

Configurar a VPN site a site baseada em rota entre o ASA e o FTD com o BGP como sobreposição

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configurar a VPN IPSec no FTD usando o FMC](#)

[Configurar a interface de loopback no FTD usando o FMC](#)

[Configurar VPN IPSec no ASA](#)

[Configurar a interface de loopback no ASA](#)

[Configurar o BGP de sobreposição no FTD usando o FMC](#)

[Configurar o BGP de sobreposição no ASA](#)

[Verificar](#)

[Saídas no FTD](#)

[Saídas no ASA](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar um túnel VPN site a site baseado em rota entre o Adaptive Security Appliance (ASA) e o Firepower Threat Defense gerenciado (FTD) por um Firepower Management Center (FMC) com Border Gateway Protocol (BGP) de roteamento dinâmico como uma sobreposição.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão básica da VPN de site a site IPsec
- Configurações de BGP em FTD e ASA
- Experiência com o FMC

Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A VPN baseada em rotas permite a determinação de tráfego interessante a ser criptografado ou enviado por um túnel VPN e usa o roteamento de tráfego em vez de política/lista de acesso como em uma VPN baseada em política ou em mapa de criptografia. O domínio de criptografia é definido para permitir qualquer tráfego que entre no túnel IPsec. Os seletores de tráfego local e remoto IPsec são definidos como 0.0.0.0/0.0.0.0. Qualquer tráfego roteado para o túnel IPsec é criptografado, independentemente da sub-rede de origem/destino.

Este documento enfoca a configuração da Interface de Túnel Virtual Estático (SVTI - Static Virtual Tunnel Interface) com o roteamento dinâmico BGP como uma sobreposição.

Configurar

Esta seção descreve a configuração necessária no ASA e no FTD para ativar a vizinhança BGP através de um túnel IPsec SVTI.

Diagrama de Rede

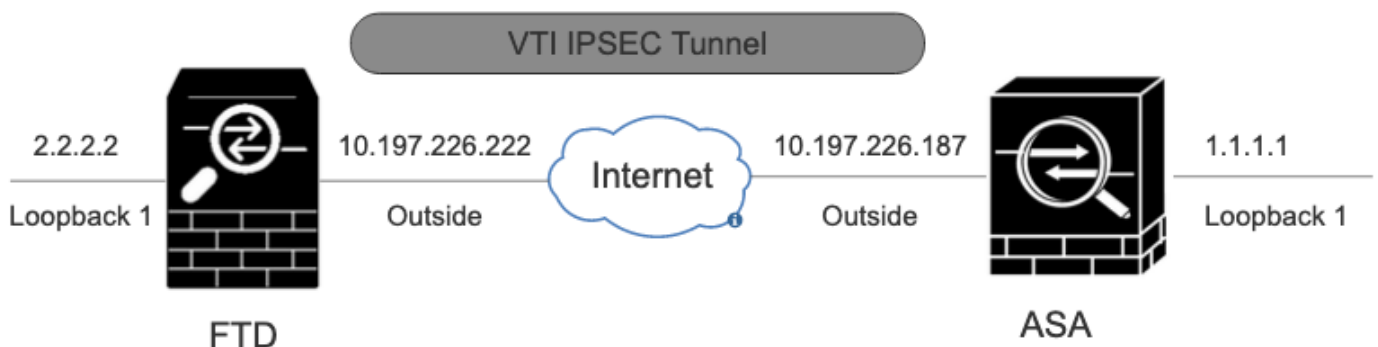


Diagrama de Rede

Configurações

Configurar a VPN IPsec no FTD usando o FMC

Etapa 1. Navegue até `Devices > VPN > Site To Site`.

Etapa 2. Clique em +Site to Site VPN .



