

Configurazione della VPN da sito a sito basata su route tra ASA e FTD con BGP come overlay

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurare la VPN IPSec su FTD tramite FMC](#)

[Configurazione dell'interfaccia di loopback su FTD mediante FMC](#)

[Configurazione della VPN IPSec sull'appliance ASA](#)

[Configurazione dell'interfaccia di loopback sull'appliance ASA](#)

[Configurare l'overlay di BGP su FTD tramite FMC](#)

[Configurazione dell'overlay di BGP sull'appliance ASA](#)

[Verifica](#)

[Output su FTD](#)

[Output sull'appliance ASA](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare un tunnel VPN da sito a sito basato su percorso tra Adaptive Security Appliance (ASA) e Firepower Threat Defense gestito (FTD) da un Firepower Management Center (FMC) con routing dinamico Border Gateway Protocol (BGP) come sovrapposizione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base della VPN da sito a sito IPsec
- Configurazioni BGP su FTD e ASA
- Esperienza con FMC

Componenti usati

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

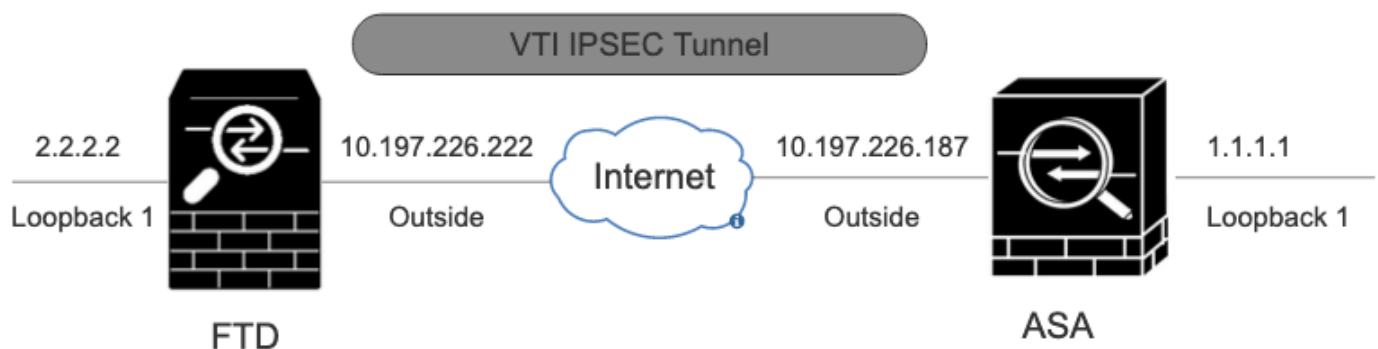
La VPN basata sulla route consente di determinare se il traffico è da crittografare o inviare su un tunnel VPN e utilizza il routing del traffico anziché un elenco di policy o di accesso, come avviene per le VPN basate su policy o su mappa crittografica. Il dominio di crittografia è impostato per consentire tutto il traffico in entrata nel tunnel IPsec. I selettori di traffico locale e remoto IPsec sono impostati su 0.0.0.0/0.0.0.0. Il traffico indirizzato nel tunnel IPsec viene crittografato indipendentemente dalla subnet di origine/destinazione.

Nel documento si fa riferimento alla configurazione SVTI (Static Virtual Tunnel Interface) con routing dinamico BGP come overlay.

Configurazione

In questa sezione viene descritta la configurazione necessaria sull'appliance ASA e sull'FTD per configurare il protocollo BGP adiacente tramite un tunnel IPsec SVTI.

Esempio di rete



Esempio di rete

Configurazioni

Configurare la VPN IPsec su FTD tramite FMC

Passaggio 1. Passare a [Devices > VPN > Site To Site](#) .

Passaggio 2. Fare clic su [+Site to Site VPN](#) .



