) [Edit VTI](#)

☐ Tunnel Source IP is Private

☐ Send Local Identity to Peers

[+ Add Backup VTI \(optional\)](#)

Additional Configuration ⓘ

Route traffic to the VTI : [Routing Policy](#)

Permit VPN traffic : [AC Policy](#)

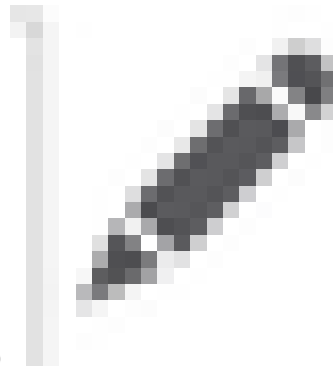
Node B

Device:*
 Extranet

Device Name*:
 ASAv-Peer

Endpoint IP Address*:
 10.197.226.187

B ياهنل ةطقن ةدقع



قوف رقنا IKE بيوبتل ةمالع ىل لقتنا 8 ةوطخل ةمالع Policy راوجب دوجومل رزل+ قوف رقنل وأ Policy اق بس م فرعم م ادختس رايتخا كنكمي . ديدج دحاو عاشنل بيوبتل

ددج و جهنل ل Name ري فوتب مق (. ةديج IKEv2 ةسايس عاشنل اب تمق اذا ، يرايتخا) 9 ةوطخل Save. رقنا جهنل ا ي ف هم ادختس م تيس يذل Algorithms جهنل

يحيضوتل ضرعلا اذه لجأ نم

- م سالا : ASAv-IKEv2-policy
- 256-يس هي : لم اكلتلا تاي م زراوخ
- 256-س هي : ري فشتلا تاي م زراوخ
- 256-يس هي : PRF تاي م زراوخ
- Diffie-Hellman: 14 ةعومجم

Edit IKEv2 Policy



Name:*

ASAv-IKEv2-Policy

Description:

Priority: (1-65535)

1

Lifetime: seconds (120-2147483647)

86400

Available Algorithms

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

MD5

SHA

SHA512

SHA256

SHA384

NULL

Add

Selected Algorithms

SHA256



Cancel

Save

IKEv2-Policy

مادختسإ م ت اذإ Authentication Type. دجوي يذلاPolicy وأ اتي دحPolicy هؤاشنإ م ت يذلا رتخأ. 10 ةوطخل
عبرم ال KeyConfirm Key يف حاتفم ال لخدأف، اقبس م كرتشم يودي حاتفم

يحيضوتال ضرعلا اذه لجأ نم

- اساي سل: ASAv-IKEv2-Policy
- اقبس م كرتشم يودي حاتفم: ةقداصل م عون

IKEv2 Settings

Policies:* ASAv-IKEv2-Policy

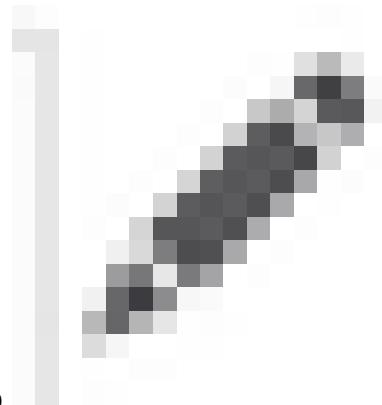
Authentication Type: Pre-shared Manual Key ▼

Key:*

Confirm Key:*

☐ Enforce hex-based pre-shared key only

ةقداصملا



رقننلا .بېوېتلا ةمالع IPsec لىلى لقتنا . 11 ةوطخلال
رقنا .ديج حرتقم ءاشنن و اق بسم فرعلم ال "IKEv2 ل IPsec حرتقم" مادختسا رايتخا نكمي
بېوېتلا ةمالع IPsec Proposal راوچب دوجوملا رزل+قوف

ضرعلا ددحو حرتقم لName لخدأ .(ديج IPsec IKEv2 حارتقا ءاشناب تمق اذا ،يرايتخا) . 12 ةوطخلال
Save .رقنا .ضرعلا يف همادختسا متيس Algorithms يذلا

