Configurazione di Secure Access con Secure FTD e ASA per l'accesso privato con NAT

Sommario

Introduzione

In questo documento viene descritto come configurare il gruppo di tunnel di rete ad accesso sicuro con Network Address Translation.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Firewall Management Center
- Cisco Secure Firewall Threat Defense
- Cisco Secure Access

- Cisco Adaptive Security Appliance
- Network Address Translation
- Policy Based Routing
- Acquisizioni pacchetti sul firewall

Componenti usati

Le informazioni fornite in questo documento si basano su:

- Cisco Firewall Management Center 7.10
- Cisco Secure Firewall Threat Defense 7.10
- Cisco Secure Access
- Cisco Adaptive Security Appliance 9.2
- Router Cisco

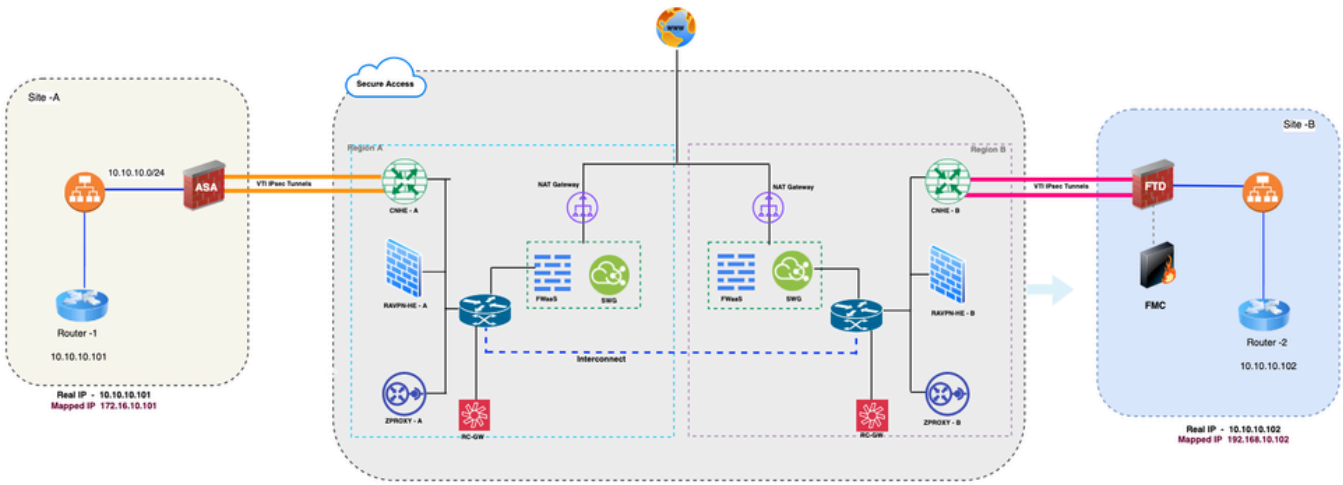
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Premesse

Cisco Secure Access offre funzionalità Secure Service Edge native del cloud, tra cui Secure Internet Access (SIA) e Secure Private Access (SPA). Per le organizzazioni che estendono l'accesso alle applicazioni private a utenti remoti senza sottoporre a backhaul tutto il traffico attraverso un centro dati, Secure Access utilizza i gruppi di tunnel di rete (NTG) IPsec per creare tunnel crittografati tra i dispositivi di rete locali, ad esempio Cisco Firewall Threat Defense (FTD), Adaptive Security Appliance (ASA) e i punti di presenza (PoP) del cloud Cisco Secure Access.

In questo documento viene descritto come stabilire un tunnel IPsec basato su routing utilizzando il protocollo IKEv2 tra Cisco FTD, ASA e Cisco Secure Access, in modo da abilitare Network Address Translation (NAT) su Secure Access e Policy-Based Routing (PBR) su FTD e ASA per indirizzare nel tunnel solo il traffico con accesso privato.