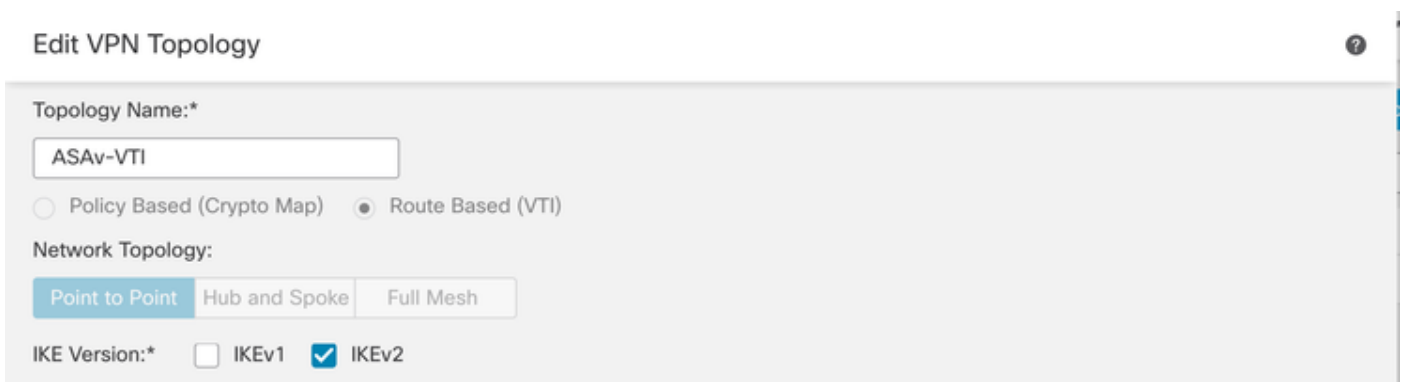
VPN da sito a sito

Passaggio 3. Fornire un Topology Name nome e selezionare il Tipo di VPN come Route Based (VTI). Scegliere il IKE Version.

Per questa dimostrazione:

Nome topologia: ASAv-VTI

Versione IKE: IKEv2



VPN-Topology

Passaggio 4. Scegliere Device il tunnel da configurare. È possibile aggiungere una nuova interfaccia del tunnel virtuale (fare clic sull'+ icona) o selezionarne una dall'elenco esistente.

Node A

Device:*

Virtual Tunnel Interface:*



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

Send Local Identity to Peers

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

▶ Advanced Settings

Nodo endpoint A

Passaggio 5. Definite i parametri di New Virtual Tunnel Interface. Fare clic su .Ok

Per questa dimostrazione:

Nome: ASA-VTI

Descrizione (Facoltativa): tunnel VTI con ASA Extranet

Area di sicurezza: VTI-Zone

ID tunnel: 1

Indirizzo IP: 169.254.2.1/24

Origine tunnel: Gigabit Ethernet 0/1 (esterna)