يحيضوتلا ضرعلا اذه لجأ نم

- مسالال : ASAv-IPSec-Policy
- 256-يس هي : ESP ةئجت
- 256-سإ هي : ESP ريفشت

New IKEv2 IPsec Proposal



Name:*

ASAv-IPSec-Policy

Description:

ESP Hash

ESP Encryption

Available Algorithms

SHA-512

SHA-384

SHA-256

SHA-1

MD5

NULL

Add

Selected Algorithms

SHA-256



Cancel

Save

IPsec IKEv2 Configuration

ةرفوتم لا تاحارتقالا ةمئاق نم دجوي يذلالProposal وأ ائيدح هؤاشنإ مت يذلالProposal رتخأ. 13 ةوطخلا
رقنأ OK.

IKEv2 IPsec Proposal



Available Transform Sets



Search

AES-256-SHA-256

AES-GCM

AES-SHA

ASAv-IPSec-Policy

DES_SHA-1

Umbrella-AES-GCM-256

Add

Selected Transform Sets

ASAv-IPSec-Policy



Cancel

OK

ليوحت ةومجم

IPsec Lifetime Duration and Lifetime Size. تادادعإالPerfect Forward Secrecy (يرايخأ). 14 ةوطخل

حيزضوتالضرعلا اذه لجأ نم

- 14 لود ةومجم :ةيلاثملا هيحوتلا ةداعإ ةيرس
- (يضا رتفالال) 28800 :يضا رتفالال رمعلا دم
- (يضا رتفالال) 4608000 :يضا رتفالال رمعلا مح

Endpoints IKE IPsec Advanced

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

tunnel_aes256_sha

ASAv-IPSec-Policy

☐ Enable Security Association (SA) Strength Enforcement

☒ Enable Perfect Forward Secrecy

Modulus Group: 14

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

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

ةيوت PFS

ةروصل هذه يف حضورم وه امك ،Saveرقنا .ةنوكمل تاداعإل نم ققحت 15 ةوطخل

Edit VPN Topology

Topology Name:*

ASA-vTI

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point Hub and Spoke Full Mesh

IKE Version:*

☐ IKEv1 ☒ IKEv2

Endpoints IKE IPsec Advanced

Node A

Device:*

FTD

Virtual Tunnel Interface:*

ASA-vTI (IP: 169.254.2.1)

Tunnel Source: Outside (IP: 10.197.226.222)Edit VTI

☐ Tunnel Source IP is Private

☐ Send Local Identity to Peers

[Add Backup VTI \(optional\)](#)

Additional Configuration ⓘ

Route traffic to the VTI : [Routing Policy](#)

Permit VPN traffic : [ACL Policy](#)

Node B

Device:*

Extranet

Device Name:*

ASA-Peer

Endpoint IP Address:*

10.197.226.187

Cancel Save

نيوكتل ظفح

FMC مادختساب FTD ىل عاچرتسال ةهجاو نيوكت

عاچرتسال نيوكت مزلي شيح زاهجلا ريرحتب مق .Devices > Device Management ىل لقتنا

Interfaces > Add Interfaces > Loopback Interface. ىل لقتنا 1 ةوطخل

Device

Routing

Interfaces

Inline Sets

DHCP

VTEP

All Interfaces

Virtual Tunnels

Search by name

Sync Device

Add Interfaces +
New Interface

Redundant Interface

Bridge Group Interface

Loopback Interface

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management/0	management	Physical				Disabled	Global	
GigabitEthernet/0	inside	Physical	Inside		10.197.224.227/23(Static)	Disabled	Global	

عاچرتسال ةهجاو ىل لقتنا

نراقلا نكمي و "1" id عاچرتسإ دوزي ،"loopback" مسإل 2 ةوطخ لخدي

Edit Loopback Interface



General

IPv4

IPv6

Name:

loopback

☒ Enabled

Loopback ID:*

1

(1-1024)

Description

Cancel

OK

عاجز تسالال ةهجاو نيكم ت

OK. قوف رقنا ،ةهجاو لل IP ناو نع نيوك تب مق 3. ةوطخلا

Edit Loopback Interface



General

IPv4

IPv6

IP Type:

Use Static IP

IP Address:

2.2.2.2/24

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

Cancel

OK

عاجز تسال الة هاول IP ناونع ريفوت

ASA ىل ع IPSec VPN ني وكت

!--- Configure IKEv2 Policy ---!