Esempio di rete



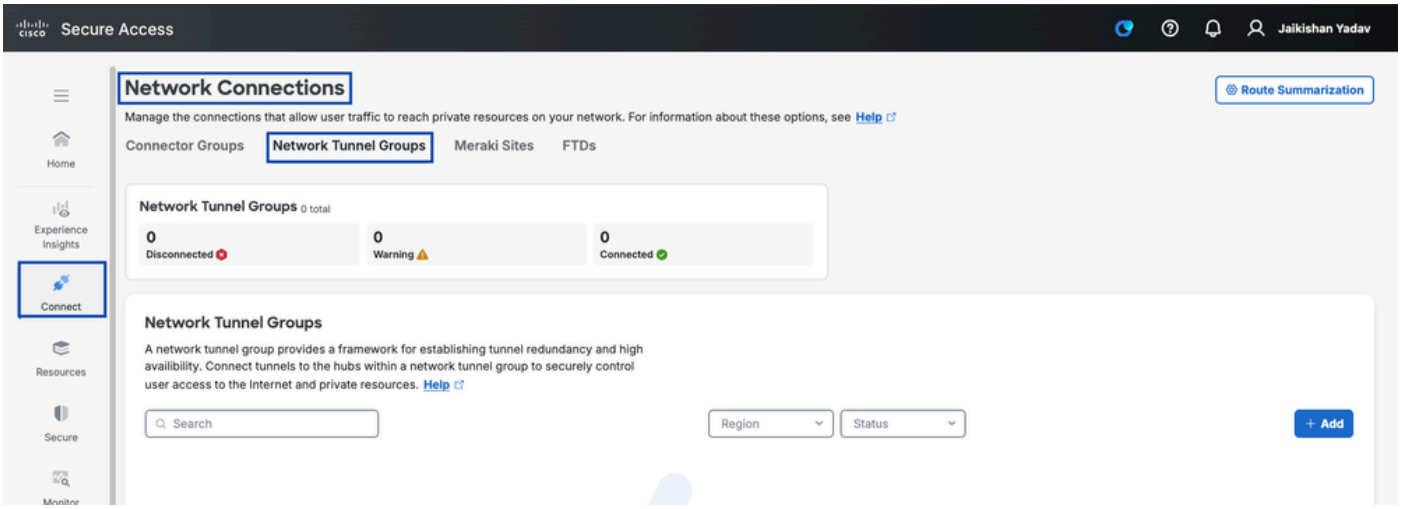
Topologia della rete

Configurazione

Secure Access e Secure Firewall Thread Defense - VPN dinamica (BGP) basata su route con PBR

Configura Network Tunnel Group su accesso protetto

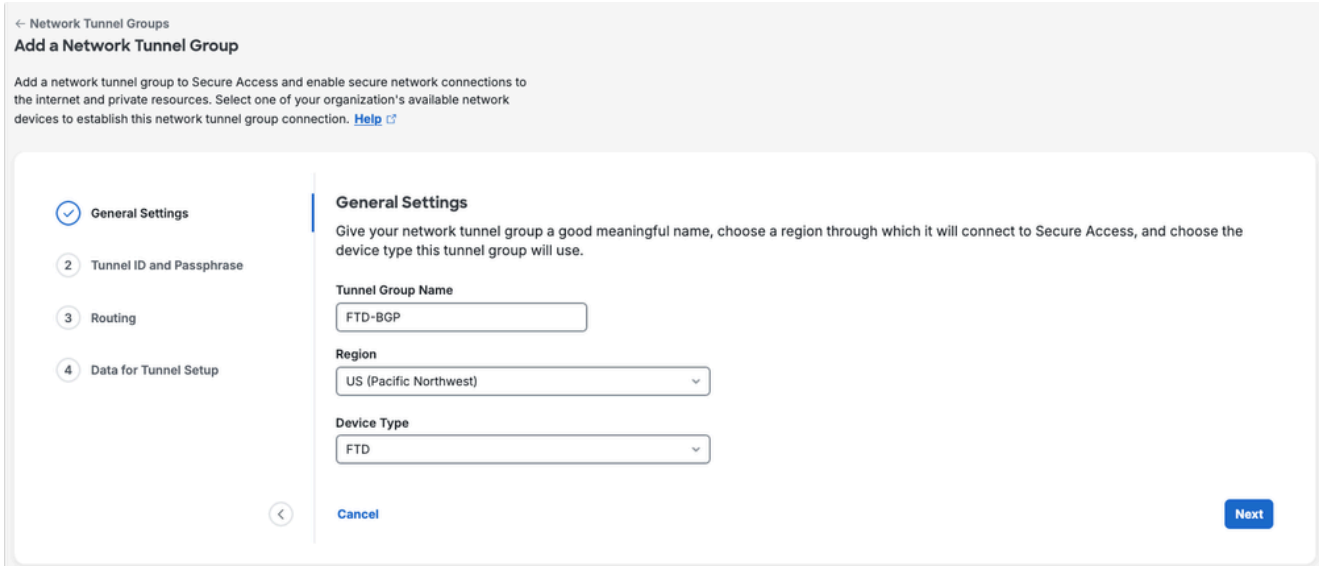
1. Accesso al dashboard Accesso sicuro Accesso sicuro
2. Passare a Connetti > Connessioni di rete > Gruppi di tunnel di rete e fare clic su +Aggiungi per configurare il gruppo di tunnel di rete



