

نم راسملاء لىا ةدنتسملاء VPN ٰكبس نيوكت نيب عقوم لىا FTD و ASA عم BGP عاطل

تاييوتحملاء

قمدقملا

[قيس اس الابل طتملا](#)

[تابل طتملا](#)

[قمدخت سملاءات انوكت ملأ](#)

[قيس اس ا تامولعم](#)

[نيوكتل](#)

[ٰكبس ليل طخت لام سيل](#)

[تانيوكتل](#)

[مادخت سلاب FTD مارع IPSec VPN نيوكت](#)

[مادخت سلاب FTD مارع عاجرت سلا قه جاو نيوكت](#)

[مادخت سلاب ASA مارع IPSec VPN نيوكت](#)

[مادخت سلاب ASA مارع عاجرت سلا قه جاو نيوكت](#)

[مادخت سلاب BGP مارع FTD مارع طخت ل](#)

[BGP نيوكت مارع طخت ل](#)

قحص لانم قرحتل

[قعرس لىا قىزاف لاس بالا جمانىرب راطا يف جت اون ل](#)

[دجوملا عادل ارش فمب ققل عتملا جت اون ل](#)

[اهحالص او عاطخ الافاش كتسا](#)

قمدقملا

نيب عقوم لىا عقوم نم راسملاء لىا دنتسم VPN قفن نيوكت ئيفيك دنتسملا اذه حضوي
ةرادا زكرم ئطساوب (FTD) FirePOWER (ASA) فيكىتلل لباقلالا ناما لازا
FirePOWER (FMC) يكيمانيدلا هيچوغلوكوتورب عم (BGP). ئيشغتك.

قيس اس الابل طتملا

تابل طتملا

قيس اس ا فرعون كيدل نوكوت نأب Cisco يصوت:

- عقوم لىا عقوم نم VPN ٰكبس ل يس اس ال مهفل
- عقوم لىا ع القوم نم IPsec و FTD و ASA تانىوكوت
- ع عم ئبرجت FMC

ةم دختس ملأ تانوكملأ

- Cisco ASA 9.2(2)2 رادص إلأ
- Cisco FMC ، 7.4.1 رادص إلأ
- Cisco FTD ، 7.4.1 رادص إلأ

ةصالح ةيلمعم ةئيب يف ةدوجملا ةزهجألا نم دنتسملا اذه يف ةدراولا تامولعملاءاشنامت تناك اذا . (يضرارت فا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجألا عيمج تأدبل رمأ يأ لمحملاريا ثأتلل كمهف نم داكتف ، ليغشتلا ديق كتكبش.

ةيساسأ تامولعم

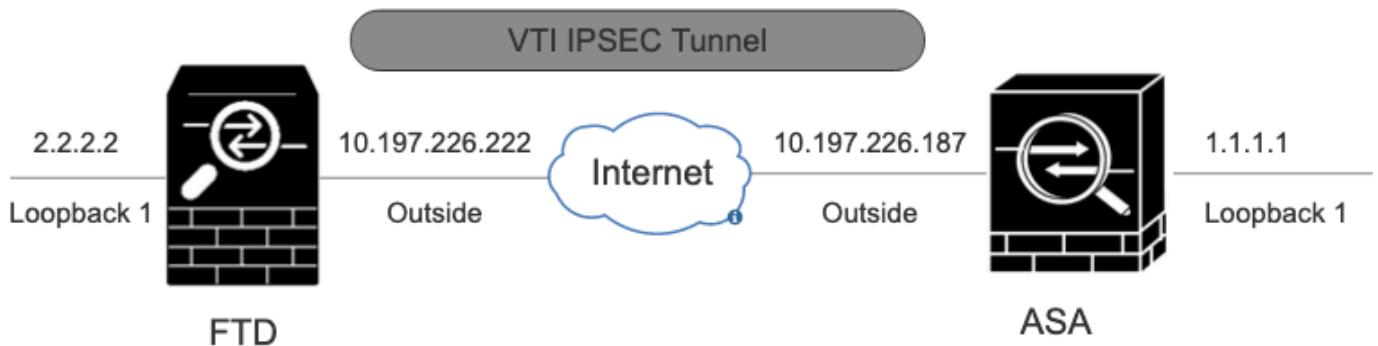
رورم ةكرح ديدجت ريفشت براسملأىلإ ةدنتسملأ (VPN) ةيرهاظلا ةصالحلا ةكبشلا حمسنتم الدب تانايبلا رورم ةكرح هيجوت مدخلتسن و ، VPN قفن رباع اهلأسرا وأ ، ةديفملا تانايبلا وأ ريفشتلا ةطيرخ ئلإ ةدنتسملأ VPN ةكبش يف لاحلا وه امك ةسايسلأا /لوصولا ةمئاق قفن لخدت رورم ةكرح يأب حامسلل ريفشتلا لاجم نيعت مت . ةسايسلأا ئلعل ةمئاق IPsec ئلعل 0.0.0.0/0.0.0.0 ل ةديعبلأاو ةيلحملاتانايبلا رورم ةكرح تاددم نيعت مت . ةيعرفلا ةكبشلا نع رظنلا ضغب قفن ئلإ اههيجوت مت ي رورم ةكرح يأ ريفشت متى ههجولأا /ردصلل.