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

!--- Enable IKEv2 on the outside interface ---!

```
crypto ikev2 enable outside
```

!---Configure Tunnel-Group with pre-shared-key---!

```
tunnel-group 10.197.226.222 type ipsec-l2l
tunnel-group 10.197.226.222 ipsec-attributes
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
```

!--- Configure IPSec Policy ---!

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

!--- Configure IPSec Profile ---!

```
crypto ipsec profile ipsec_profile_for_FTD
set ikev2 ipsec-proposal FTD-ipsec-proposal
set pfs group14
```

!--- Configure VTI ---!

```
interface Tunnel1
nameif FTD-VTI
ip address 169.254.2.2 255.255.255.0
tunnel source interface outside
tunnel destination 10.197.226.222
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec_profile_for_FTD
```

!--- Configure the WAN routes ---!

```
route outside 0.0.0.0 0.0.0.0 10.197.226.1 1
```

ASA ىل عاچرت سالا ةهجاو نيوكت

```
interface Loopback1
nameif loopback
ip address 1.1.1.1 255.255.255.0
```

FMC مادختساب FTD ىل عيطخت ال BGP نيوكت

> Routing الى لقتنا مٲ، هب VTI قفن نيوكت مت يذلا زاهجل Edit | Device Management > Devices الى لقتنا
General Settings > BGP.

يف حضوم وه امك، هجوم ال فرعمو (AS) يتاذل ماظن ال مقرر نيوكتو BGP نيكم تب مق 1. ةوطخل

ةروصل هذه.

ASA و FTD نيزاهال نم لك ىلع هسفن وه مقرلا نوكي نأ مزلي امك

BGP في كراشم هجوم لك ديدحتل هجومل فرعم مادختسا متي

Device Routing Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EGRP

RP

Policy Based Routing

BGP

General

Enable BGP: ☒

AS Number*: 1000 (1-4294967295 or 1-65535:65535)

☐ Override BGP general settings router-id address:

Router ID: Manual

IP Address*: 10.1.1.1

General

Scanning Interval: 60

Number of AS numbers in AS_PATH attribute of received routes: None

Log Neighbor Changes: Yes

Use TCP path MTU discovery: Yes

Reset session upon fallover: Yes

Enforce the first AS is peer's AS for EGP routes: Yes

Use dot notation for AS number: No

Aggregate Timer: 30

Neighbor Timers

Keepalive Interval: 60

Hold time: 180

Min hold time: 0

Next Hop

Address tracking: Yes

Delay interval: 5

Graceful Restart (used in BGP peer relationship recovery mode)

Graceful Restart: No

Restart time: 120

Stalepath time: 180

Best Path Selection

Default local preference: 100

Allow comparing MED from different neighbors: No

Compare Router ID for identical EBGP paths: No

Pick the best-MED path among paths advertised by neighbor AS: No

Treat missing MED as the best preferred path: No

BGP نيوكتل لقتنا

FTD ىلع هنكمت و IPv4 BGP ىلى لقتنا 2. ةوطخل

Device Routing Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EGRP

RP

Policy Based Routing

BGP

General

Enable IPv4: ☒

AS Number: 1000

General Neighbor Add Aggregate Address Filtering Networks Redistribution Route Injection

Setting

Learned Route Map

Routes and Synchronization

Generate default routes: No

Summarize subnet routes into network level routes: No

Advertise inactive routes: Yes

Synchronize between BGP and IGP systems: No

Redistribute BGP into IGP (Use filtering to limit the number of prefixes that are redistributed): No