Accesso sicuro - Gruppi di tunnel di rete

3. Configurare il gruppo di tunnel di rete - Impostazioni generali

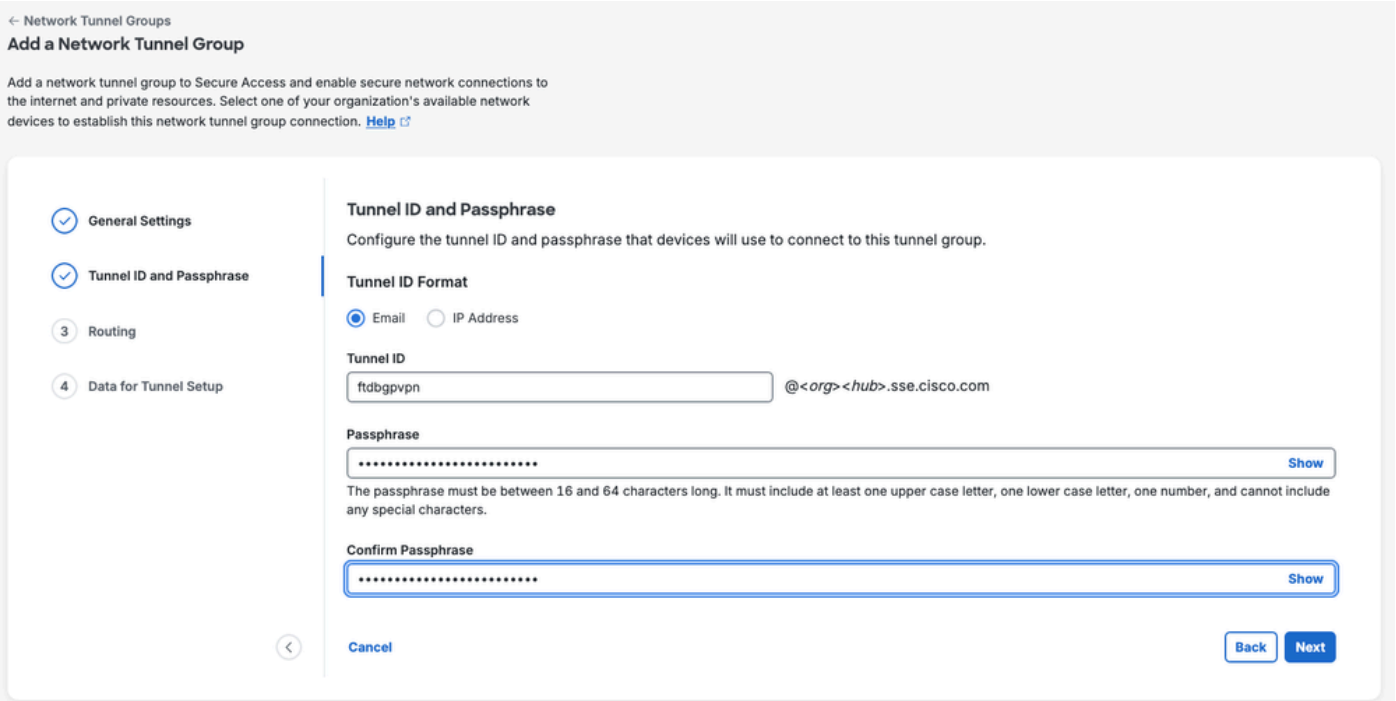
- Configura nome gruppo tunnel, area e tipo di dispositivo
- Fare clic su Avanti.



Accesso sicuro - Impostazioni generali gruppi tunnel di rete

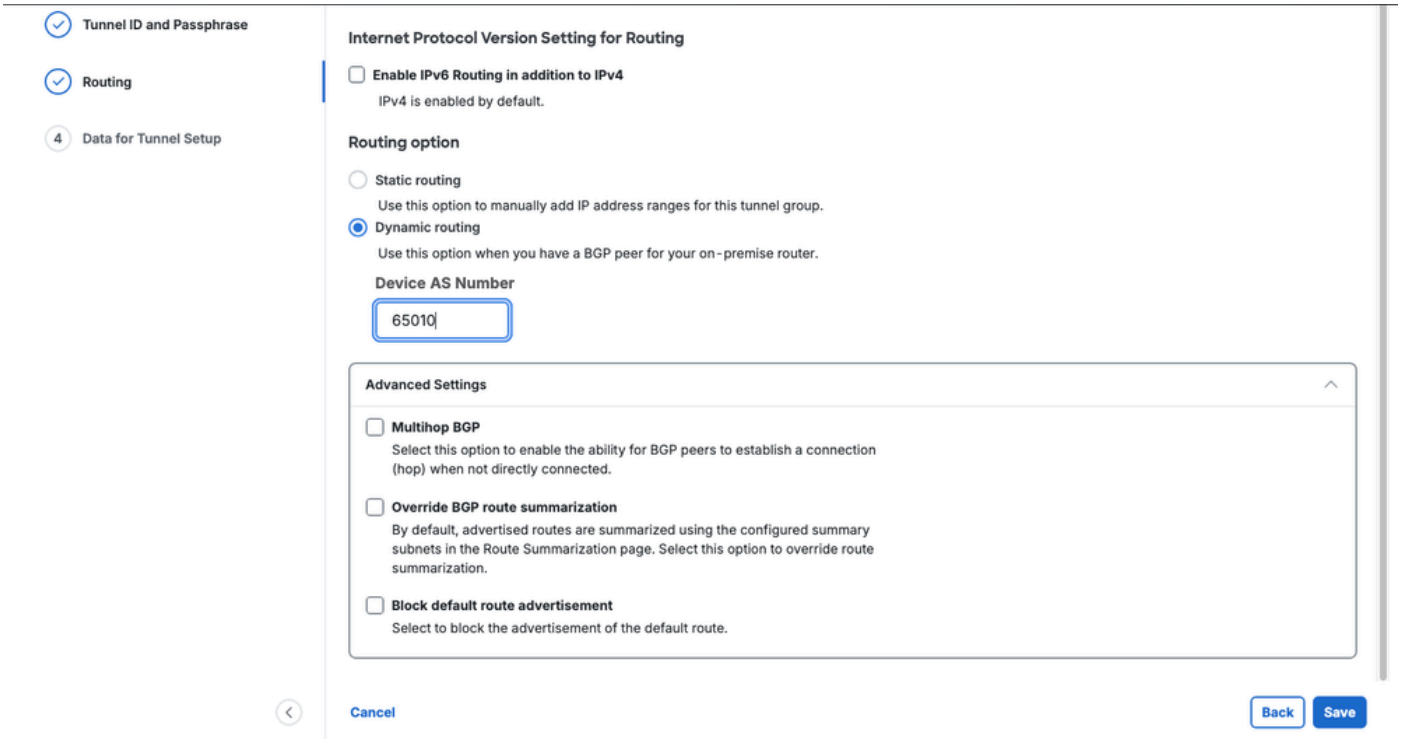
4. Configurare l'ID tunnel e la passphrase.