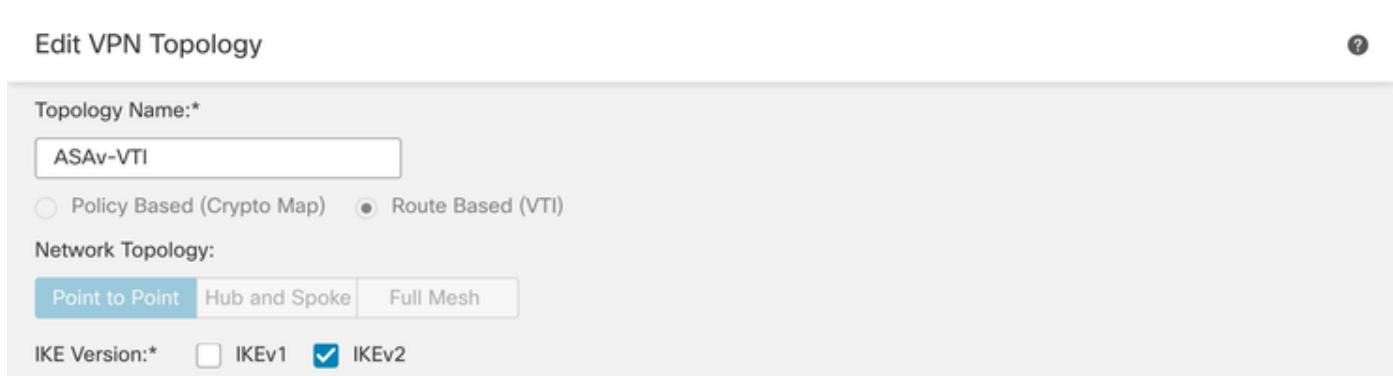
VPN site a site

Etapa 3. Forneça um Topology Name e selecione o Tipo de VPN como Route Based (VTI). Escolha o IKE Version.

Para esta demonstração:

Nome da topologia: ASAv-VTI

Versão do IKE: IKEv2

A screenshot of a web form titled 'Edit VPN Topology'. The form contains the following fields and options:

- Topology Name:*** A text input field containing 'ASAv-VTI'.
- VPN Type:** Two radio buttons: 'Policy Based (Crypto Map)' (unselected) and 'Route Based (VTI)' (selected).
- Network Topology:** Three buttons: 'Point to Point' (selected), 'Hub and Spoke', and 'Full Mesh'.
- IKE Version:*** Two checkboxes: 'IKEv1' (unselected) and 'IKEv2' (checked).

Topologia de VPN

Etapa 4. Escolha o Device no qual o túnel precisa ser configurado. Você pode adicionar uma nova Virtual Tunnel Interface (clique no ícone+) ou selecionar uma na lista existente.

Node A

Device:*

Virtual Tunnel Interface:*



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

Send Local Identity to Peers

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

▶ Advanced Settings

Nó de ponto final A

Etapa 5. Defina os parâmetros do New Virtual Tunnel Interface. Clique em Ok.

Para esta demonstração:

Nome: ASA-VTI

Descrição (Opcional): Túnel VTI com Extranet ASA

Zona de segurança: VTI-Zone

ID do túnel: 1

Endereço IP: 169.254.2.1/24

Origem do Túnel: GigabitEthernet0/1 (Externo)

Modo de túnel 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

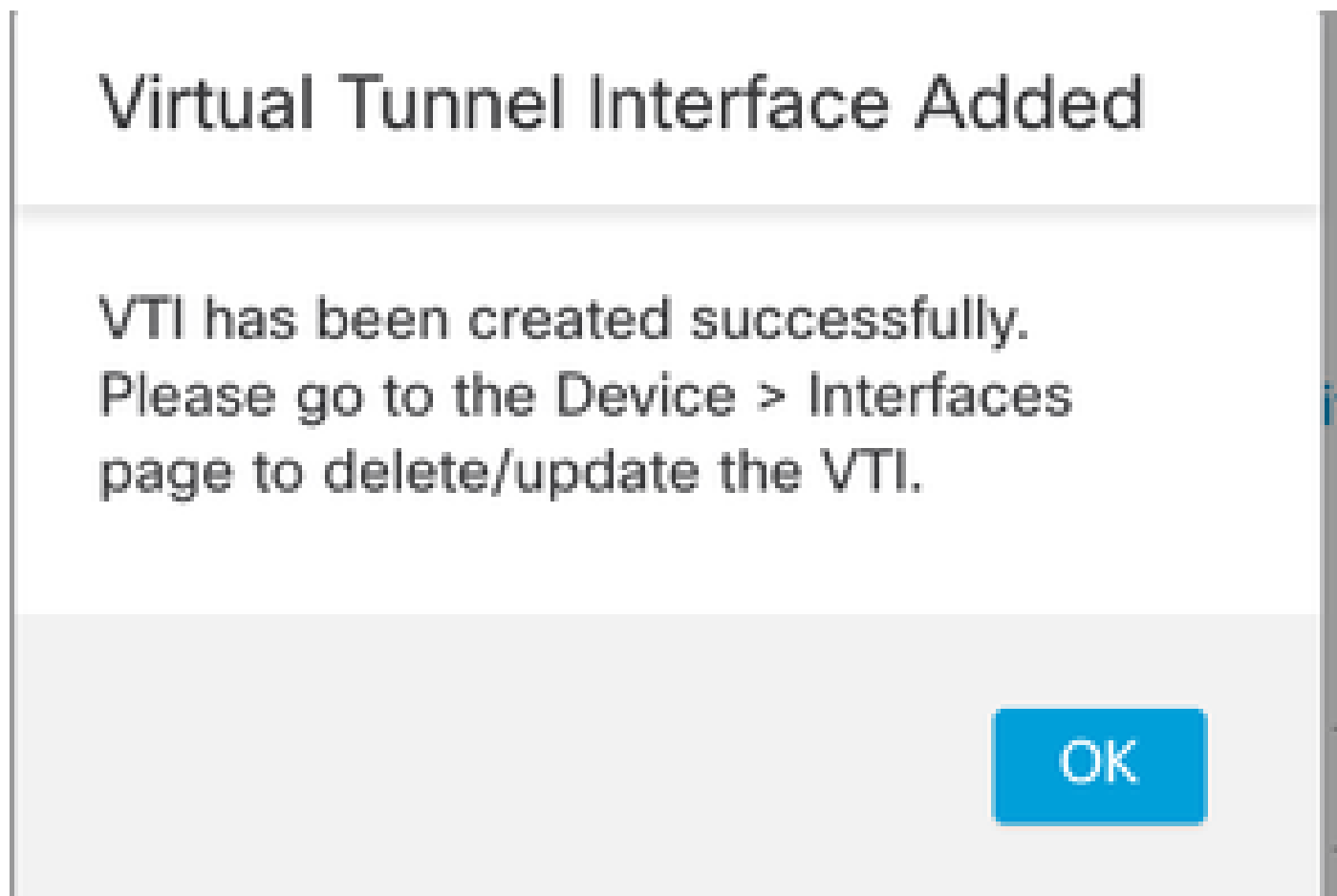
Borrow IP (IP unnumbered)

Loopback1 (loopback)

Cancel

OK

Etapa 6. Clique OK no pop-up que menciona que o novo VTI foi criado.



Passo 7. Escolha o VTI recém-criado ou um VTI em Virtual Tunnel Interface. Forneça as informações para o Nó B (que é o dispositivo peer).

Para esta demonstração:

Dispositivo: Extranet

Nome do dispositivo: ASAv-Peer

Endereço IP do endpoint: 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

Nó de ponto final B



Etapa 8. Navegue até a guia **IKE**. Clique em . Você pode optar por usar um predefinido Policy ou clicar no +botão ao lado da Policyguia para criar um novo.

Etapa 9. (Opcional, se você criar uma nova Política IKEv2.) Forneça um Namepara a política e selecione o Algorithms a ser usado na política. Clique em Save.

Para esta demonstração:

Nome: ASAv-IKEv2-policy

Algoritmos de integridade: SHA-256

Algoritmos de criptografia: AES-256

Algoritmos PRF: SHA-256

Grupo Diffie-Hellman: 14

Edit IKEv2 Policy



Name:*

ASAv-IKEv2-Policy

Description:

Priority: (1-65535)

1

Lifetime: seconds (120-2147483647)

86400

	Available Algorithms		Selected Algorithms
<ul style="list-style-type: none">Integrity AlgorithmsEncryption AlgorithmsPRF AlgorithmsDiffie-Hellman Group	MD5 SHA SHA512 SHA256 SHA384 NULL	Add	SHA256

Cancel

Save

IKEv2-Política

Etapa 10. Escolha o recém-criado Policy ou o Policy que existe. Selecione o Authentication Type. Se uma chave manual pré-compartilhada for usada, insira a chave na caixa KeyConfirm Key .

Para esta demonstração:

Política: ASAv-IKEv2-Política

Tipo de autenticação: chave manual pré-compartilhada

IKEv2 Settings

Policies:*

Authentication Type:


Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Autenticação



Etapa 11. Navegue até a IPsec guia. Clique em  para escolher usar uma proposta de IPsec IKEv2 predefinida ou criar uma nova. Clique no +botão ao lado da IKEv2 IPsec Proposal guia.

Etapa 12. (Opcional, se você criar uma nova proposta de IKEv2 IPsec.) Insira uma Name para a Proposta e selecione a Algorithms a ser usada na Proposta. Clique em Save.

Para esta demonstração:

Nome: ASAv-IPSec-Policy

Hash ESP: SHA-256

Criptografia ESP: 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-Proposal

Etapa 13. Na lista de propostas disponíveis, escolha o Proposal ou Proposalque foi criado recentemente. Clique em OK.

IKEv2 IPsec Proposal



Available Transform Sets ⊞

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

Transform Set

Etapa 14. (Opcional) Escolha as Perfect Forward Secrecy configurações. Configure o IPsec Lifetime Duration and Lifetime Size.

Para esta demonstração:

Segredo de encaminhamento perfeito: Grupo de módulos 14

Duração da Vida Útil: 28800 (Padrão)

Tamanho do Tempo de Vida: 4608000 (Padrão)

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)

Etapa 15. Verifique as configurações definidas. Clique em Save, conforme mostrado nesta imagem.

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

Salvando a configuração

Configurar a interface de loopback no FTD usando o FMC

Navegue até Devices > Device Management . Edite o dispositivo onde o loopback precisa ser configurado.

Etapa 1. Ir para. Interfaces > Add Interfaces > Loopback Interface



Navegue até a interface de loopback

Etapa 2. Insira o nome "loopback", forneça um ID de loopback "1" e ative a interface.

Edit Loopback Interface



General

IPv4

IPv6

Name:

loopback

Enabled

Loopback ID:*

1

(1-1024)

Description

Cancel

OK

Ativando a interface de loopback

Etapa 3. Configure o endereço IP para a interface e clique em 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

Forneça o endereço IP para a interface de loopback

Configurar VPN IPSec no 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
```

Configurar a interface de loopback no ASA

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

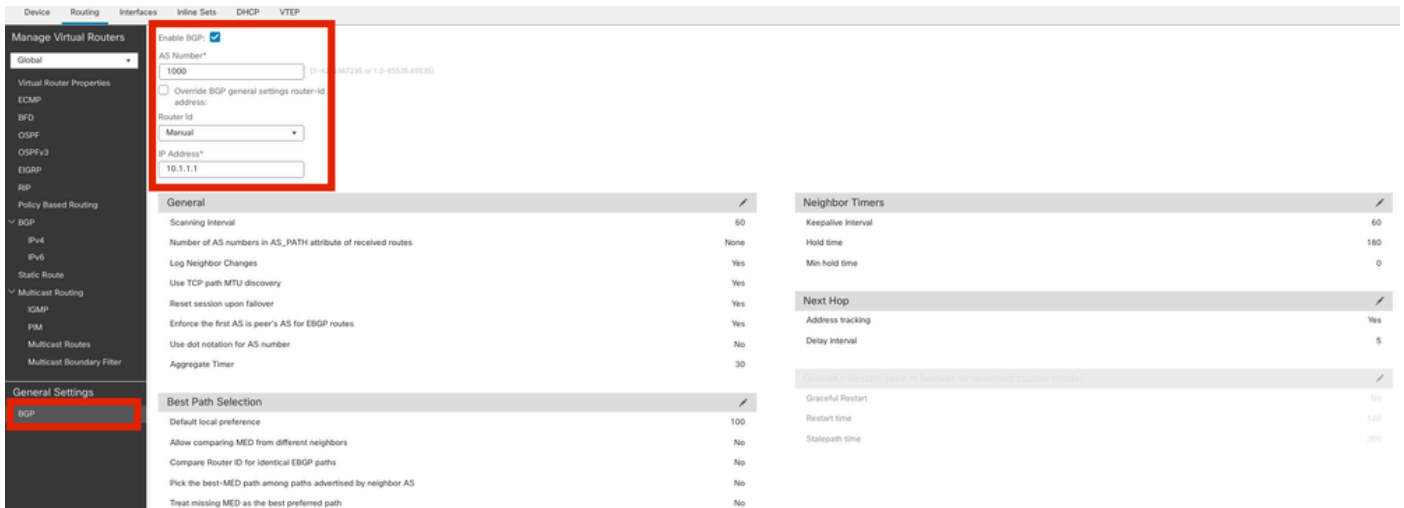
Configurar o BGP de sobreposição no FTD usando o FMC

Navegue até **Devices > Device Management**. Edite o dispositivo onde o túnel VTI está configurado e navegue até **Routing > General Settings > BGP**.

Etapa 1. Ative o BGP e configure o número do sistema autônomo (AS) e o ID do roteador, como mostrado nesta imagem.

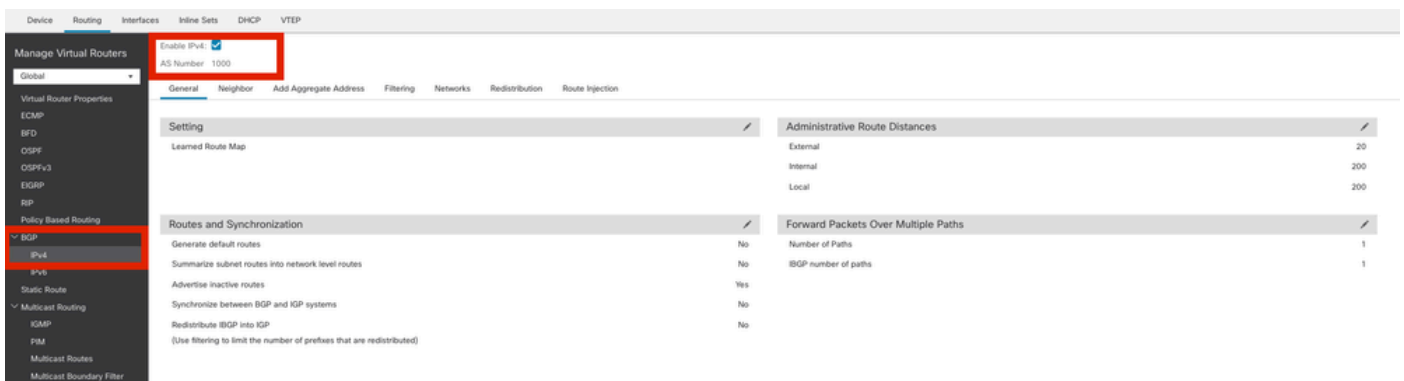
O número AS precisa ser o mesmo no FTD e no ASA dos dispositivos.

O ID do roteador é usado para identificar cada roteador que participa do BGP.



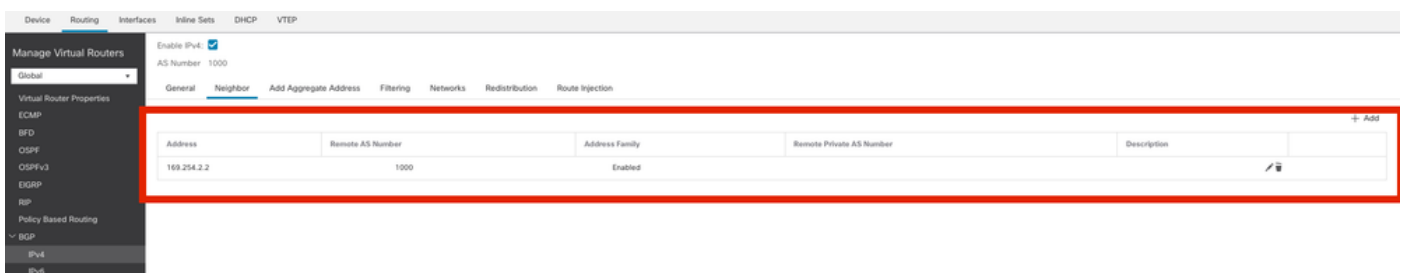
Navegue para configurar o BGP

Etapa 2. Navegue para BGP > IPv4 e habilite o BGP IPv4 no FTD.



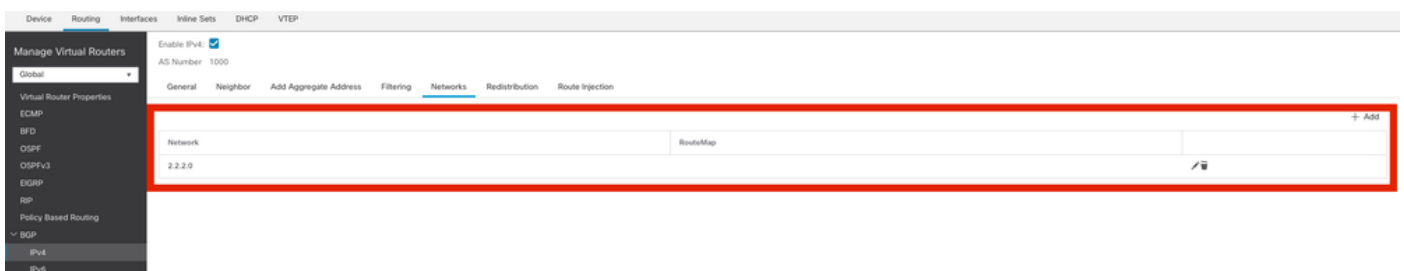
Habilitar BGP

Etapa 3. NaNeighbor guia, adicione o endereço ip do túnel VTI do ASAv como um vizinho e habilite o vizinho.



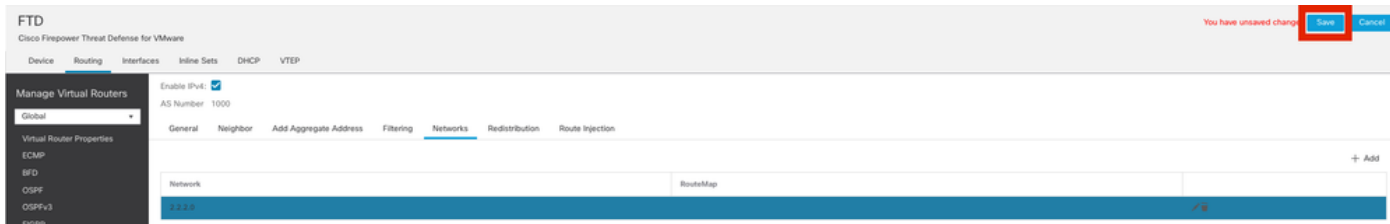
Adicionar vizinho BGP

Etapa 4. Em Networks, adicione as redes que você deseja anunciar através do BGP que precisam passar pelo túnel VTI, neste caso, loopback1.



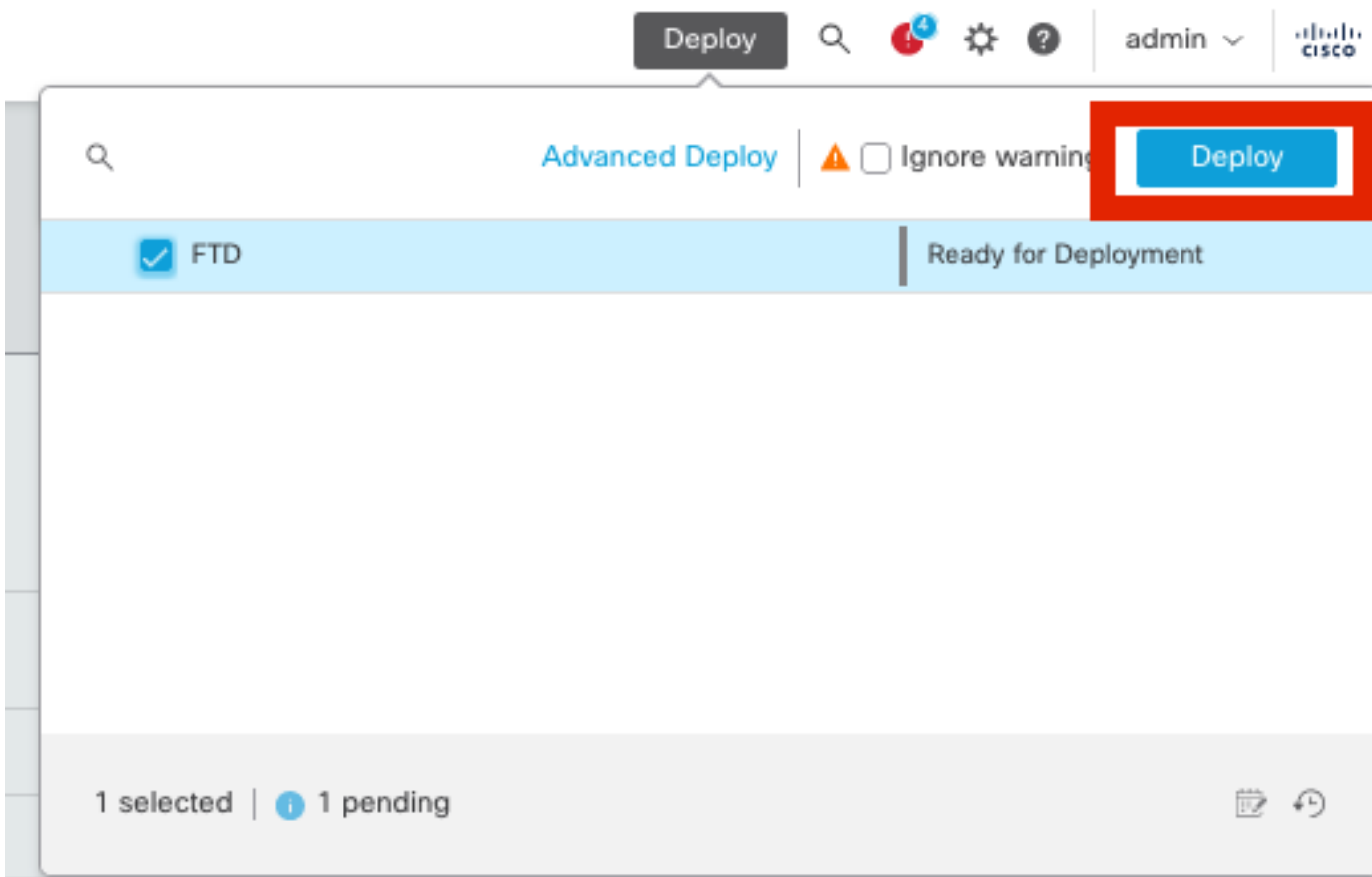
Adicionar redes BGP

Etapa 5. Todas as outras configurações de BGP são opcionais e você pode configurá-las de acordo com seu ambiente. Verifique a configuração e clique em Save.



Salvar configuração de BGP

Etapa 6. Implante todas as configurações.



Implantação

Configurar o BGP de sobreposição no ASA

```
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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Saídas no FTD

<#root>

#show crypto ikev2 sa

IKEv2 SAs:

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

Tunnel-id	Local	Remote	fvr/f/ivrf	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 (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 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

Saídas no 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 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

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

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

- Suporta somente interfaces IPv4, bem como IPv4, redes protegidas ou payload de VPN (Sem suporte para IPv6).

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.