Modalità 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

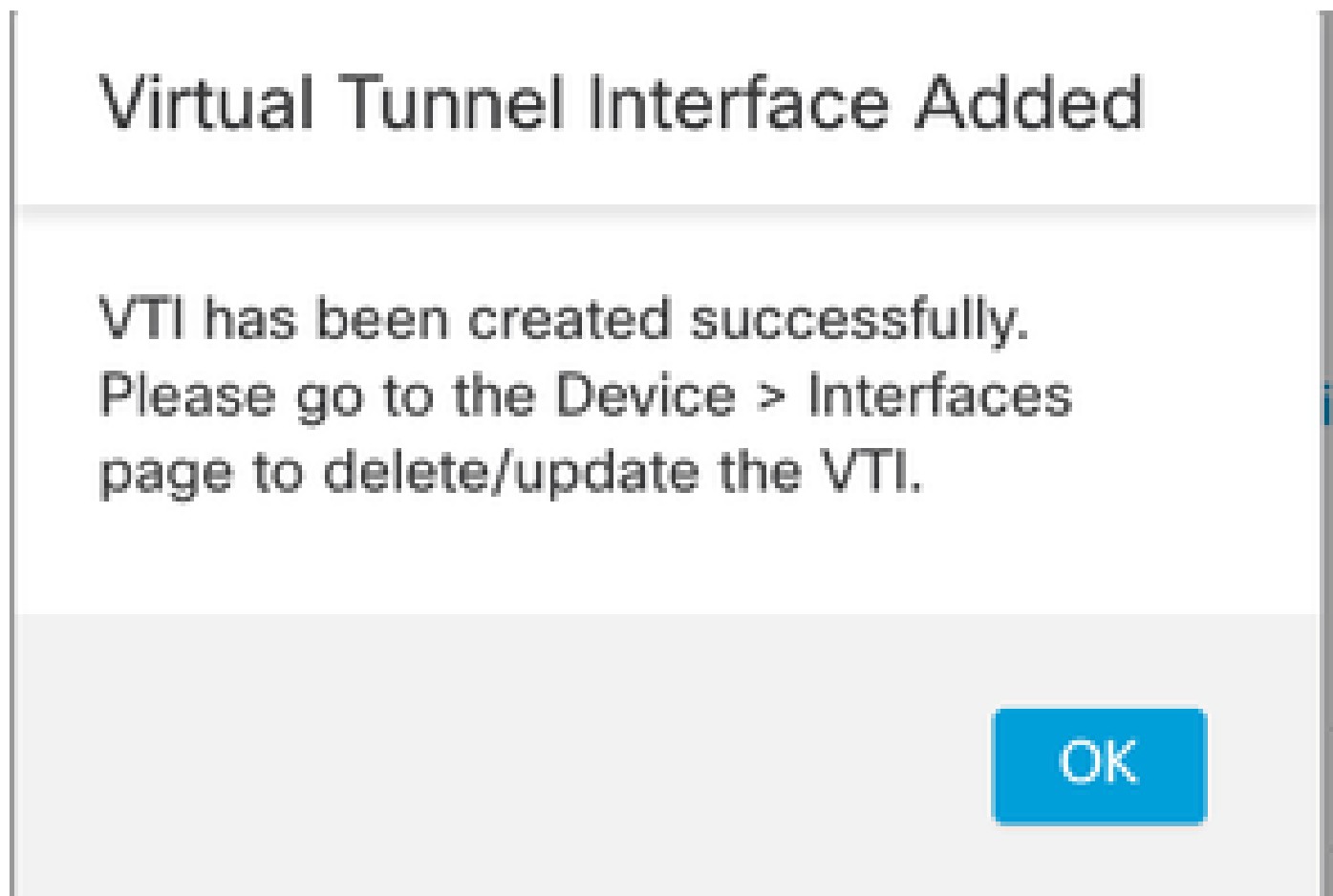
Borrow IP (IP unnumbered)

Loopback1 (loopback)

Cancel

OK

Passaggio 6. Fare OK clic sul menu a comparsa per indicare che la nuova VTI è stata creata.



Passaggio 7. Scegliere la VTI appena creata o una VTI in Virtual Tunnel Interface. Fornire le informazioni per il nodo B (che è il dispositivo peer).

Per questa dimostrazione:

Dispositivo: Extranet

Nome dispositivo: ASAv-Peer

Indirizzo IP 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

Nodo endpoint B



Passaggio 8. Passare alla scheda **IKE**. Fare clic su

. È possibile scegliere di utilizzare un predefinito Policy o fare clic sul +pulsante accanto alla Policyscheda per crearne uno nuovo.

Passaggio 9. (Facoltativo, se si crea un nuovo criterio IKEv2.) Fornire un Namenome per il criterio e selezionare quello Algorithms da utilizzare nel criterio. Fare clic su .Save

Per questa dimostrazione:

Nome: ASAv-IKEv2-policy

Algoritmi di integrità: SHA-256

Algoritmi di crittografia: AES-256

Algoritmi PRF: SHA-256

Gruppo 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

Criteria IKEv2

Passaggio 10. Scegliere il file appena creato Policy o Policyquello esistente. Selezionare la Authentication Type voce. Key Se si utilizza una chiave manuale già condivisa, immettere la chiave nella Confirm Key casella e.