Administrative Route Distances

External: 20

Internal: 200

Local: 200

Forward Packets Over Multiple Paths

Number of Paths: 1

BGP number of paths: 1

BGP نكمت

نيكمت و راجك ASA VTI قفنب صاخال IP ناو نع فضا، بيوبتال ةمال Neighbor تحت 3. ةوطخل رواجمل

Device Routing Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EGRP

RP

Policy Based Routing

BGP

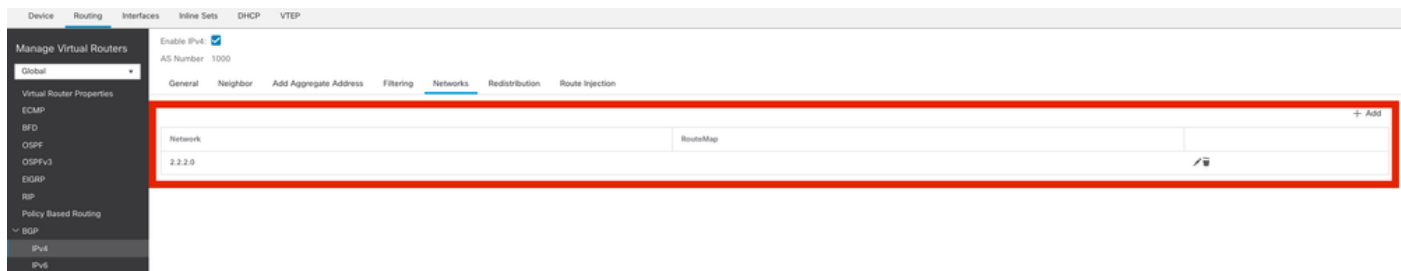
General Neighbor Add Aggregate Address Filtering Networks Redistribution Route Injection

Neighbor

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
169.254.2.2	1000	Enabled		

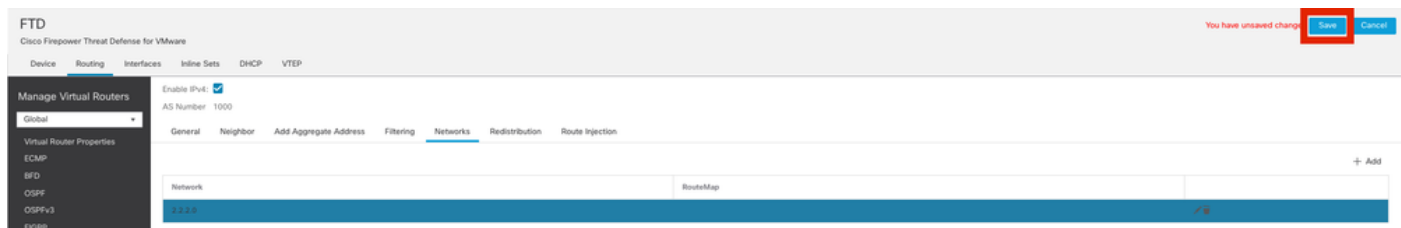
BGP راج ةفاضل

ىلى اجاتحت يتي BGP لالخنم اهنع نالعال ديترت يتي تالكبشال فضا، Networks تحت 4. ةوطخل loopback1، ةالجال هذه في، VTI قفن ربع رورمل