- Configurare l'ID del tunnel e la passphrase.
- Fare clic su Avanti

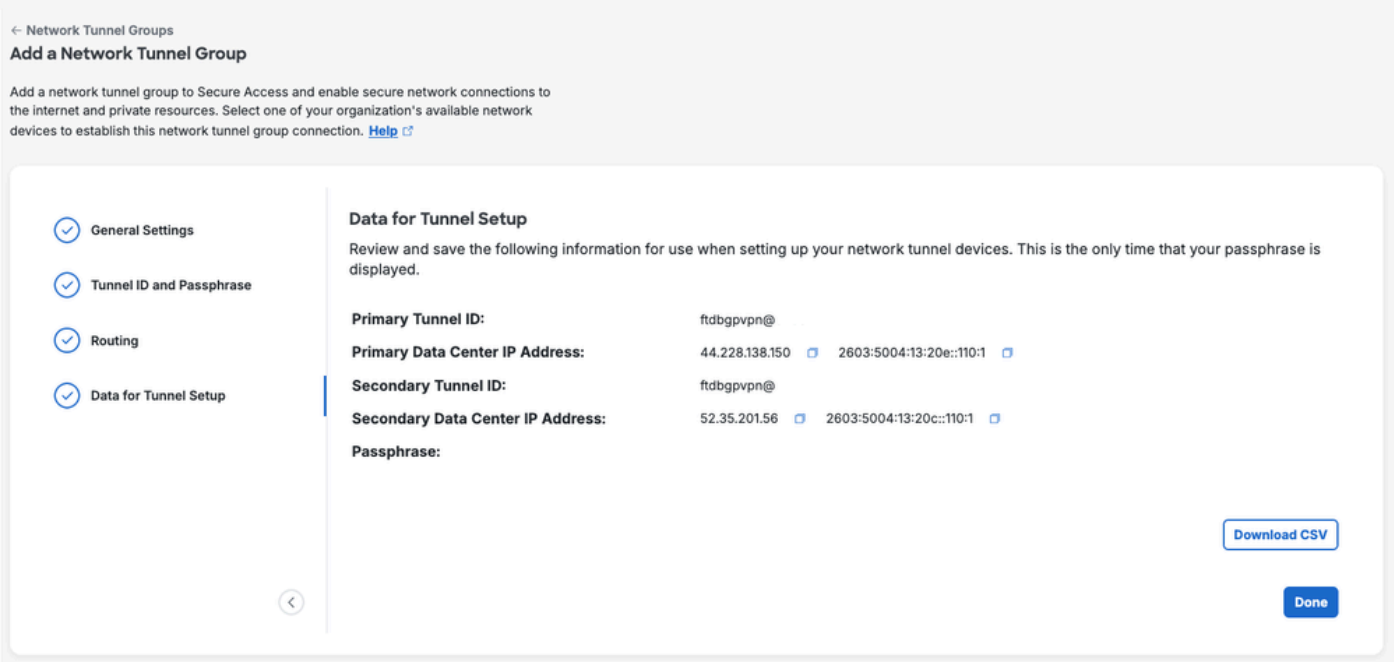


5. Configurare il routing

- Configura numero AS dispositivo
- Fare clic su Salva.



6. Salvataggio della configurazione di un gruppo di tunnel di rete



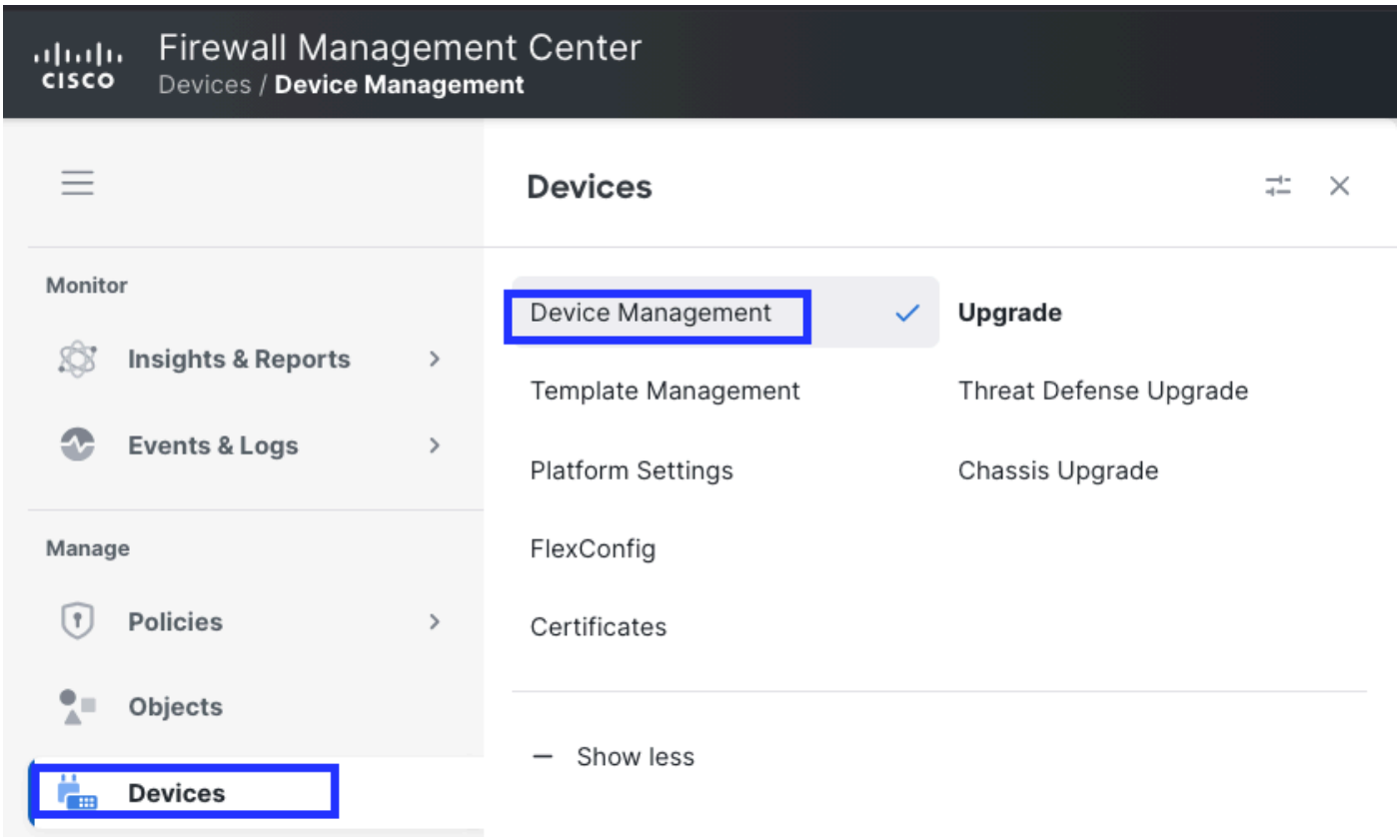
Accesso sicuro - Gruppi di tunnel di rete

Configurare la VPN IPsec basata su route dinamica su Secure Firewall Threat Defense (FTD) con PBR

1. Accedere a Centro gestione firewall (FMC)

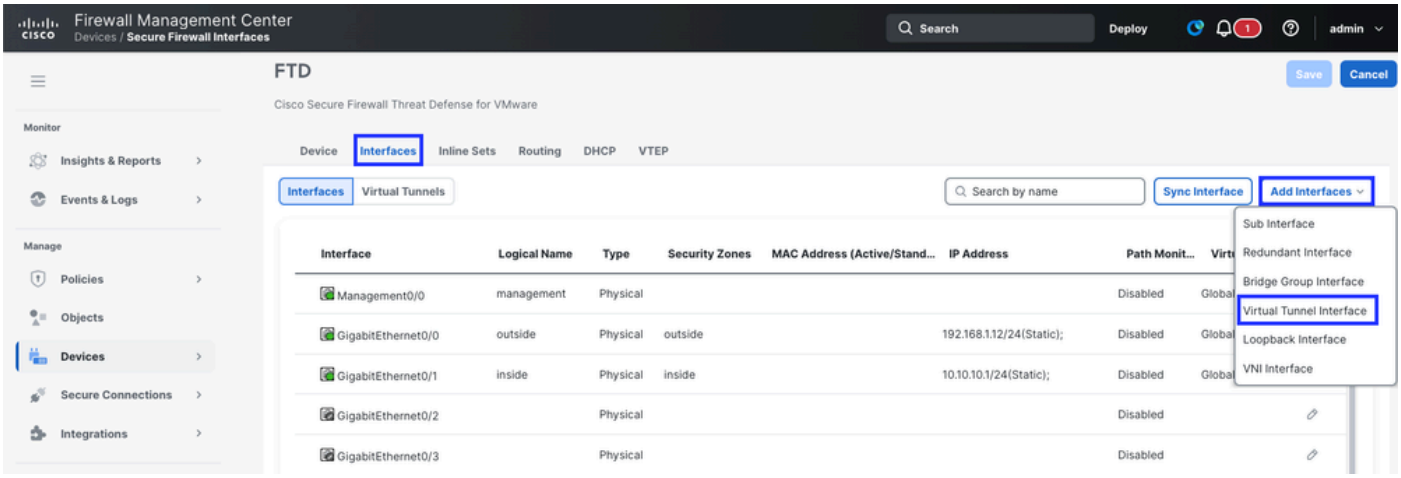
2. Configurare la VTI Virtual Tunnel Interface

- Selezionare Dispositivi > Gestione dispositivi



Gestione protetta dei firewall - Dashboard

- Fare clic sull'icona a forma di matita accanto al dispositivo e passare alla sezione Interface (Interfaccia)
- Fare clic su Add interfaces (Aggiungi interfacce), quindi selezionare Virtual Tunnel Interface (Interfaccia tunnel virtuale)



Gestione protetta dei firewall - Configurazione VTI FTD

- Configurazione VTI

Add Virtual Tunnel Interface

General | Path Monitoring

Tunnel Type

(•) Static ( ) Dynamic

Name:*

VTI-1

[x] Enabled

Description:

Virtual Tunnel interface for Primary VTI VPN

Security Zone:

vti

Priority:

0 *(0 - 65535)*

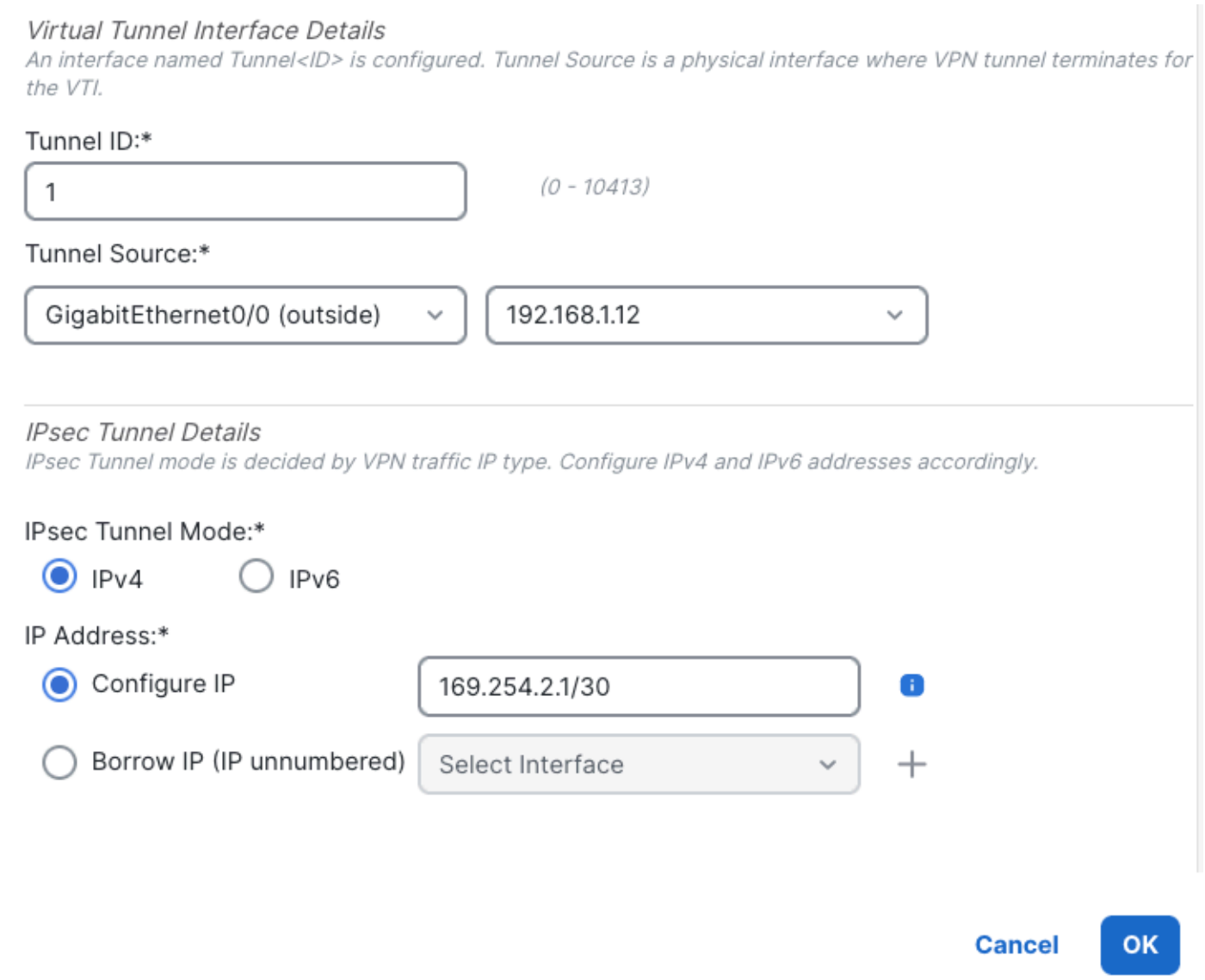
Propagate Security Group Tag: [x]