Per questa dimostrazione:

Criterio: ASAv-IKEv2-Policy

Tipo di autenticazione: chiave manuale già condivisa

IKEv2 Settings

Policies:*

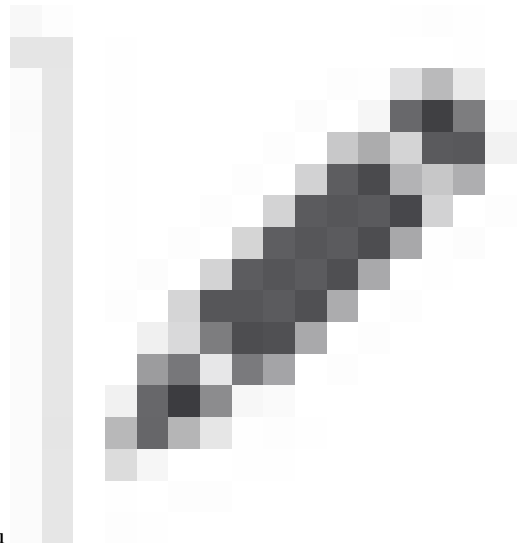
Authentication Type:


Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Autenticazione



Passaggio 11. Passare alla IPsec scheda. Fare clic su . Può scegliere se utilizzare una proposta IPsec IKEv2 predefinita o crearne una nuova. Fare clic sul + pulsante accanto alla IKEv2 IPsec Proposal scheda.

Passaggio 12. (Facoltativo, se si crea una nuova proposta IPsec IKEv2.) Immettere un valore Name per la proposta e selezionare quello Algorithms da utilizzare nella proposta. Fare clic su .Save

Per questa dimostrazione:

Nome: ASAv-IPSec-Policy

Hash ESP: SHA-256

Crittografia 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

Proposta IKEv2-IPsec

Passaggio 13. Scegliere la nuova proposta creata Proposal o Proposalquella esistente dall'elenco delle proposte disponibili. Fare clic su .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

Set di trasformazioni

Passaggio 14. (Facoltativo) Scegliere le Perfect Forward Secrecy impostazioni. Configurare IPSecLifetime Duration and Lifetime Size.



Per questa dimostrazione:

Perfect Forward Secrecy: Gruppo di moduli 14

Durata: 28800 (predefinita)

Dimensione durata: 4608000 (predefinita)

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)

Passaggio 15. Controllare le impostazioni configurate. Fare clic su Save, come mostrato nell'immagine.

Edit VPN Topology

Topology Name:*
ASAw-VTI

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:
 Point to Point Hub and Spoke Full Mesh

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

Cancel Save

Salvataggio della configurazione

Configurazione dell'interfaccia di loopback su FTD mediante FMC

Passare a Devices > Device Management . Modificare il dispositivo in cui è necessario configurare il loopback.

Passaggio 1. Andare su Interfaces > Add Interfaces > Loopback Interface .

Device Routing **Interfaces** Inline Sets DHCP VTEP

All Interfaces Virtual Tunnels

Search by name Sync Device

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GlobalEthernet0/0	inside	Physical	Inside		10.197.224.227(2)(Static)	Disabled	Global

Add Interfaces +

- Redundant Interface
- Bridge Group Interface
- Loopback Interface

Passa all'interfaccia di loopback

Passaggio 2. Immettere il nome "loopback", fornire un ID loopback "1" e abilitare l'interfaccia.

Edit Loopback Interface



General

IPv4

IPv6

Name:

loopback

Enabled

Loopback ID:*

1

(1-1024)

Description

Cancel

OK

Abilitazione dell'interfaccia di loopback

Passaggio 3. Configurare l'indirizzo IP per l'interfaccia, quindi fare clic su 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

Specificare l'indirizzo IP per l'interfaccia di loopback

Configurazione della VPN IPsec sull'appliance 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
```

Configurazione dell'interfaccia di loopback sull'appliance ASA

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

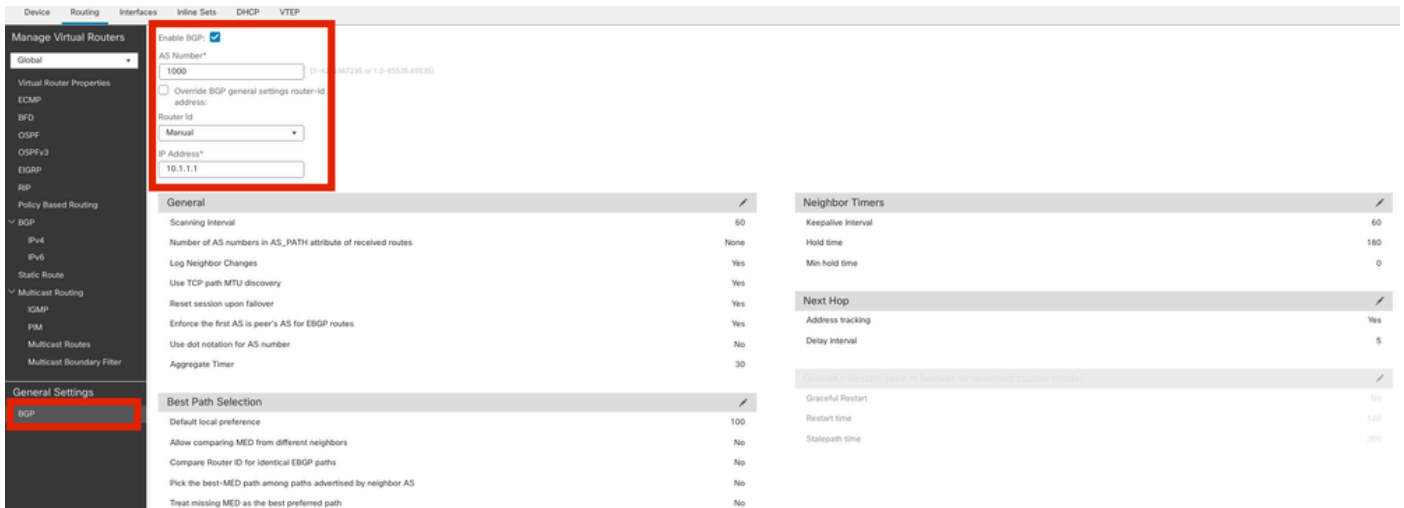
Configurare l'overlay di BGP su FTD tramite FMC

Passare a Devices > Device Management. Edit il dispositivo su cui è configurato il tunnel VTI, quindi passare a Routing > General Settings > BGP.

Passaggio 1. Abilitare BGP e configurare il numero AS (Autonomous System) e l'ID del router, come mostrato in questa immagine.

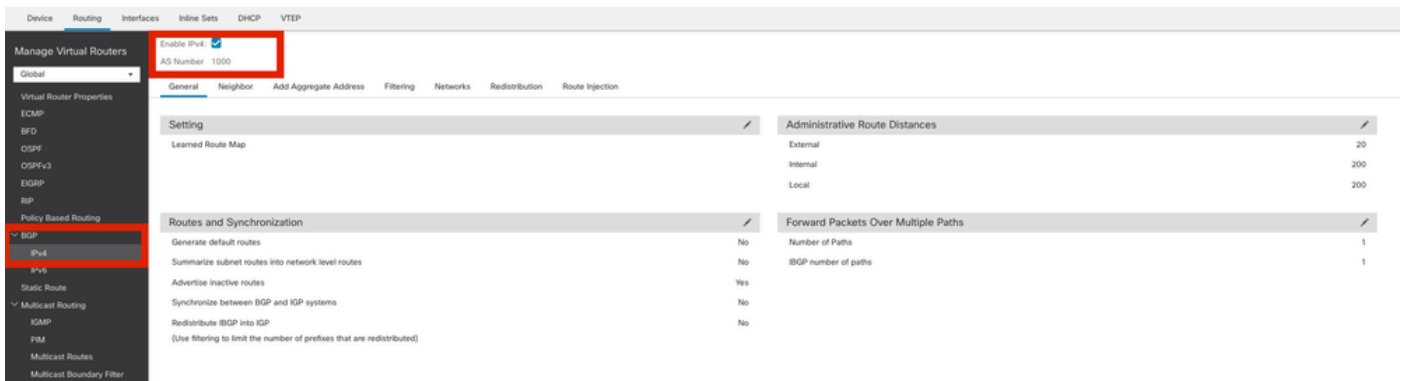
Il numero AS deve essere lo stesso su entrambi i dispositivi FTD e ASA.