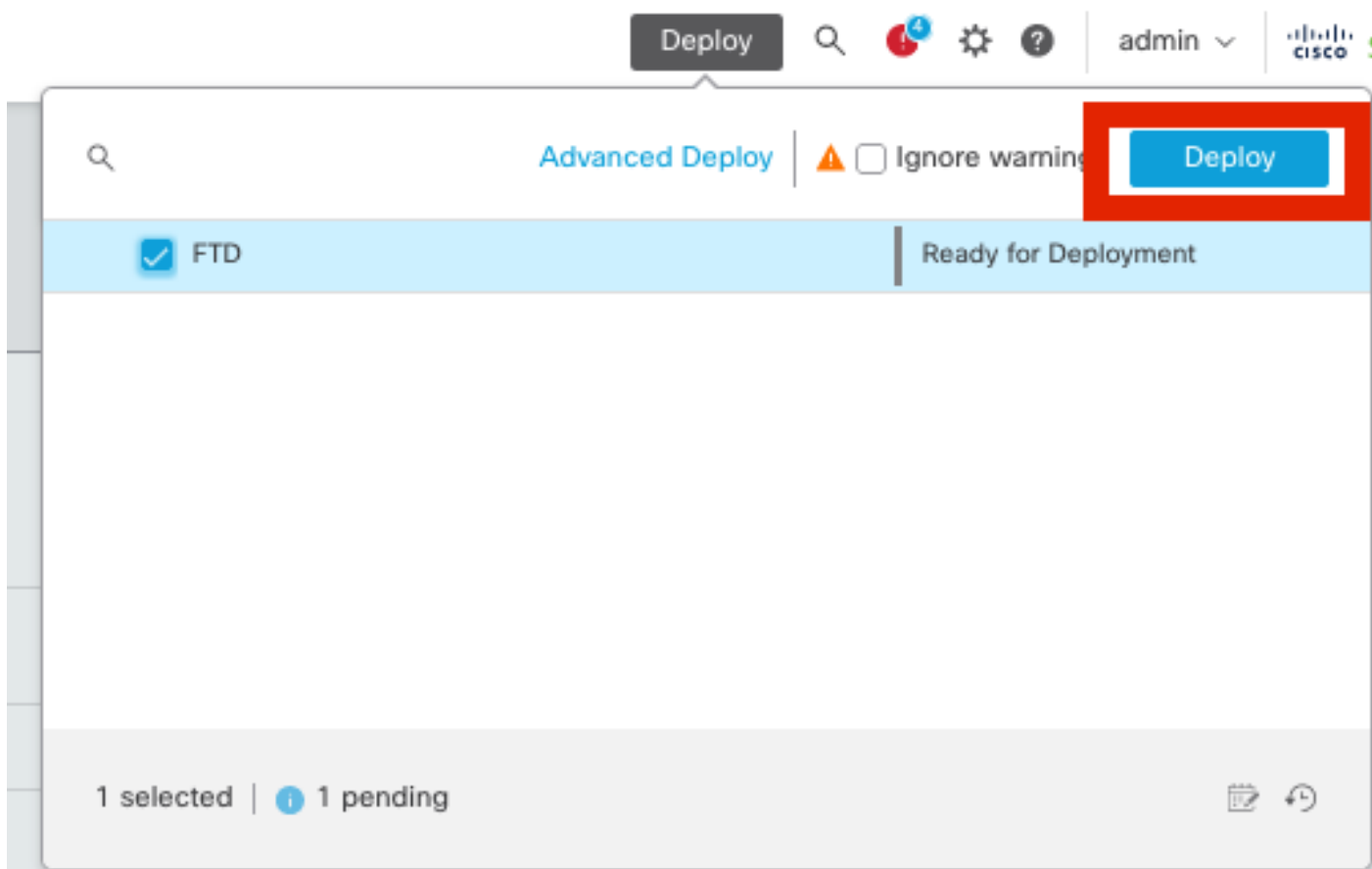
BGP تالکېش ټافاضا

قوحت .كتئيبل اقفو اهنويوكت كنكمي و ټرايخا ځړالا BGP تادادع ا عي مچ نوكت .5 ټوطلال قوف Saveرقن او نويوكتال نم .