لوكوتورب عم (SVTI) ةتباثلا ةيرهاظلا قفنلا ةهجاونيوكت ئلعل دنتسملا اذه زكري ةيشغتك يكيمانيدلا هيجوتل.

نيوكتلا

قفن لالخ نم BGP راوج ضرعل FTD و ASA ئلعل بولطملا نيوكتلا مسقلما اذه فصي IPsec.

ةكبشلل يطيطرختلا مسرا



ةكبشلل يطيطرختلا مسرا

تانايكوتلا

مادختسا ب FTD نيوكت IPSec VPN ئلعل

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

ووطخلا 2. رقنا + Site to Site VPN .



عقوم ئىلما عقوم نم ئىكبسن VPN

وطخلا 3. ريفوت ديدحت وون عون ئىكبسا بـ VPN ئىلما Route Based (VTI). IKE Version.

يحيصوتلا ضرعلا اذه لجأ نم:

اساسا مسالا: ASA v - VTI

رادصا IKE: IKEv2

Edit VPN Topology

Topology Name: *
ASA v - VTI

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:
 Point to Point Hub and Spoke Full Mesh

IKE Version: * IKEv1 IKEv2

ايچولوبط VPN

وطخلا 4. قيبلل قفنل ديفيل ديدحت او (زميلا + ئىلما رقنا) ئىدج ييرها ئاقلا ئاموملا دوجوملا فەنەن كەن كەمەي .

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](#)

ةياهنلا قطعن قدح A

رقنا New Virtual Tunnel Interface. Ok. ووطخل 5. مقتب ديدحت اتملعا.

لجم اذه ضرعلا صرعتلا يحيضوتلا:

ASA-VTI: مسالا

Extranet ASA (يرايتحا) فصوص vTI ع قفن: ASA

ةقطنم مقطنم: vTI-Zone

فرع فرنل: 1

نارونع IP: 169.254.2.1/24

(يجراخ) GigabitEthernet0/1: قفن ردصم

ضو ع قفن IPsec: IPv4

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

يەھا ئۆلە قەنۇلە ئەھجاو

تىقلىخ دىدج VTI لى نأ ركذىي قىثبىنملە ئىلۇ OK تىققىطقەت 6. ۋە ئۆطخىل.

Virtual Tunnel Interface Added

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

OK

يەھا ئۆلە قەنۇلە ئەھجاو ئەفاسىا تەمت

زاهج يەھ پەتلەو ب ۋە دىقىعىلىلى تامولۇمەلە رىفوتب مۇق. Virtual Tunnel Interface. تەختتى VTI newly created وۇ VTI تەرەت خا 7. ۋە ئۆطخىل (رىيظەنلە).

يەھىيىضۇتلىا ضىرعلى اذە لىجأ نەم:

تەنارتىس كە: زاهج لە

ماسە: زاهج لە ASAv-Peer

نەونۇن IP ئەنلە ئەطقىنلە: 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 (1)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

ةياهنلا ةطقون ةدع



قف رقنا بـ IKE. قوف رقنا ددحو جهـنـلـلـ Algorithms Name رـيـفـوـتـبـ مـقـ (ـدـيـدـجـ IKEv2ـ).ـ

ـدـيـدـجـ دـحـاوـ عـاـشـنـاـلـ بـيـوـبـتـلـاـ ةـمـالـعـ يـلـاـ لـقـتـنـاـ 8ـ.ـ وـطـخـلـاـ.

ـمـتـيـسـ يـذـلـاـ دـدـحـوـ جـهـنـلـلـ Algorithms Name رـيـفـوـتـبـ مـقـ (ـدـيـدـجـ IKEv2ـ).ـ

ـرـقـنـاـ جـهـنـلـاـ يـفـ هـمـادـخـتـسـاـ Save

ـيـحـيـضـوـتـلـاـ ضـرـعـلـاـ اـذـهـ لـجـأـ نـمـ:

ـمـسـالـاـ: ASAv-IKEv2-policy

ـلـمـاـكـتـلـاـ تـايـمـزـراـخـ: SHA-256

ـرـيـفـشـتـلـاـ تـايـمـزـراـخـ: AES-256

ـتـايـمـزـراـخـ PRF: SHA-256

ـمـوـجـمـعـةـ Diffie-Hellman: 14

Edit IKEv2 Policy



Name:*

ASAv-IKEv2-Policy

Description:

Priority: (1-65535)

1

Lifetime: seconds (120-2147483647)

86400

Available Algorithms		Selected Algorithms
Integrity Algorithms		
Encryption Algorithms		SHA256
PRF Algorithms		
Diffie-Hellman Group		
MD5		
SHA		
SHA512		
SHA256		
SHA384		
NULL		

IKEv2-Policy

Cancel Save

كرتشم يودي حاتفم مادختس ام اذا Policy لـ Authentication Type. دجاجاوي نأوي newly created Policy دده.

يعني حاتفم KeyConfirm Key، اقبسم لخداف.

اقبسم كرتشم يودي حاتفم: ASAว-IKEv2-Policy

اقبسم كرتشم يودي حاتفم: QoS ACL

IKEv2 Settings

Policies:*	<input type="text" value="ASAv-IKEv2-Policy"/>
Authentication Type:	<input type="text" value="Pre-shared Manual Key"/>
Key:*	<input type="text" value="....."/>
Confirm Key:*	<input type="text" value="....."/>
<input type="checkbox"/> Enforce hex-based pre-shared key only	

ةقداصملأا

قوف رقنلا راتخي نأ نكمي .بـيوبـتـلـا ةـمـالـع IPsec ىـلـا لـقـتـنـا .11 ةـوـطـخـلـا
ةـمـالـع IKEv2 IPsec Proposal رـاـجـب دـوـجـوـمـلـا رـزـلـا + قـوـفـ رـقـنـا .دـيـدـجـ حـرـتـقـمـ عـاـشـنـابـ تـمـقـ اـذـا ،ـيـرـايـتـخـاـ) .12 ةـوـطـخـلـا
بـيـوبـتـلـا .

متـيـس Algorithms يـذـلـا ضـرـعـلـا دـدـجـوـحـرـتـقـمـلـ Name لـخـدـأـ (ـدـيـدـجـ IKEv2 IPsec حـارـتـقـاـ عـاـشـنـابـ تـمـقـ اـذـا ،ـيـرـايـتـخـاـ) .12 ةـوـطـخـلـا
رقـنـاـ ضـرـعـلـاـ يـفـ هـمـادـخـتـسـاـ .ـضـرـعـلـاـ Saveـ

يـحـيـضـوـتـلـاـ ضـرـعـلـاـ اـذـهـ لـجـأـ نـمـ

مسـالـاـ: ASAv-IPSec-Policy

ةـئـزـجـتـ ESP: SHA-256

رىـفـشـتـ ESP: AES-256

New IKEv2 IPsec Proposal



Name:^{*}

Description:

Available Algorithms

ESP Hash

ESP Encryption

SHA-512

SHA-384

SHA-256

SHA-1

MD5

NULL

Add

Selected Algorithms

SHA-256



[Cancel](#)

[Save](#)

حروف مترقبة IKEv2-IPsec

OK. ورطخاً 13. Proposal Proposals تجارتقا نم دوجومل ارقنا. ورطخاً 13. OK.

IKEv2 IPsec Proposal



Available Transform Sets C +

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

لیوحت ڈعویٰ مجنم

نیوکتب مق. تادادعإا IPsec Lifetime Duration and Lifetime Size. رخآ (یرایتخا) 14 ڈوطخلہ Perfect Forward Secrecy.

یحیضوتلا ضرعلا اذہ لجأ نم:

14 تالماعملہ ڈعویٰ مجنم: ڈیلاثملہ ہیجوتلا ڈداعا ڈیرس

(یضارتفالا) 28800: رمعلا ڈدم

(یضارتفالا) 4608000: یضارتفالا رمعلا مجح

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)

ةئيھت PFS

ةروصلا هذه يف حضوم وە امك، رقنا، اهنيوكت مەت يىتلە تادادعەلە نەم ققحەت 15. ۋەطخەل.

Edit VPN Topology

Topology Name*: ASA4-VTI

Policy Based (Crypto Map) Route Based (VTI)

Network Topology: Point to Point

IKE Version: IKEv1 IKEv2

Endpoints [IKE](#) [IPsec](#) [Advanced](#)

Node A	Node B
Device: FTD	Device: Extranet
Virtual Tunnel Interface: ASA4-VTI (IP: 169.254.2.1)	Device Name: ASA4-Peer
Tunnel Source: Outside (IP: 10.197.226.222) Edit VTI	Endpoint IP Address: 10.197.226.187
<input type="checkbox"/> Tunnel Source IP is Private	
<input type="checkbox"/> Send Local Identity to Peers	

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

Additional Configuration:

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

Permit VPN traffic : [AC Policy](#)

[Cancel](#) [Save](#)

نېوكتلە ظفح

مادختىساب FTD ىلۇع عاجرتسىالا ۋەجاو نېوكت

عاجرتسىالا نېوكت مزلى ثىچ زاھىلە رىرەت بىمەق . Devices > Device Management

عاجرتسىالا ۋەجاو ىلە لىقتنى 1. ۋەطخەل

Device	Routing	Interfaces	Inline Sets	DHCP	VTEP	Search by name	Sync Device	Add Interface
		All Interfaces	Virtual Tunnels					Loopback Interface
		Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring Virtual Router

عاجرتسىالا ۋەجاو ىلە لىقتنى

2. ۋەطخەل "loopback" فرعەم رىفوت بىمەق، مسالا لىخدا.

Edit Loopback Interface



General

IPv4

IPv6

Name:

loopback

Enabled

Loopback ID:*

1

(1-1024)

Description

Cancel

OK

عاجرسسالا ڈھج او نیکمٹ

تقطق طقط ، نرافق لل ناون علا تلکش 3. ڈووط خل .

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

عاجرتسى الـ ڈھج اول IP ناونع ريفوت

نېوکت IPSec VPN ىلۇغ ASA

!---- 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
```

ىلע عاجرسالا ڈھج او نیوکت ASA

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

مادختس اب FTD ىلع يطختل ا BGP نیوکت FMC

ىلإ لقتنا مث ، بـ VTI قفن نیوکت مث یذلا راهجلا Devices > Device Management.Edit ىلإ Routing >General Settings > BGP.

ةروصلـا هـذـه يـف حـضـوم وـه اـمـك ، هـجـوـمـلـا فـرـعـمـوـ (AS) یـتـاذـلـا مـاظـنـلـا مـقـرـنـیـوـکـتـوـ BGP نـیـکـمـتـبـ مـقـ 1. ڈـوـطـخـلـا.

نـیـزـاـھـجـلـا نـمـ لـكـ ىـلـعـ مـسـفـنـ وـه مـقـرـلـا نـوـکـيـ نـأـ مـزـلـيـ اـمـكـ FTD وـ ASA.

يـف كـراـشـم هـجـومـ لـكـ دـيـدـحـتـلـ هـجـومـاـ فـرـعـمـ مـادـخـتـسـاـ مـتـيـ

Manage Virtual Routers

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

BGP

IPv4

IPv6

Static Route

Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary Filter

General Settings

BGP

Enable BGP:

AS Number*: 1000

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 failover: Yes

Enforce the first AS's peer's AS for EBGP 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

Restart time: 120

Stalepath time: 360

نـيـوكـتـلـ لـقـتـنـاـ BGP

ىـلـعـ هـنـيـكـمـتـ وـلـاـ لـقـتـنـاـ 2ـ ـوـطـخـلـاـ BGP > IPv4 BGP IPv4 FTD.

Manage Virtual Routers

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

BGP

IPv4

IPv6

Static Route

Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary Filter

Enable IPv4:

AS Number: 1000

General Neighbor Add Aggregate Address Filtering Networks Redistribution Route Injection

Setting

Learned Route Map

Administrative Route Distances

External: 20

Internal: 200

Local: 200

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 IBGP into IGP: No

(Use filtering to limit the number of prefixes that are redistributed)

Forward Packets Over Multiple Paths

Number of Paths: 1

IBGP number of paths: 1

نـيـكـمـتـ BGP

روـاجـمـلـاـ نـيـكـمـتـ وـرـاجـكـ VTIـ نـاـونـعـ فـضـأـ،ـبـيـوـبـتـلـاـ ـةـمـالـعـ تـحـتـ 3ـ ـوـطـخـلـاـ.

Manage Virtual Routers

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

BGP

IPv4

IPv6

General Neighbor Add Aggregate Address Filtering Networks Redistribution Route Injection

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

+ Add

رـاجـ ةـفـاضـلـاـ BGP

هـذـهـ يـفـ قـفـنـ رـبـعـ رـوـرـمـلـاـ ـلـاـ جـاتـحـتـ يـتـلـاـ BGPـ لـاـلـخـ نـمـ اـهـنـعـ نـاـلـعـاـلـاـ دـيـرـتـ يـتـلـاـ تـاـكـبـشـلـاـ فـضـأـ،ـبـيـوـبـتـلـاـ ـةـمـالـعـ تـحـتـ 4ـ ـوـطـخـلـاـ Networksـ،ـوـلـاـ loopback1ـ.

Manage Virtual Routers

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

BGP

IPv4

IPv6

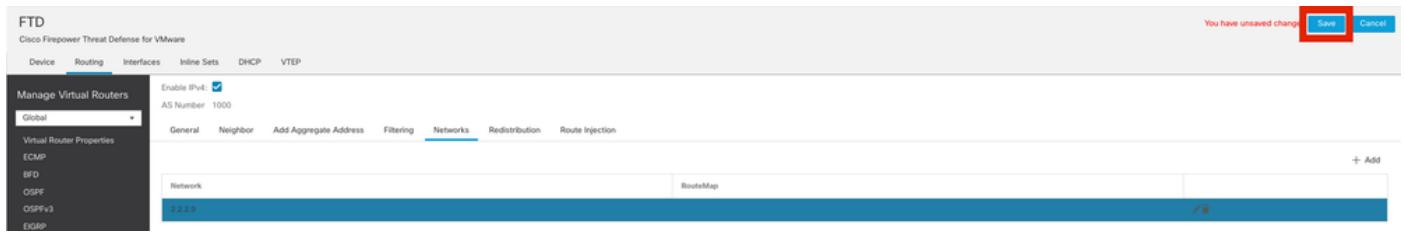
General Neighbor Add Aggregate Address Filtering Networks Redistribution Route Injection

Network	RouteMap
2.2.2.0	

+ Add

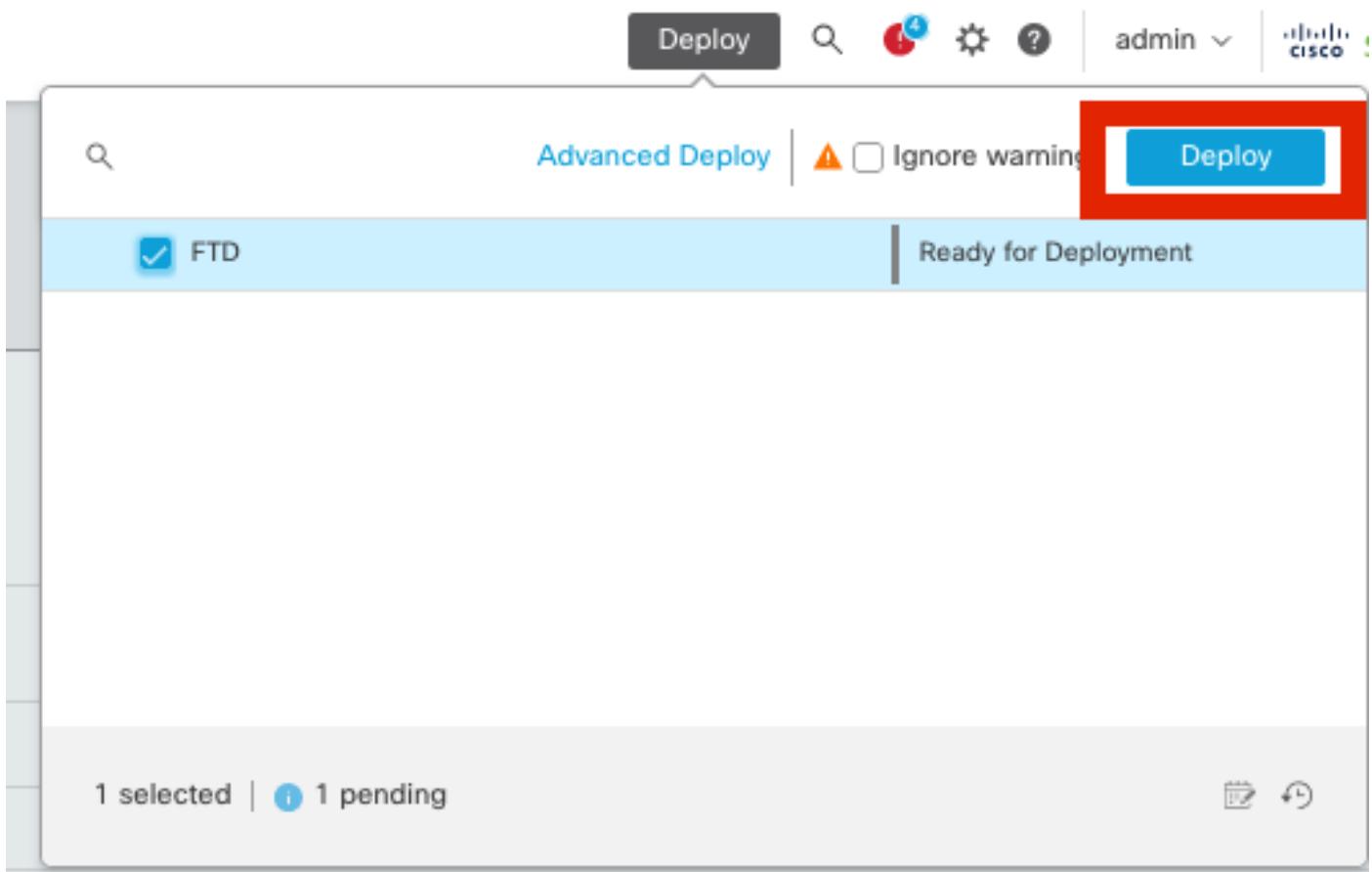
تاكبش ئافاصل BGP

رقن او نويوكتلار نم ققحت. كې ئەصالخا ئىيېپللى اقبط اهنىوكت كەنكمىو ئىرایتىخا ئىرخالا BGP تادادعى عىمەج نوكت. 5. ۋوطخلۇ قوف.



نويوكت ظفح BGP

تانىوكتلار عىمەج رشننپ مۇق. 6. ۋوطخلۇ.



رشنلار

ىلۇع يەطختىلار بىنار ئىيېپك

```
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
```

ةحصـلـا نـم قـقـحـتـلـا

حيـحـصـ لـكـشـبـ نـيـوـكـتـلـاـ لـمـعـ دـيـكـأـتـلـ مـسـقـلـاـ اـذـ مـدـخـتـسـاـ

ةـعـرـسـلـاـ قـيـافـ لـاسـرـالـاـ جـمـانـرـبـ رـاطـاـ يـفـ جـتـاـونـلـاـ

```
<#root>
```

```
#show crypto ikev2 sa
```

IKEv2 SAs:

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

Tunnel-id	Local	Remote	fvrif/ivrf	Status	Role
666846307	10.197.226.222/500	10.197.226.187/500	Global/Global	READY	RESPONDER
Encr: AES-CBC, keysiz: 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: ASA-VTI

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

Protected vrf (ivrf): 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
```

دحوملـا عادـلـا رـشـوـمـبـ قـقـلـعـتـمـلـا جـتـاـونـلـا

```
<#root>
```

```
#show crypto ikev2 sa
```

IKEv2 SAs:

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

Tunnel-id	Local	Remote	fvrif/ivrf	Status
442126361	10.197.226.187/500	10.197.226.222/500	Global/Global	READY
Enr: AES-CBC, keysiz: 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 (ivrf): 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 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: 169.254.2.1

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's 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
```

اھالص او ءاطخألا فاشكتسا

اھالص او نيوكتللإا ءاطخألا فاشكتسا امدادختسا کنکمي تامولعم مسقلما اذه رفوی.

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

- مع دجوي ال) ئيرهاظلا ئصالخا ئكبشلا ئلومح وأ ئيمحملاتاكبشلا وأ IPv4 ئيلإ ئفاصالاب، طقف IPv4 تاهجاو معدي ل IPv6).

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).