L'ID del router viene usato per identificare ciascun router che partecipa al BGP.



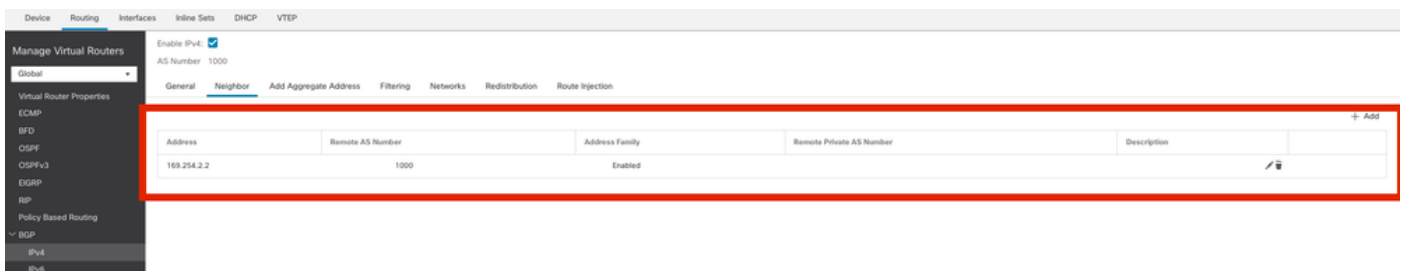
Passare alla configurazione di BGP

Passaggio 2. Passare BGP > IPv4 a BGP IPv4 su FTD e abilitarlo.



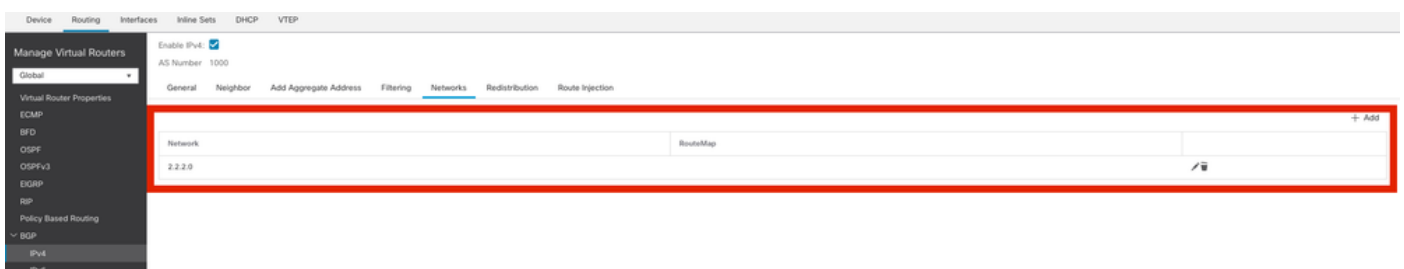
Abilita BGP

Passaggio 3. Nella Neighbor scheda, aggiungere l'indirizzo IP del tunnel VTI ASAv come router adiacente e abilitare il router adiacente.



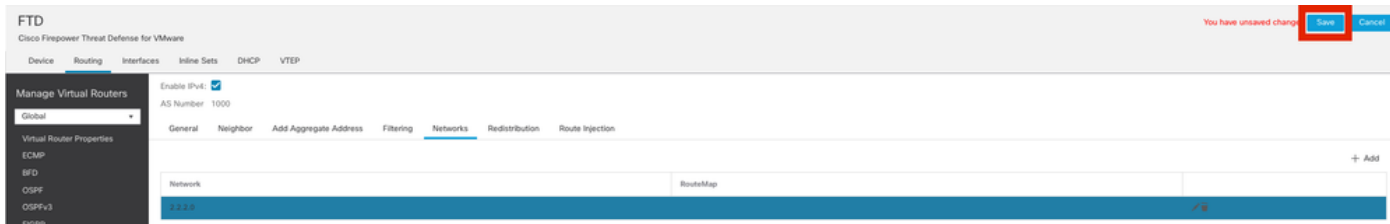
Aggiungi BGP adiacente

Passaggio 4. In Networks aggiungere le reti che si desidera annunciare tramite BGP che devono passare attraverso il tunnel VTI, in questo caso loopback1.



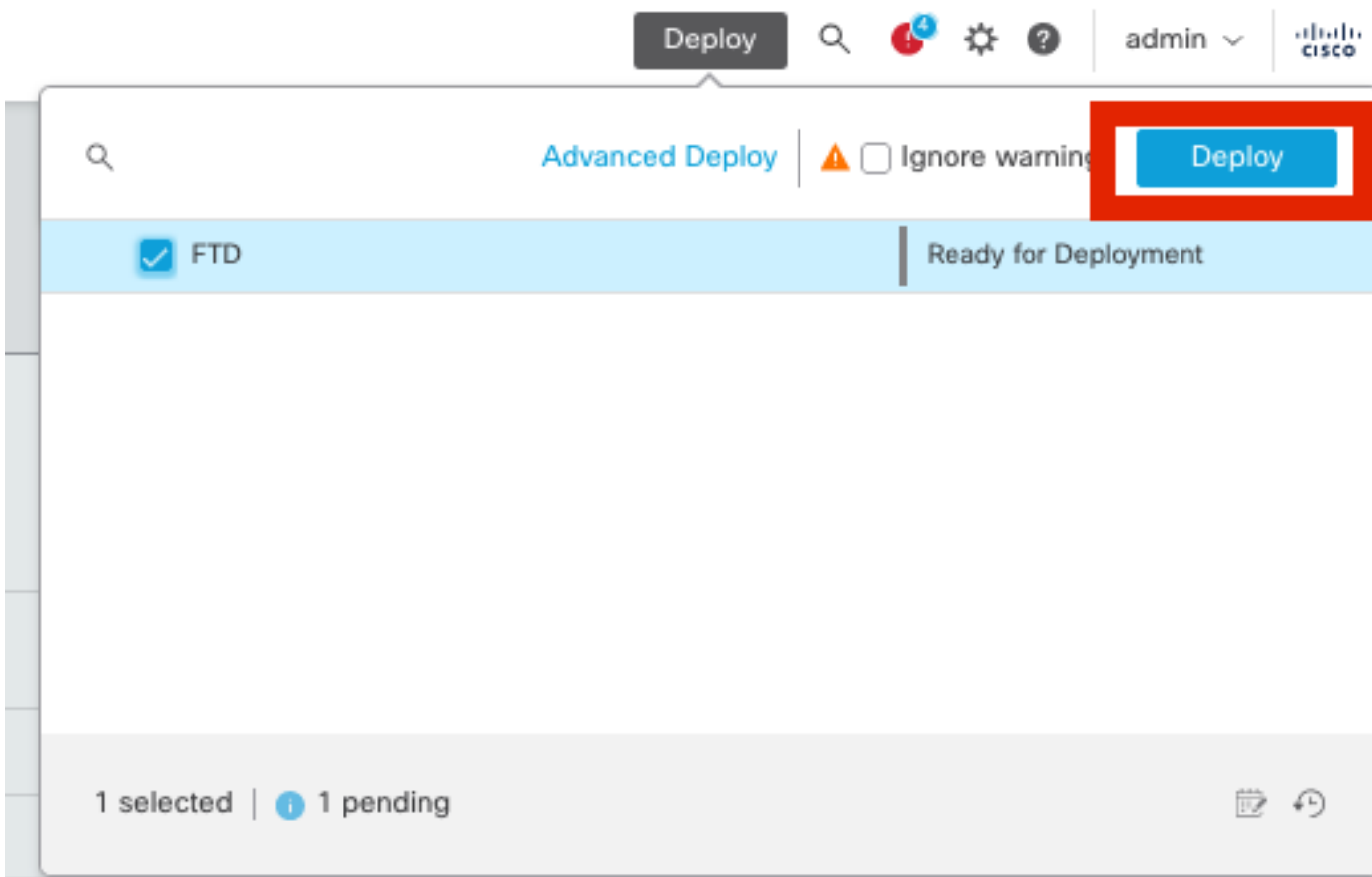
Aggiungi reti BGP

Passaggio 5. Tutte le altre impostazioni BGP sono facoltative ed è possibile configurarle in base all'ambiente. Verificare la configurazione e fare clic su Save.



Salva configurazione BGP

Passaggio 6. distribuire tutte le configurazioni.



Implementazione

Configurazione dell'overlay di BGP sull'appliance 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
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Output su 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 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

Output sull'appliance 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

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

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

- Supporta solo interfacce IPv4, IPv4, reti protette o payload VPN (nessun supporto per IPv6).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).