BGP نويوكت ظفح

.تانويوكتال عي مچ رشن .6 ټوطلال



رشنال

ASA ځل عي طختال BGP نويوكت

```
router bgp 1000
bgp log-neighbor-changes
bgp router-id 10.1.1.2
address-family ipv4 unicast
neighbor 169.254.2.1 remote-as 1000
neighbor 169.254.2.1 transport path-mtu-discovery disable
neighbor 169.254.2.1 activate
network 1.1.1.0 mask 255.255.255.0
no auto-summary
no synchronization
exit-address-family
```

ةحصلال نم ققحتلا

ححص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا

ةعرسلال قئاف لاسلال جمانرب راطا يف جتاونلا

<#root>

#show crypto ikev2 sa

IKEv2 SAs:

Session-id:20, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote	fvr/fivr	Status	Role
666846307	10.197.226.222/500	10.197.226.187/500	Global/Global	READY	RESPOND

Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/1201 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0xa14edaf6/0x8540d49e

#show crypto ipsec sa

interface: ASAv-VTI

Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 10.197.226.222

Protected vrf (ivr): Global

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

current_peer: 10.197.226.187

#pkts encaps: 45, #pkts encrypt: 45, #pkts digest: 45

#pkts decaps: 44, #pkts decrypt: 44, #pkts verify: 44

#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

#send errors: 0, #recv errors: 0

local crypto endpt.: 10.197.226.222/500, remote crypto endpt.: 10.197.226.187/500
path mtu 1500, ipsec overhead 78(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 8540D49E
current inbound spi : A14EDAF6

inbound esp sas:

spi: 0xA14EDAF6 (2706299638)
SA State: active
transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={L2L, Tunnel, PFS Group 14, IKEv2, VTI, }
slot: 0, conn_id: 49, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4331517/27595)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
000001FFF 0xFFFFFFFF

outbound esp sas:

spi: 0x8540D49E (2235618462)
SA State: active
transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={L2L, Tunnel, PFS Group 14, IKEv2, VTI, }
slot: 0, conn_id: 49, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4101117/27595)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

#show bgp summary

BGP router identifier 10.1.1.1, local AS number 1000
BGP table version is 5, main routing table version 5
2 network entries using 400 bytes of memory
2 path entries using 160 bytes of memory
2/2 BGP path/bestpath attribute entries using 416 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 976 total bytes of memory
BGP activity 21/19 prefixes, 24/22 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down
169.254.2.2	4	1000	22	22	5		0	0

#show bgp neighbors

BGP neighbor is 169.254.2.2, vrf single_vf, remote AS 1000, internal link
BGP version 4, remote router ID 10.1.1.2
BGP state = Established, up for 00:19:49
Last read 00:01:04, last write 00:00:38, hold time is 180, keepalive interval is 60 seconds
Neighbor sessions:
1 active, is not multisession capable (disabled)
Neighbor capabilities:
Route refresh: advertised and received(new)
Four-octets ASN Capability: advertised and received
Address family IPv4 Unicast: advertised and received
Multisession Capability:

```

Message statistics:
  InQ depth is 0
  OutQ depth is 0

Sent      Rcvd
Opens      1      1
Notifications: 0      0
Updates:    2      2
Keepalives: 19     19
Route Refresh: 0      0
Total:      22     22
Default minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast
  Session: 169.254.2.2
  BGP table version 5, neighbor version 5/0
  Output queue size : 0
  Index 15
  15 update-group member

Sent      Rcvd
Prefix activity: ----
Prefixes Current: 1      1      (Consumes 80 bytes)
Prefixes Total: 1      1
Implicit Withdraw: 0      0
Explicit Withdraw: 0      0
Used as bestpath: n/a     1
Used as multipath: n/a     0

Outbound      Inbound
Local Policy Denied Prefixes: -----
Bestpath from this peer: 1      n/a
Invalid Path: 1      n/a
Total: 2      0
Number of NLRI's in the update sent: max 1, min 0

Address tracking is enabled, the RIB does have a route to 169.254.2.2
Connections established 7; dropped 6
Last reset 00:20:06, due to Peer closed the session of session 1
Transport(tcp) path-mtu-discovery is disabled
Graceful-Restart is disabled

```

#show route bgp

```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.197.226.1 to network 0.0.0.0

B      1.1.1.0 255.255.255.0 [200/0] via 169.254.2.2, 00:19:55

```

دحوم الءادل رشؤمب ةق لعت مل جتاو نل

<#root>

#show crypto ikev2 sa

IKEv2 SAs:

