

Konfigurieren eines routenbasierten Site-to-Site-VPNs zwischen ASA und FTD mit BGP als Overlay

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Konfigurieren von IPSec VPN auf FTD mit FMC](#)

[Loopback-Schnittstelle auf FTD mit FMC konfigurieren](#)

[Konfigurieren von IPSec-VPN auf ASA](#)

[Konfigurieren der Loopback-Schnittstelle auf ASA](#)

[Konfigurieren des Overlay-BGP auf FTD mit FMC](#)

[Overlay-BGP auf ASA konfigurieren](#)

[Überprüfung](#)

[FTD-Outputs](#)

[Ausgänge auf ASA](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird die Konfiguration eines routenbasierten Site-to-Site-VPN-Tunnels zwischen der Adaptive Security Appliance (ASA) und dem von einem FirePOWER Management Center (FMC) verwalteten FirePOWER Threat Defense (FTD) mit dynamischem Routing und Border Gateway Protocol (BGP) als Overlay beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegendes Verständnis von IPsec Site-to-Site-VPN
- BGP-Konfigurationen auf FTD und ASA
- Erfahrungen mit FMC

Verwendete Komponenten

- Cisco ASA Version 9.20(2)2
- Cisco FMC Version 7.4.1
- Cisco FTD Version 7.4.1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

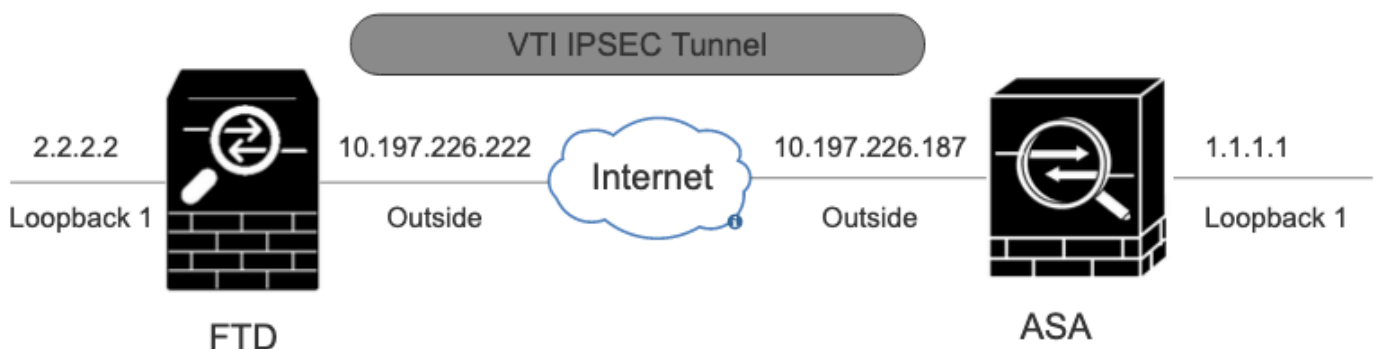
Routenbasiertes VPN ermöglicht die Bestimmung des relevanten Datenverkehrs, der verschlüsselt oder über einen VPN-Tunnel gesendet werden soll, und verwendet Datenverkehrs-Routing anstelle von Richtlinien/Zugriffslisten wie in einem richtlinienbasierten oder Krypto-Map-basierten VPN. Die Verschlüsselungsdomäne ist so festgelegt, dass jeder Datenverkehr zugelassen wird, der in den IPsec-Tunnel eintritt. IPsec-Auswahlen für lokalen und Remote-Datenverkehr werden auf 0.0.0.0/0.0.0.0 gesetzt. Jeder Datenverkehr, der in den IPsec-Tunnel geleitet wird, wird unabhängig vom Quell-/Ziel-Subnetz verschlüsselt.

Der Schwerpunkt dieses Dokuments liegt auf der SVTI-Konfiguration (Static Virtual Tunnel Interface) mit dynamischem Routing und BGP als Overlay.

Konfigurieren

In diesem Abschnitt wird die Konfiguration beschrieben, die für ASA und FTD erforderlich ist, um die BGP-Nachbarschaft über einen SVTI IPsec-Tunnel zu aktivieren.

Netzwerkdiagramm



Netzwerkdiagramm

Konfigurationen

Konfigurieren von IPsec VPN auf FTD mit FMC

Schritt 1: Navigieren Sie zu **Devices > VPN > Site To Site** .

Schritt 2: Klicken Sie auf **+Site to Site VPN** .



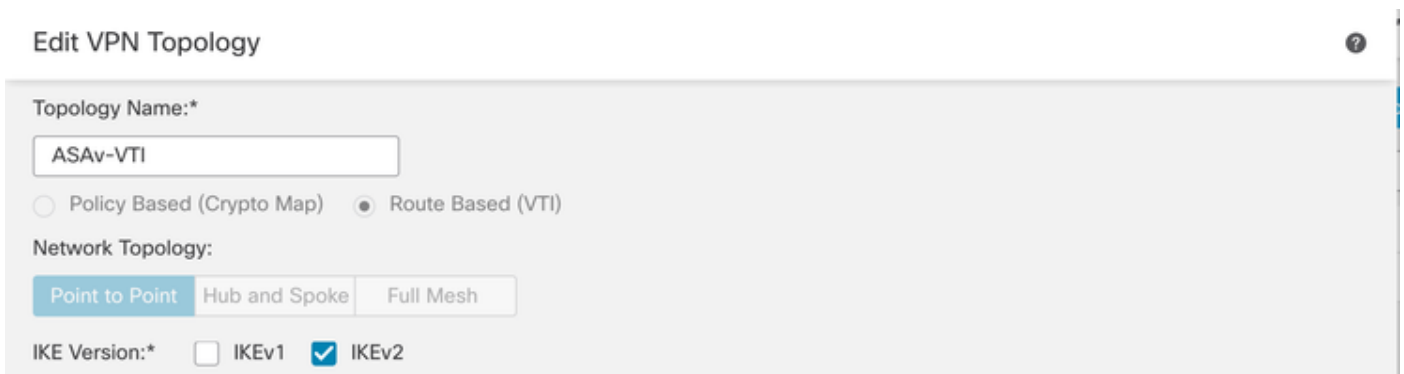
Standortübergreifendes VPN

Schritt 3: Geben Sie ein Topology Name an, und wählen Sie den VPN-Typ aus, als Route Based (VTI). Wählen Sie den IKE Version.

Für diese Demonstration:

Topologienname: ASAv-VTI

IKE-Version: IKEv2



VPN-Topologie

Schritt 4: Wählen Sie Device aus, auf welchem Tunnel der Tunnel konfiguriert werden soll. Sie können eine neue Virtual Tunnel Interface hinzufügen (klicken Sie auf das + Symbol), oder wählen Sie eine aus der vorhandenen Liste aus.

Node A

Device:*

Virtual Tunnel Interface:*



Tunnel Source IP is Private [Edit VTI](#)

Send Local Identity to Peers

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

▶ Advanced Settings

Endpunktknoten A

Schritt 5: Definieren Sie die Parameter der New Virtual Tunnel Interface. Klicken Sie auf .Ok

Für diese Demonstration:

Name: ASA-VTI

Beschreibung (optional): VTI-Tunnel mit Extranet-ASA

Sicherheitszone: VTI-Zone

Tunnel-ID: 1

IP-Adresse: 169.254.2.1/24

Tunnelquelle: GigabitEthernet0/1 (außen)

IPsec-Tunnelmodus: 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

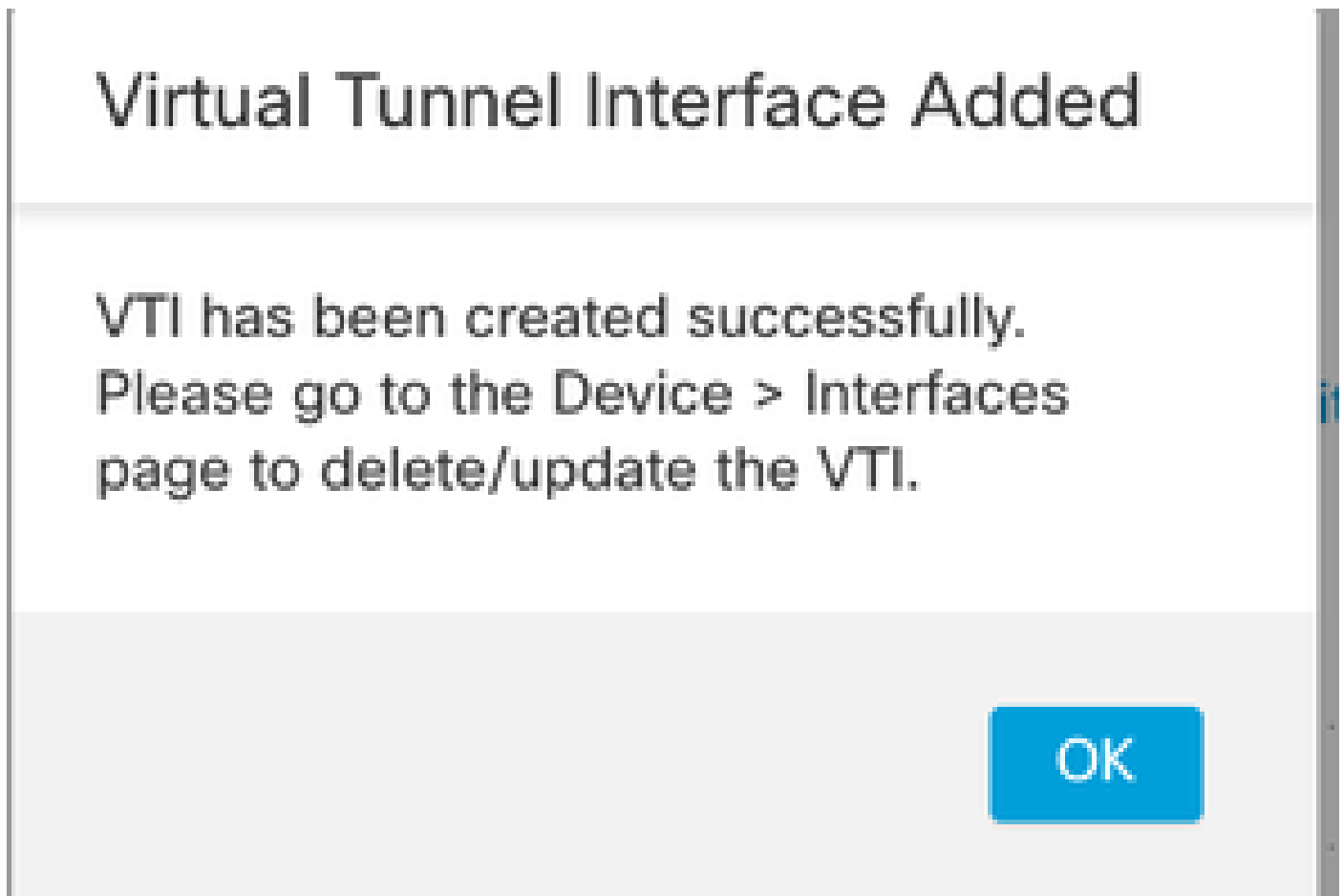
Borrow IP (IP unnumbered)

Loopback1 (loopback)

Cancel

OK

Schritt 6: Klicken Sie OK auf das Pop-Up, um zu erwähnen, dass das neue VTI erstellt wurde.



Virtual Tunnel Interface hinzugefügt

Schritt 7. Wählen Sie den neu erstellten VTI oder einen VTI unter Virtual Tunnel Interface. Geben Sie die Informationen für Knoten B (das Peer-Gerät) an.

Für diese Demonstration:

Gerät: Extranet

Gerätename: ASAv-Peer

Endpunkt-IP-Adresse: 10.197.226.187

Node A

Device:*

Virtual Tunnel Interface:*

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](#)

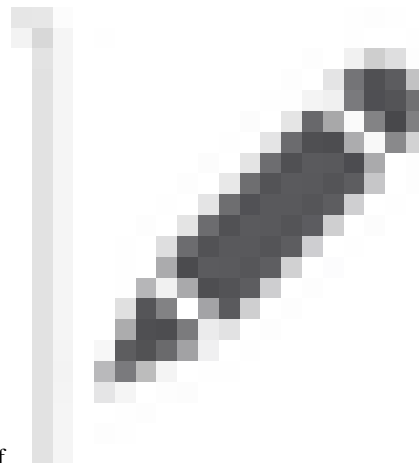
Node B

Device:*

Device Name*:

Endpoint IP Address*:

Endpunktknoten B



Schritt 8: Navigieren Sie zur Registerkarte **IKE**. Klicken Sie auf

. Sie können eine vordefinierte Policy Option auswählen oder auf die +Schaltfläche neben der Policy Registerkarte klicken, um eine neue zu erstellen.

Schritt 9: (Optional, wenn Sie eine neue IKEv2-Richtlinie erstellen.) Geben Sie eine Name für die Richtlinie an, und wählen Sie die Algorithms aus, die in der Richtlinie verwendet werden soll. Klicken Sie auf .Save

Für diese Demonstration:

Name: ASAv-IKEv2-policy

Integritätsalgorithmen: SHA-256

Verschlüsselungsalgorithmen: AES-256

PRF-Algorithmen: SHA-256

Diffie-Hellman-Gruppe: 14

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-Richtlinie

Schritt 10. Wählen Sie die neu erstellte Policy oder die Policyvorhandene aus. Wählen Sie den Authentication Type. Wenn ein vorinstallierter manueller Schlüssel verwendet wird, geben Sie den Schlüssel in das Confirm Key Feld Keyund ein.

Für diese Demonstration:

Richtlinie: ASAv-IKEv2-Richtlinie

Authentifizierungstyp: Vorinstallierter manueller Schlüssel

IKEv2 Settings

Policies:*

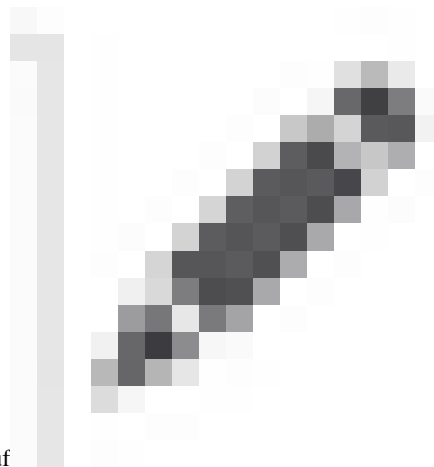
Authentication Type:


Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Authentifizierung



Schritt 11. Navigieren Sie zur IPsec Registerkarte. Klicken Sie auf , um ein vordefiniertes IKEv2 IPsec-Angebot zu verwenden oder ein neues zu erstellen. Klicken Sie auf die +Schaltfläche neben der IKEv2 IPsec Proposal Registerkarte.

Schritt 12: (Optional, wenn Sie ein neues IKEv2 IPsec-Angebot erstellen.) Geben Sie einen Namen für den Vorschlag ein, und wählen Sie den Algorithmus aus, der für den Vorschlag verwendet werden soll. Klicken Sie auf **.Save**

Für diese Demonstration:

Name: ASAv-IPSec-Policy

ESP-Hash: SHA-256

ESP-Verschlüsselung: AES-256

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

IKEv2-IPsec-Vorschlag

Schritt 13: Wählen Sie in der Liste der verfügbaren Angebote die neu erstellte Proposal oder die vorhandene aus. Klicken Sie auf .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

Transformationsatz

Schritt 14. (Optional) Wählen Sie die Perfect Forward Secrecy Einstellungen aus. Konfigurieren Sie IPsec Lifetime Duration and Lifetime Size.

Für diese Demonstration:

Perfect Forward Secrecy: Modulus Group 14

Lebensdauer: 28800 (Standard)

Lebenszeitgröße: 4608000 (Standard)

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:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

Schritt 15: Überprüfen Sie die konfigurierten Einstellungen. Klicken Sie Save, wie in diesem Bild dargestellt.

Edit VPN Topology

Topology Name: ASAw-VTI

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

IKE Version: IKEv1 IKEv2

Endpoints | **IKE** | IPsec | Advanced

Node A

Device: FTD

Virtual Tunnel Interface: ASAw-VTI (IP: 169.254.3.1) +

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: ASAw-Peer

Endpoint IP Address: 10.197.226.187

Speichern der Konfiguration

Loopback-Schnittstelle auf FTD mit FMC konfigurieren

Navigieren Sie zu Devices > Device Management . Bearbeiten Sie das Gerät, auf dem der Loopback konfiguriert werden muss.

Schritt 1: Fahren Sie mit Interfaces > Add Interfaces > Loopback Interface fort.

Device | Routing | **Interfaces** | Inline Sets | DHCP | VTEP

All Interfaces | Virtual Tunnels

Search by name

Sync Device

Add Interfaces

- Loopback Interface
- Redundant Interface
- Bridge Group Interface

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0	inside	Physical	Inside		10.197.224.227(2)(Static)	Disabled	Global

Zur Loopback-Schnittstelle navigieren

Schritt 2: Geben Sie den Namen "loopback" ein, geben Sie eine Loopback-ID "1" an, und aktivieren Sie die Schnittstelle.

Edit Loopback Interface



General

IPv4

IPv6

Name:

loopback

Enabled

Loopback ID:*

1

(1-1024)

Description

Cancel

OK

Loopback-Schnittstelle aktivieren

Schritt 3: Konfigurieren Sie die IP-Adresse für die Schnittstelle, und klicken Sie auf OK .

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

Bereitstellen der IP-Adresse für die Loopback-Schnittstelle

Konfigurieren von IPSec-VPN auf 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
```

Konfigurieren der Loopback-Schnittstelle auf ASA

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

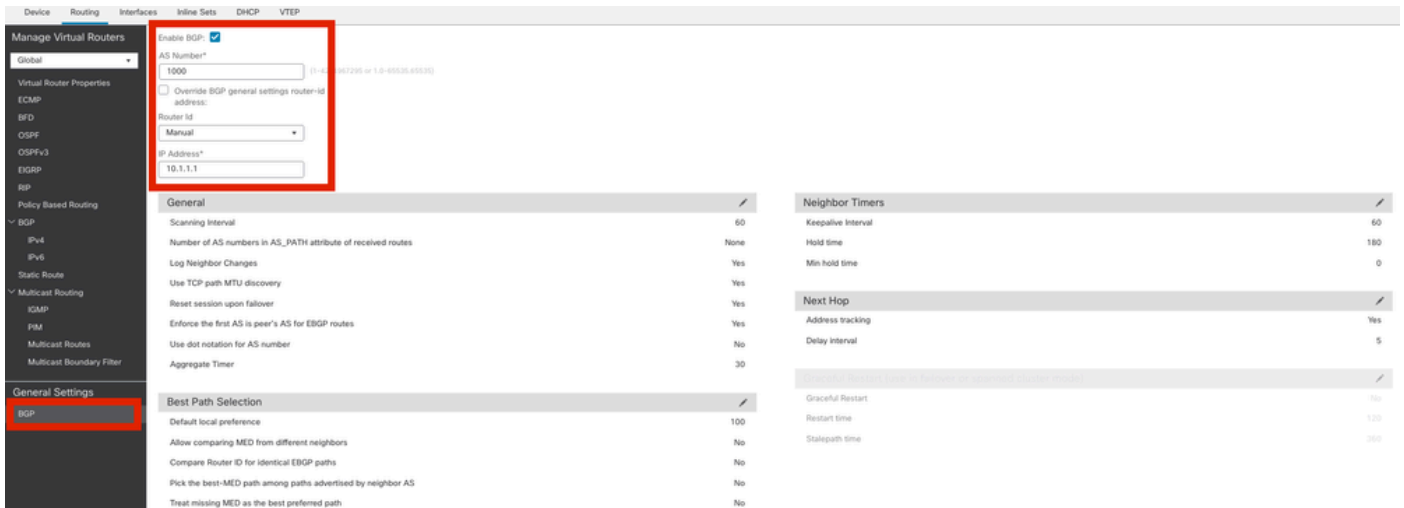
Konfigurieren des Overlay-BGP auf FTD mit FMC

Navigieren Sie zu Devices > Device Management. Edit dem Gerät, auf dem der VTI-Tunnel konfiguriert ist, und navigieren Sie dann zu Routing > General Settings > BGP.

Schritt 1: Aktivieren Sie BGP, und konfigurieren Sie die AS-Nummer (Autonomous System) und Router-ID, wie in diesem Bild gezeigt.

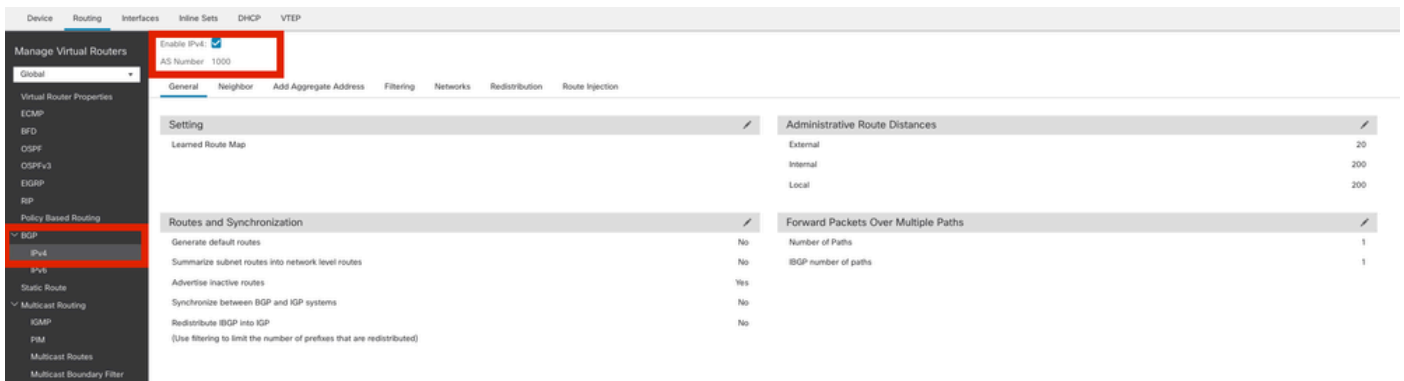
Die AS-Nummer muss auf den Geräten FTD und ASA identisch sein.

Die Router-ID wird verwendet, um alle Router zu identifizieren, die am BGP teilnehmen.



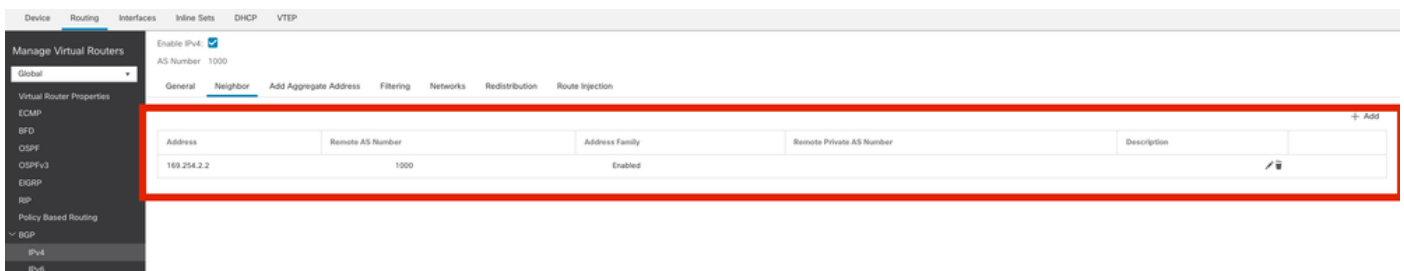
Navigieren zur BGP-Konfiguration

Schritt 2: BGP > IPv4 Navigieren Sie im FTD zu BGP IPv4, und aktivieren Sie es.



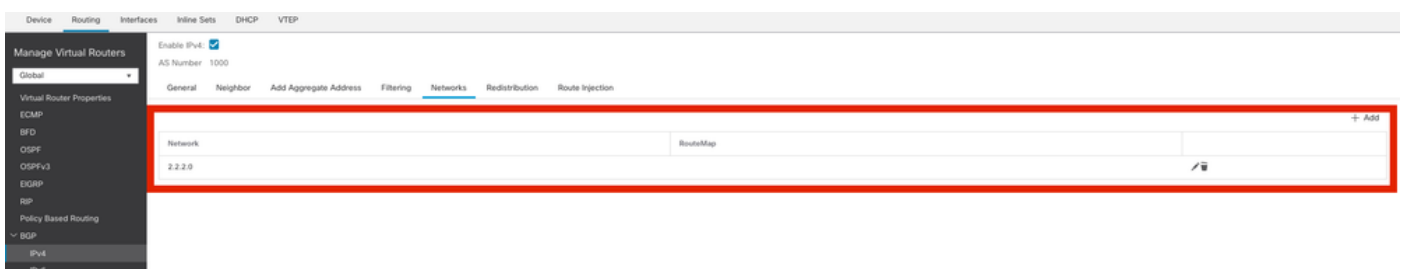
BGP aktivieren

Schritt 3: Fügen Sie auf derNeighbor Registerkarte die IP-Adresse des ASA v VTI-Tunnels als Nachbar hinzu, und aktivieren Sie den Nachbar.



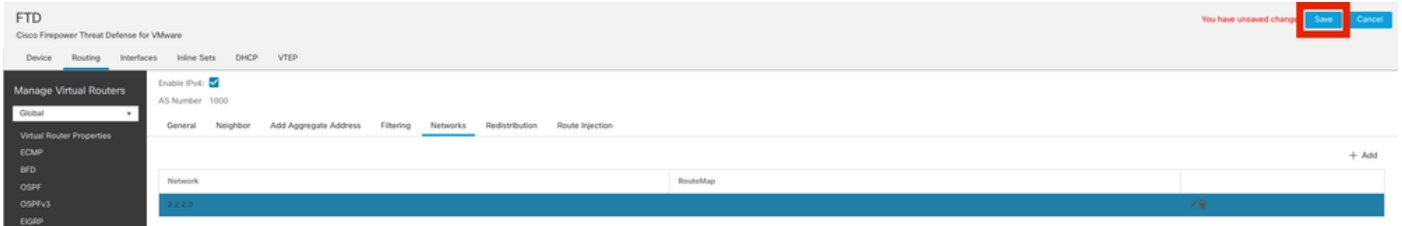
BGP-Nachbar hinzufügen

Schritt 4: Fügen Sie unterNetworks die Netzwerke hinzu, die über BGP angekündigt werden sollen und den VTI-Tunnel durchlaufen müssen, in diesem Fall Loopback1.



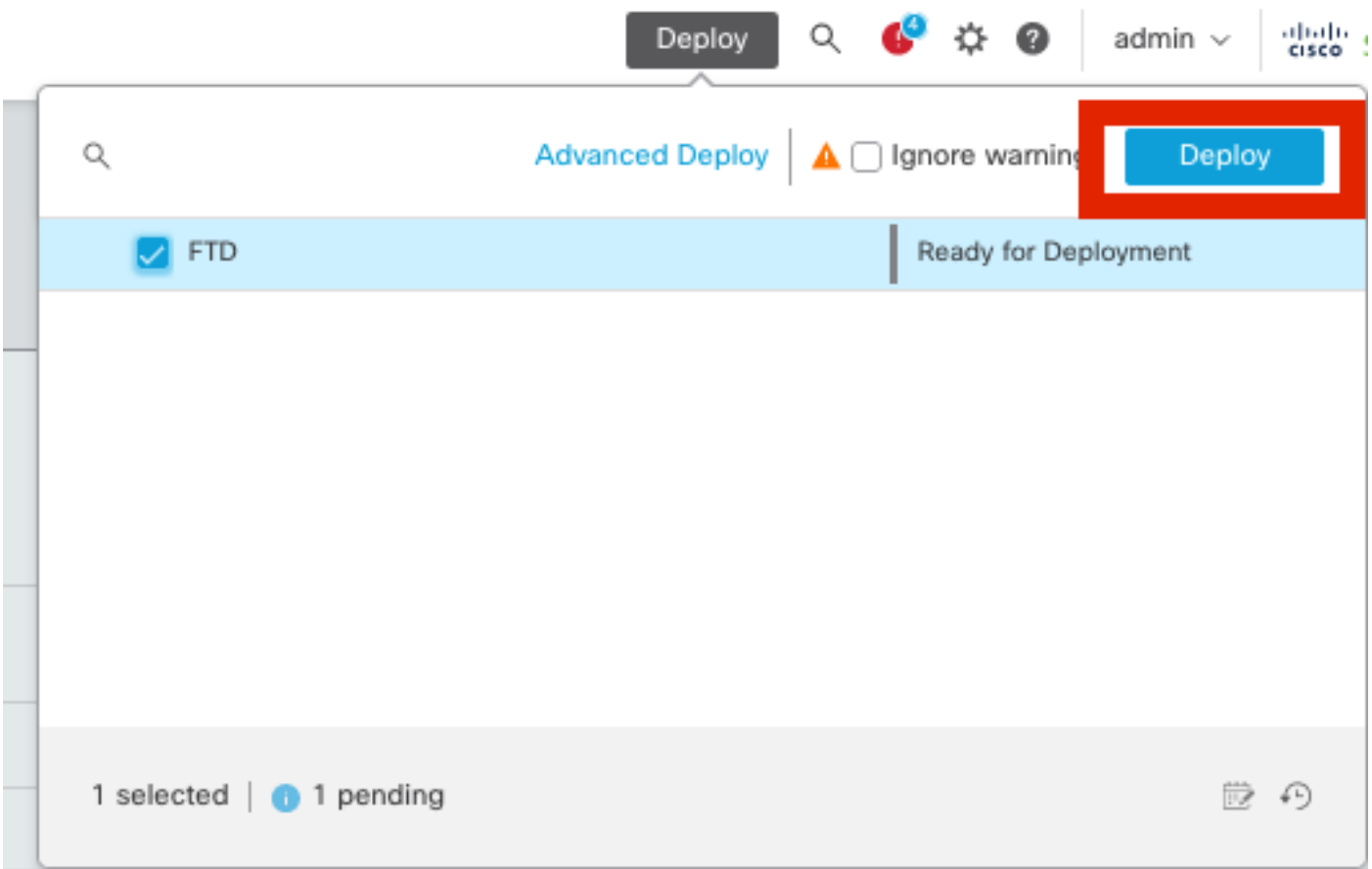
BGP-Netzwerke hinzufügen

Schritt 5: Alle anderen BGP-Einstellungen sind optional und können entsprechend Ihrer Umgebung konfiguriert werden. Überprüfen Sie die Konfiguration, und klicken Sie auf Save.



BGP-Konfiguration speichern

Schritt 6: Bereitstellen aller Konfigurationen



Bereitstellung

Overlay-BGP auf ASA konfigurieren

```
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
```

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

FTD-Outputs

<#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	RESPONDER

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 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

Ausgänge auf ASA

<#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	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): 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 0x007FFFFFF

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 NLRIs 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

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

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

- Unterstützt nur IPv4-Schnittstellen sowie IPv4, geschützte Netzwerke oder VPN-Nutzlasten (keine Unterstützung für IPv6).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.