

ASAとFTD間のルートベースのサイト間VPNの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[FMCを使用したFTDでのIPSec VPNの設定](#)

[FMCを使用したFTDのループバックインターフェイスの設定](#)

[ASAでのIPSec VPNの設定](#)

[ASAでのループバックインターフェイスの設定](#)

[FMCを使用したFTDでのオーバーレイBGPの設定](#)

[ASAでのオーバーレイBGPの設定](#)

[確認](#)

[FTDの出力](#)

[ASAでの出力](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、ダイナミックルーティングBGPをオーバーレイとして使用するFMCによって、ASAとFTDの間にルートベースのサイト間VPN(VPN)トンネルを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- IPSecサイト間VPNの基本的な知識
- Firepower Threat Defense(FTD)マネージド(FTD)および適応型セキュリティアプライアンス(ASA)でのBorder Gateway Protocol(BGP)の設定
- Firepower Management Center(FMC)の使用経験

使用するコンポーネント

- Cisco ASAvバージョン9.20(2)2
- Cisco FMCバージョン7.4.1
- Cisco FTDバージョン7.4.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

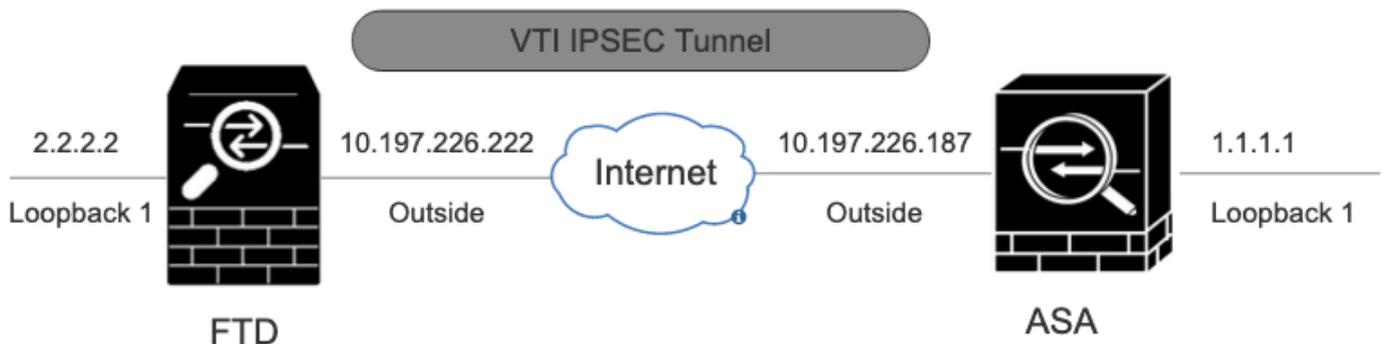
ルートベースのVPNでは、暗号化するトラフィック、またはVPNトンネル経由で送信するトラフィックを判別できません。また、ポリシーベースまたはクリプトマップベースのVPNのように、ポリシー/アクセスリストの代わりにトラフィックルーティングを使用します。暗号化ドメインは、IPsecトンネルに入るすべてのトラフィックを許可するように設定されます。IPsecローカルおよびリモートトラフィックセレクトは0.0.0.0/0.0.0.0に設定されます。IPsecトンネルにルーティングされるトラフィックは、送信元/宛先サブネットに関係なく暗号化されます。

このドキュメントでは、ダイナミックルーティングBGPをオーバーレイとして使用したスタティック仮想トンネルインターフェイス(SVTI)の設定を中心に説明します。

設定

このセクションでは、SVTI IPsecトンネル経由でBGPプロキシミティを起動するためにASAおよびFTDで必要な設定について説明します。

ネットワーク図



ネットワーク図

コンフィギュレーション

FMCを使用したFTDでのIPSec VPNの設定

ステップ 1 : Devices > VPN > Site To Siteの順に移動します。

ステップ 2 : +Site to Site VPNをクリックします。

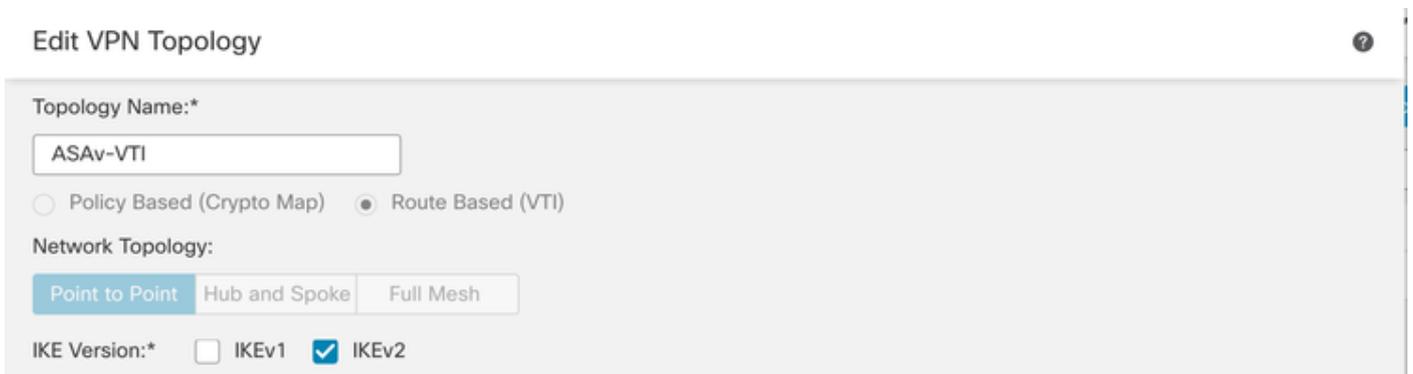


サイト間 VPN

ステップ 3：トポロジ名を指定し、VPNのタイプとしてRoute Based (VTI)を選択します。IKE Versionを選択します。

このデモンストレーションの内容：

- トポロジ名：ASAv-VTI
- IKEバージョン：IKEv2



VPNトポロジ

ステップ 4：トンネルを設定する必要があるデバイスを選択します。新しい仮想トンネルインターフェイスを追加するか(+アイコンをクリック)、既存のリストからインターフェイスを選択します。

Node A

Device:*

Virtual Tunnel Interface:*



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

Send Local Identity to Peers

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

▶ Advanced Settings

エンドポイントノードA

ステップ 5 : New Virtual Tunnel Interfaceのパラメータを定義します。[OK] をクリックします。

このデモンストレーションの内容 :

- 名前 : ASA-VTI
- 説明 (オプション) : エクストラネットASAを使用したVTIトンネル
- セキュリティゾーン : VTIゾーン
- トンネルID:1
- IPアドレス : 169.254.2.1/24
- トンネル送信元 : GigabitEthernet0/1 (外部)
- IPsecトンネルモード : 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

手順 6 : 新しいVTIが作成されたことを示すポップアップで[OK]をクリックします。

Virtual Tunnel Interface Added

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

OK

仮想トンネルインターフェイスの追加

手順 7 : 新しく作成したVTIまたはVirtual Tunnel Interfaceの下のVTIを選択します。ノードB (ピアデバイス) の情報を入力します。

このデモンストレーションの内容 :

- デバイス : エクストラネット
- デバイス名 : ASAv-Peer
- エンドポイントIPアドレス : 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*:

エンドポイントノードB



ステップ 8 : IKE タブに移動します。クリック

.定義済みのポリシーを使用するか、 Policytabの横にある+ボタンをクリックして新しいポリシーを作成するかを選択できます。

ステップ9: (新しいIKEv2ポリシーを作成する場合はオプション) ポリシーの名前を指定し、ポリシーで使用するアルゴリズムを選択します。[Save] をクリックします。

このデモンストレーションの内容 :

- 名前 : ASAv-IKEv2-policy
- 整合性アルゴリズム : SHA-256
- 暗号化アルゴリズム : AES-256
- PRFアルゴリズム : SHA-256
- Diffie-Hellmanグループ : 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ポリシー

ステップ 10 : 新しく作成したPolicyまたは存在するPoliciesを選択します。Authentication Typeを選択します。事前共有手動キーを使用する場合は、Key and Confirm Keyボックスにキーを入力します。

このデモンストレーションの内容 :

- ポリシー : ASAv-IKEv2-Policy
- 認証タイプ : 事前共有手動キー

IKEv2 Settings

Policies:* ASAv-IKEv2-Policy

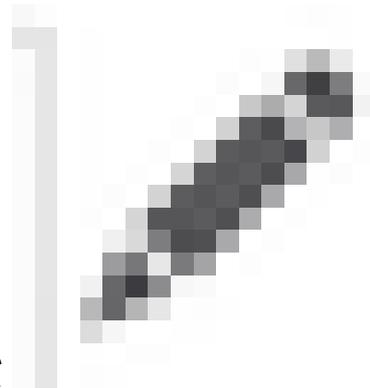
Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

認証



ステップ 11 IPsec タブに移動します。クリック ノイズ

事前に定義されたIKEv2 IPsecプロポーザルを使用するか、新しいプロポーザルを作成するかを選択できます。IKEv2 IPsec Proposal タブの横にある+ボタンをクリックします。

ステップ12. (新しいIKEv2 IPsecプロポーザルを作成する場合はオプション) プロポーザルの名前を入力し、プロポーザルで使用するアルゴリズムを選択します。[Save] をクリックします。

このデモンストレーションの内容：

- 名前：ASAv-IPSec-Policy
- ESPハッシュ：SHA-256
- ESP暗号化：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 – プロポーザル

ステップ 13 使用可能なプロポーザルのリストから、新しく作成したProposalまたはProposalを選択します。[OK] をクリックします。

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

変換セット

ステップ14: (オプション) Perfect Forward Secrecy設定を選択します。IPSecのライフタイム期間とライフタイムサイズを設定します。

このデモンストレーションの内容 :

- 完全転送秘密 : モジュラスグループ14
- ライフタイム期間 : 28800 (デフォルト)
- Lifetime Size (ライフタイムサイズ) :4608000 (デフォルト)

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)

ステップ 15 : 設定を確認します。次の図に示すように、Saveをクリックします。

Edit VPN Topology ?

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

IKE Version:* IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Node A

Device:*

Virtual Tunnel Interface:*

Tunnel Source: Outside (IP: 10.197.226.223) [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:*

Device Name*:

Endpoint IP Address*:

設定を保存します。

FMCを使用したFTDのループバックインターフェイスの設定

[Device] > [Device Management]に移動します。ループバックを設定する必要があるデバイスを編集します。

ステップ 1 : Interfaces > Add Interfaces > Loopback Interfaceの順に選択します。

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management/0	management	Physical				Disabled	Global	Add Interfaces
GlobalEthernet/0	inside	Physical	Inside		10.197.224.227(2/3/Static)	Disabled	Global	Loopback Interface

ループバックインターフェイスに移動します

ステップ 2 : 「loopback」という名前を入力し、ループバックID「1」を指定して、インターフェイスを有効にします。

Edit Loopback Interface



General

IPv4

IPv6

Name:

loopback

Enabled

Loopback ID:*

1

(1-1024)

Description

Cancel

OK

ループバックインターフェイスの有効化

ステップ 3 : インターフェイスのIPアドレスを設定し、OKをクリックします。

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

ループバックインターフェイスにIPアドレスを提供

ASAでのIPSec VPNの設定

!--- 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でのループバックインターフェイスの設定

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

FMCを使用したFTDでのオーバーレイBGPの設定

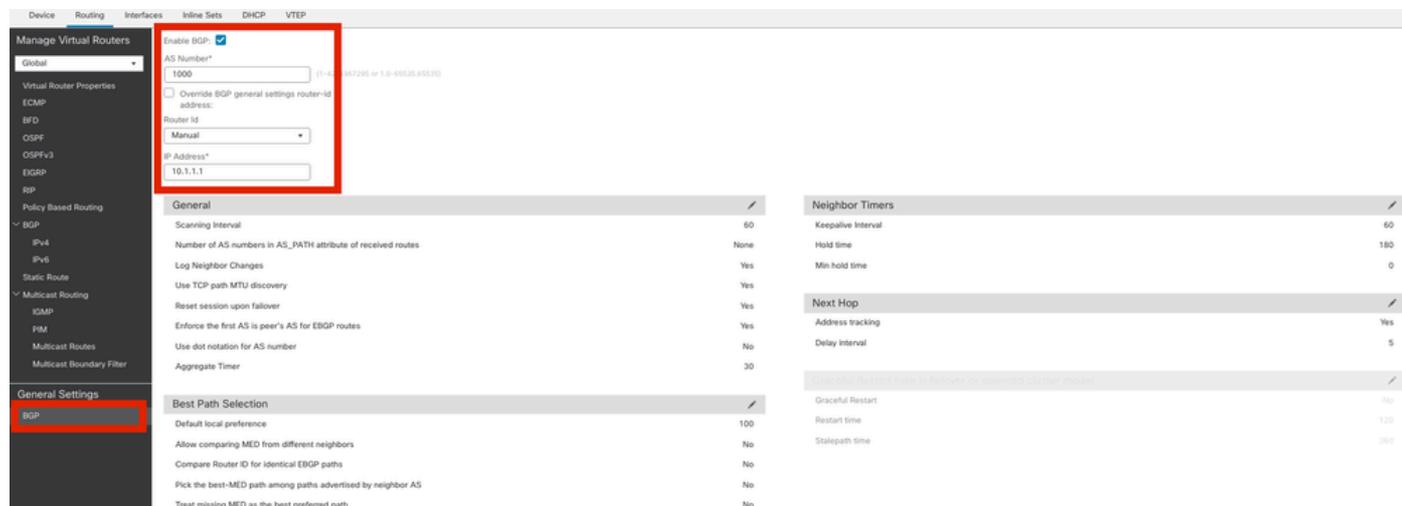
Devices > Device Managementの順に移動します。VTIトンネルが設定されているデバイスをEditしてから、Routing > General Settings > BGPの順に移動します。

ステップ 1 : BGPを有効にして、自律システム(AS)番号とルータIDを設定します (次の図を参照

)。

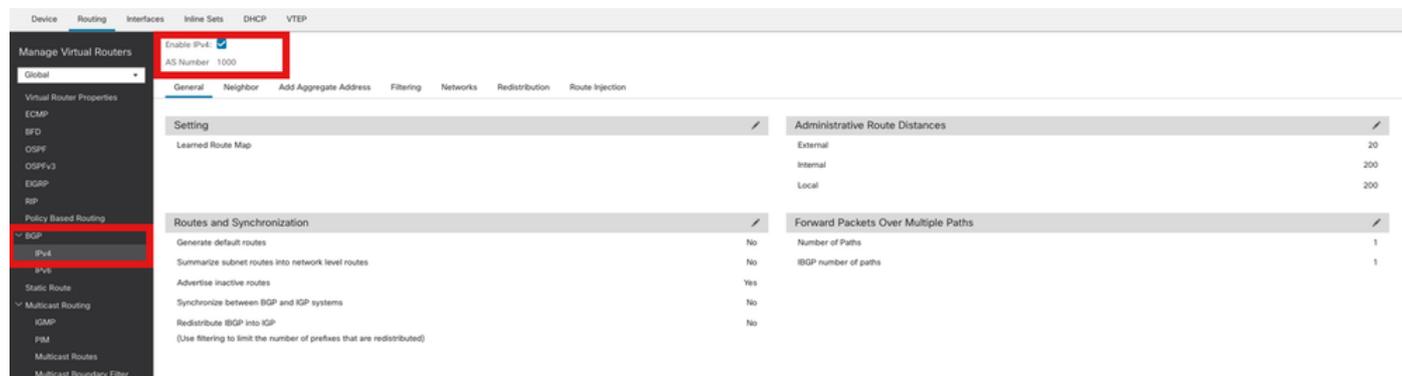
AS番号は、デバイスFTDとASAの両方で同じである必要があります。

ルータIDは、BGPに参加している各ルータを識別するために使用されます。



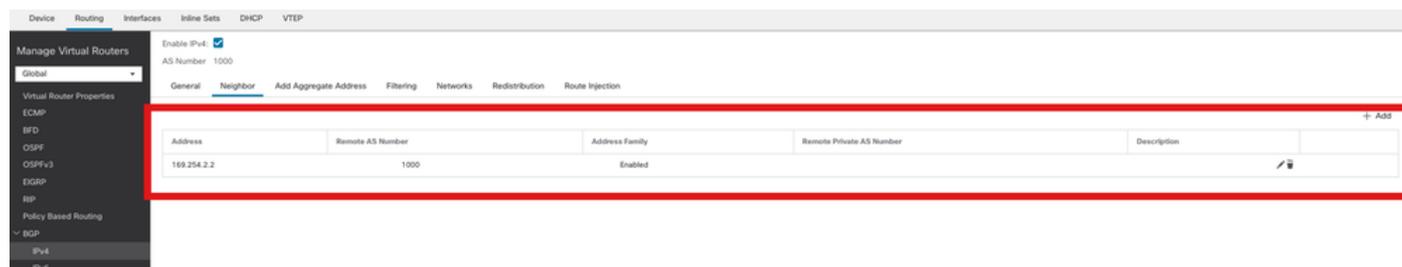
BGPを設定します

ステップ 2 : BGP > IPv4 に移動し、FTD で BGP IPv4 を有効にします。



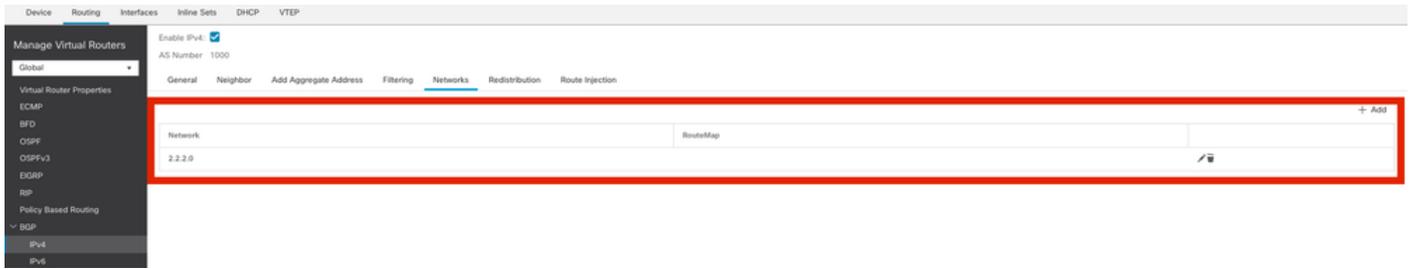
BGPの有効化

ステップ 3 : Neighbortab で、ネイバーとして ASAv VTI トンネルの IP アドレスを追加し、ネイバーを有効にします。



BGPネイバーの追加

ステップ 4 : Networks の下で、BGP を介してアドバタイズするネットワークのうち、VTI トンネルを通過する必要があるネットワーク (この場合は loopback1) を追加します。



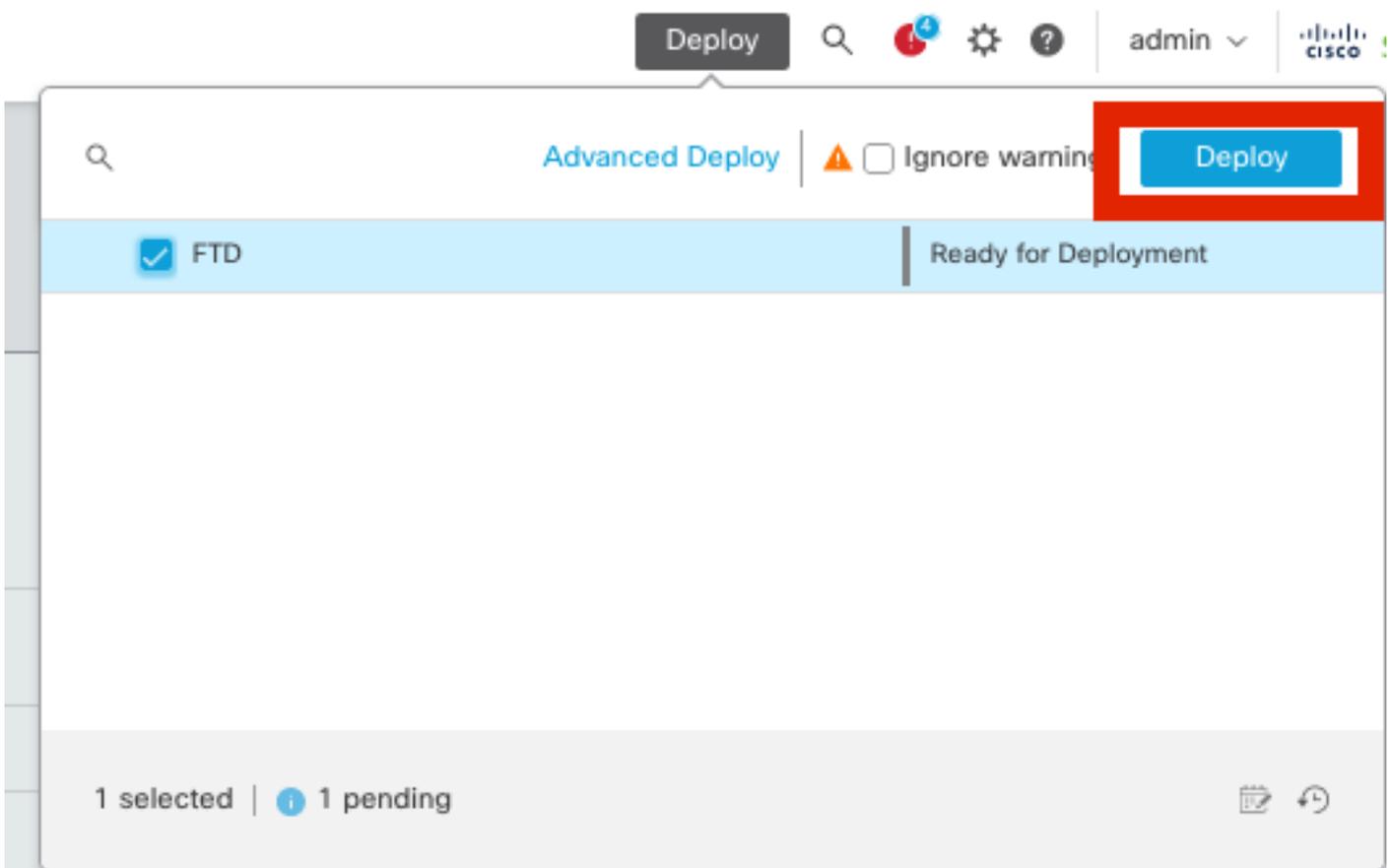
BGPネットワークの追加

ステップ 5：その他のBGP設定はすべてオプションであり、環境に応じて設定できます。設定を確認し、Saveをクリックします。



BGP設定の保存

手順 6：すべての設定を展開します。



導入

ASAでのオーバーレイBGPの設定

```
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
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

FTDの出力

```
<#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	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 (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 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: 169.254.2.2
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 NLRIs 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

ASAでの出力

<#root>

```
#show crypto ikev2 sa
```

```
IKEv2 SAs:
```

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

```
Tunnel-id   Local                               Remote                               fvrf/ivrf                               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 (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 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

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

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

- IPv4インターフェイスと、IPv4、保護されたネットワーク、またはVPNペイロードのみをサポートします (IPv6はサポートされません)。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。