Session-id:7, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote	fvr/fivr/f	Status
442126361	10.197.226.187/500	10.197.226.222/500	Global/Global	READY
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK				
Life/Active Time: 86400/1200 sec				
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535				
remote selector 0.0.0.0/0 - 255.255.255.255/65535				
ESP spi in/out: 0x8540d49e/0xa14edaf6				

#show crypto ipsec sa

interface: FTD-VTI

Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 10.197.226.187

Protected vrf (ivr/f): Global
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 10.197.226.222

#pkts encaps: 44 #pkts encrypt: 44, #pkts digest: 44
#pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45
#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
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.197.226.187/500, remote crypto endpt.: 10.197.226.222/500
path mtu 1500, ipsec overhead 78(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: A14EDAF6
current inbound spi : 8540D49E

inbound esp sas:

spi: 0x8540D49E (2235618462)
SA State: active
transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={L2L, Tunnel, PFS Group 14, IKEv2, VTI, }
slot: 0, conn_id: 9, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4147198/27594)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x007FFFFF

outbound esp sas:

spi: 0xA14EDAF6 (2706299638)
SA State: active
transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={L2L, Tunnel, PFS Group 14, IKEv2, VTI, }
slot: 0, conn_id: 9, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (3916798/27594)

IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

#show bgp summary

BGP router identifier 10.1.1.2, local AS number 1000
BGP table version is 7, main routing table version 7
2 network entries using 400 bytes of memory
2 path entries using 160 bytes of memory
2/2 BGP path/bestpath attribute entries using 416 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 976 total bytes of memory
BGP activity 5/3 prefixes, 7/5 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/Pf
169.254.2.1	4	1000	22	22	7	0	0	00:19:42	1

#show bgp neighbors

BGP neighbor is 169.254.2.1, context single_vf, remote AS 1000, internal link
BGP version 4, remote router ID 10.1.1.1
BGP state = Established, up for 00:19:42
Last read 00:01:04, last write 00:00:38, hold time is 180, keepalive interval is 60 seconds
Neighbor sessions:
1 active, is not multiseession capable (disabled)

Neighbor capabilities:
Route refresh: advertised and received(new)
Four-octets ASN Capability: advertised and received
Address family IPv4 Unicast: advertised and received
Multiseession Capability:

Message statistics:

InQ depth is 0
OutQ depth is 0

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	2	2
Keepalives:	19	19
Route Refresh:	0	0
Total:	22	22

Default minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast

Session: 169.254.2.1
BGP table version 7, neighbor version 7/0
Output queue size : 0

Index 5

5 update-group member

	Sent	Rcvd	
Prefix activity:	----	----	
Prefixes Current:	1	1	(Consumes 80 bytes)
Prefixes Total:	1	1	
Implicit Withdraw:	0	0	
Explicit Withdraw:	0	0	
Used as bestpath:	n/a	1	
Used as multipath:	n/a	0	

	Outbound	Inbound
Local Policy Denied Prefixes:	-----	-----
Bestpath from this peer:	1	n/a
Invalid Path:	1	n/a
Total:	2	0

Number of NLRI in the update sent: max 1, min 0

Address tracking is enabled, the RIB does have a route to 169.254.2.1
Connections established 5; dropped 4
Last reset 00:20:06, due to Peer closed the session of session 1
Transport(tcp) path-mtu-discovery is disabled
Graceful-Restart is disabled

#show route bgp

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.197.226.1 to network 0.0.0.0

B 2.2.2.0 255.255.255.0 [200/0] via 169.254.2.1, 00:19:55

اهحال صاوا عا طخال فاشكتسا

اهحال صاوا نيوكتال عا طخال فاشكتسا ال اهمادختسا كنكمي تامولعم مسقلا اذه رفوي

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug ip bgp all
```

- ككيشال ةلومح وأةي محمل تاكبشال وأة IPv4 الى ةفاضال اب، طقف IPv4 تاهجاو معددي (IPv6 ل معد دجوي ال) ةي ره اظلال ةصاخلا

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا