

# Configurer un VPN site à site basé sur la route entre ASA et FTD

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configurer le VPN IPsec sur FTD à l'aide de FMC](#)

[Configurer l'interface de bouclage sur FTD en utilisant FMC](#)

[Configurer le VPN IPsec sur ASA](#)

[Configurer l'interface de bouclage sur ASA](#)

[Configurer le BGP de superposition sur FTD à l'aide de FMC](#)

[Configurer le protocole BGP de superposition sur ASA](#)

[Vérifier](#)

[Résultats sur FTD](#)

[Sorties sur ASA](#)

[Dépannage](#)

---

## Introduction

Ce document décrit comment configurer un tunnel VPN de site à site basé sur la route entre ASA et FTD par un FMC avec le routage dynamique BGP comme superposition.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base du VPN site à site IPsec
- Configurations BGP (Border Gateway Protocol) sur Firepower Threat Defense géré (FTD) et ASA (Adaptive Security Appliance)
- Expérience avec Firepower Management Center (FMC)

### Composants utilisés

- Cisco ASA v9.20(2)2

- Cisco FMC version 7.4.1
- Cisco FTD version 7.4.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Le VPN basé sur la route permet de déterminer le trafic intéressant à chiffrer, ou à envoyer sur un tunnel VPN, et utilise le routage du trafic au lieu de la politique/liste d'accès comme dans un VPN basé sur la politique ou la crypto-carte. Le domaine de chiffrement est configuré pour autoriser tout trafic qui entre dans le tunnel IPsec. Les sélecteurs de trafic local et distant IPsec sont définis sur 0.0.0.0/0.0.0.0. Tout trafic acheminé dans le tunnel IPsec est chiffré quel que soit le sous-réseau source/de destination.

Ce document se concentre sur la configuration de l'interface de tunnel virtuel statique (SVTI) avec le routage dynamique BGP comme superposition.

## Configurer

Cette section décrit la configuration requise sur l'ASA et le FTD pour activer la proximité BGP par le biais d'un tunnel IPSec SVTI.

### Diagramme du réseau

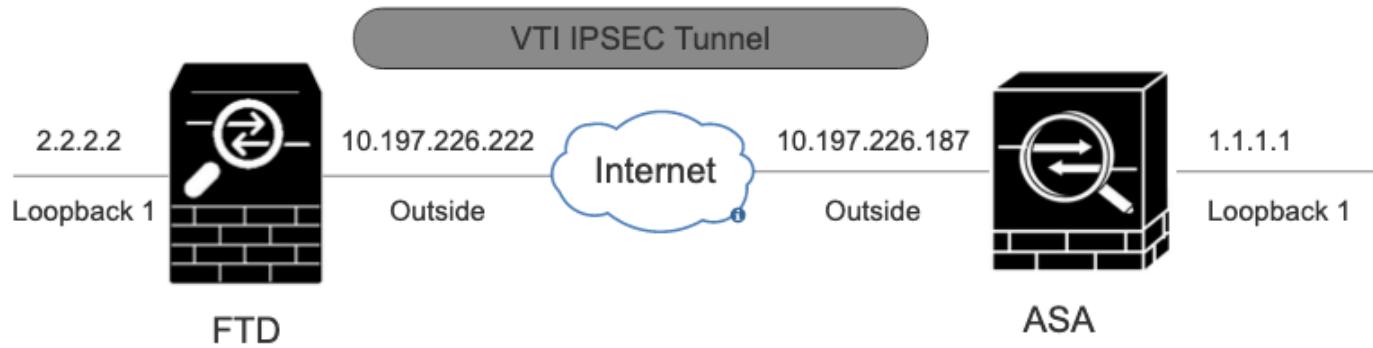


Diagramme du réseau

### Configurations

#### Configurer le VPN IPsec sur FTD à l'aide de FMC

Étape 1. Accédez à Devices > VPN > Site To Site.

Étape 2. Cliquez sur +Site to Site VPN.



VPN de site à site

Étape 3. Fournissez un **Topology Name** et sélectionnez le type de VPN comme **Route Based (VTI)**. Sélectionnez l'option **IKE Version**.

Pour cette démonstration :

- Nom de topologie : ASA-VTI
- Version IKE : IKEv2

Edit VPN Topology

Topology Name:\*

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:

Point to Point  Hub and Spoke  Full Mesh

IKE Version:\*

IKEv1  IKEv2

Topologie VPN

Étape 4. Choisissez le **Device** tunnel sur lequel le tunnel doit être configuré. Vous pouvez ajouter une nouvelle interface de tunnel virtuel (cliquez sur l'icône) ou en sélectionner une dans la liste existante.

## 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](#)

Noeud d'extrémité A

Étape 5. Définissez les paramètres du New Virtual Tunnel Interface. Cliquez sur ok.

Pour cette démonstration :

- Name : ASA-VTI
- Description (Facultatif) : Tunnel VTI avec Extranet ASA
- Zone de sécurité : Zone VTI
- ID de tunnel : 1
- Adresse IP: 169.254.2.1/24
- Source du tunnel : GigabitEthernet0/1 (externe)
- Mode tunnel 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

Étape 6.okCliquez sur la fenêtre contextuelle indiquant que la nouvelle interface VTI a été créée.

## Virtual Tunnel Interface Added

VTI has been created successfully.

Please go to the Device > Interfaces page to delete/update the VTI.

OK

Étape 7. Sélectionnez le VTI nouvellement créé ou un VTI sousVirtual Tunnel Interface. Fournissez les informations pour le noeud B (qui est le périphérique homologue).

Pour cette démonstration :

- Périphérique: Extranet
- Nom du périphérique: Homologue ASA
- Adresse IP du terminal : 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 (i)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

Noeud d'extrémité B



Étape 8. Accédez à l'onglet IKE. Cliquez sur

. Vous pouvez choisir d'utiliser un prédefiniPolicy ou cliquer sur le bouton + en regard de l'onglet Policy pour en créer un nouveau.

Étape 9. (Facultatif, si vous créez une nouvelle stratégie IKEv2.) Fournissez un Name pour la stratégie et sélectionnez les Algorithms à utiliser dans la stratégie. Cliquez sur Save.

Pour cette démonstration :

- Name : Stratégie ASA-V-IKEv2
- Algorithmes d'intégrité : SHA-256
- Algorithmes de chiffrement : AES-256
- Algorithmes PRF : SHA-256
- Groupe Diffie-Hellman : 14

## Edit IKEv2 Policy



Name:\*

ASAv-IKEv2-Policy

Description:

Priority: (1-65535)

1

Lifetime: seconds (120-2147483647)

86400

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

**IKEv2-Policy**

**Cancel** **Save**

Étape 10. Choisissez le nouveau Policy ou le Policy qui existe. Sélectionnez la Authentication Type. Si une clé manuelle pré-partagée est utilisée, entrez la clé dans la zone Key et Confirm Key .

Pour cette démonstration :

- Stratégie : ASAv-IKEv2-Policy
- Type d'authentification: Clé manuelle pré-partagée

### IKEv2 Settings

Policies:\*

Authentication Type:

Key:\*

Confirm Key:\*

Enforce hex-based pre-shared key only

Authentification

#### Étape 11. Accédez à l'IPsec onglet. Cliquer

Vous pouvez choisir d'utiliser une proposition IKEv2 IPsec prédéfinie ou d'en créer une nouvelle. Cliquez sur le bouton en regard de l'IKEv2 IPsec Proposal onglet.

Étape 12. (Facultatif, si vous créez une nouvelle proposition IKEv2 IPsec.) Saisissez un Name pour la proposition et sélectionnez les Algorithms à utiliser dans la proposition. Cliquez sur Save.

Pour cette démonstration :

- Name : Stratégie ASAv-IPSec
- Hachage ESP : SHA-256
- Cryptage ESP : AES-256

## New IKEv2 IPsec Proposal



Name:<sup>\*</sup>

Description:

### Available Algorithms

ESP Hash

ESP Encryption

SHA-512

SHA-384

SHA-256

SHA-1

MD5

NULL

Add

### Selected Algorithms

SHA-256



[Cancel](#)

[Save](#)

IKEv2-IPsec-Proposition

Étape 13. Choisissez la nouvelle **Proposal** ou **Proposal** celle qui existe dans la liste des propositions disponibles. Cliquez sur **OK**.

## IKEv2 IPsec Proposal



Available Transform Sets C +

Search

AES-256-SHA-256

Add

AES-GCM

AES-SHA

ASAv-IPSec-Policy

DES-SHA-1

Umbrella-AES-GCM-256

Selected Transform Sets

ASAv-IPSec-Policy



Cancel

OK

Jeu de transformation

Étape 14. (Facultatif) Choisissez les paramètres Perfect Forward Secrecy. Configurez IPsec Lifetime Duration and Lifetime Size.

Pour cette démonstration :

- Secret de transmission parfait : Groupe de modules 14
- Durée de vie : 28800 (Default)
- Durée de vie : 4608000 (Default)

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)

## Configuration de PFS

Étape 15. Vérifiez les paramètres configurés. Cliquez sur **Save**, comme illustré dans cette image.

Edit VPN Topology

Topology Name: **ASAv-vTI**

Policy Based (Crypto Map)  Route Based (vTI)

Network Topology: **Point to Point**

IKE Versions:  IKEv1  IKEv2

Endpoints    IKE    IPsec    Advanced

**Node A**

Device: **FTD**

Virtual Tunnel Interface: **ASAv-vTI (IP: 10.197.226.222)** [Edit VTI](#)  Tunnel Source IP is Private  Send Local Identity to Peers [Add Backup VTI \(optional\)](#)

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**

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

Enregistrement de la configuration

Configurer l'interface de bouclage sur FTD en utilisant FMC

Accédez à **Devices > Device Management**. Modifiez le périphérique sur lequel la boucle doit être configurée.

Étape 1. Accédez à **Interfaces > Add Interfaces > Loopback Interface**.

[Device](#) [Routing](#) [Interfaces](#) [Inline Sets](#) [DHCP](#) [VTEP](#)

[All Interfaces](#) [Virtual Tunnels](#)

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		10.197.224.227/23(Static)	Disabled	Global

[Search by name](#) [Sync Device](#) [Add Interfaces](#) [Loopback Interface](#)

Accédez à l'interface de bouclage

Étape 2. Entrez le nom « loopback », fournissez un ID de bouclage « 1 » et activez l'interface.

## Edit Loopback Interface



General

IPv4

IPv6

Name:

loopback

Enabled

Loopback ID:\*

1

(1-1024)

Description

Cancel

OK

Activation de l'interface de bouclage

Étape 3. Configurez l'adresse IP de l'interface, puis cliquez sur 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

Fournir une adresse IP à l'interface de bouclage

Configurer le VPN IPSec sur 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
```

## Configurer l'interface de bouclage sur ASA

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

## Configurer le BGP de superposition sur FTD à l'aide de FMC

Accédez à [Devices > Device Management](#). Éditez le périphérique sur lequel le tunnel VTI est configuré, puis accédez à [Routing > General Settings > BGP](#).

Étape 1 : activation du protocole BGP et configuration du numéro de système autonome (AS) et

de l'ID de routeur, comme illustré dans cette image

Le numéro de système autonome doit être le même sur les périphériques FTD et ASA.

L'ID de routeur est utilisé pour identifier chaque routeur participant au protocole BGP.

The screenshot shows the 'Manage Virtual Routers' interface under the 'Routing' tab. In the left sidebar, 'BGP' is selected. The main area shows the 'Global' configuration for BGP. A red box highlights the 'Enable BGP' checkbox and the 'AS Number' field (set to 1000). Other visible fields include 'Router Id' (set to 'Manual') and 'IP Address' (set to 10.1.1.1).

Naviguer pour configurer BGP

Étape 2. Accédez à BGP IPv4 et activez BGP > IPv4-le sur le FTD.

The screenshot shows the 'Manage Virtual Routers' interface under the 'Routing' tab. In the left sidebar, 'IPv4' is selected. The main area shows the 'Global' configuration for IPv4. A red box highlights the 'Enable IPv4' checkbox and the 'AS Number' field (set to 1000). Other visible tabs include 'General', 'Neighbor', 'Add Aggregate Address', 'Filtration', 'Networks', 'Redistribution', and 'Route Injection'. The 'General' tab is currently selected.

Activer BGP

Étape 3. Sous l'onglet Neighbor, ajoutez l'adresse IP du tunnel ASA VTI en tant que voisin et activez le voisin.

The screenshot shows the 'Manage Virtual Routers' interface under the 'Routing' tab. In the left sidebar, 'BGP' is selected. The main area shows the 'Global' configuration for BGP. A red box highlights the 'Neighbor' tab and the 'Add' button in the top right corner of the neighbor configuration table. The table shows one existing neighbor entry: 'Address' (169.254.2.2), 'Remote AS Number' (1000), 'Address Family' (Enabled), and 'Remote Private AS Number' (empty).

Ajouter un voisin BGP

Étape 4. Sous Networks, ajoutez les réseaux que vous voulez annoncer via BGP qui doivent passer par le tunnel VTI, dans ce cas, loopback1.

The screenshot shows the 'Manage Virtual Routers' section under the 'Routing' tab. A red box highlights the 'Networks' tab, which contains a table with one row: '2.2.2.0'. The 'RouteMap' column is empty.

Ajouter des réseaux BGP

Étape 5. Tous les autres paramètres BGP sont facultatifs et vous pouvez les configurer en fonction de votre environnement. Vérifiez la configuration et cliquez sur save.

The screenshot shows the same 'Manage Virtual Routers' interface. The 'Save' button at the top right is highlighted with a red box. The table in the 'Networks' tab now has two rows: '2.2.2.0' and '3.3.3.0'.

Enregistrer la configuration BGP

Étape 6 : déploiement de toutes les configurations

The screenshot shows the deployment interface. At the top, there's a 'Deploy' button, a search icon, and a notification badge with '4'. Below that is a toolbar with icons for search, settings, and help, followed by the user 'admin'. On the right is the Cisco logo. The main area has tabs for 'Advanced Deploy' (highlighted with a red box) and 'Ignore warning'. A large blue button labeled 'Deploy' is also highlighted with a red box. On the left, there's a checkbox for 'FTD' which is checked. To the right, it says 'Ready for Deployment'. At the bottom, it shows '1 selected | 1 pending' with a calendar and refresh icon.

Déploiement

Configurer le protocole BGP de superposition sur 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

```

## Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

### Résultats sur FTD

<#root>

```
#show crypto ikev2 sa
```

IKEv2 SAs:

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

Tunnel-id	Local	Remote	fvrf/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: 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
```

## Sorties sur ASA

```
<#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
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 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 NLRIIs 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

```

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

```

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

```

- Prend en charge uniquement les interfaces IPv4, ainsi que IPv4, les réseaux protégés ou les données utiles VPN (pas de prise en charge d'IPv6).

## À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.