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

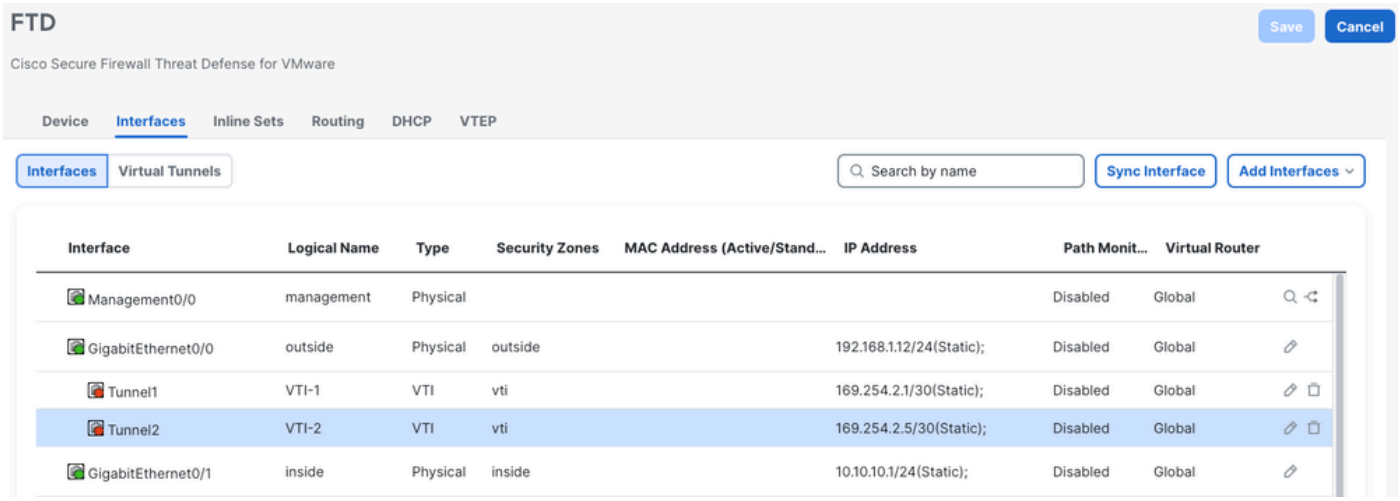
Tunnel ID:*

1 *(0 - 10413)*

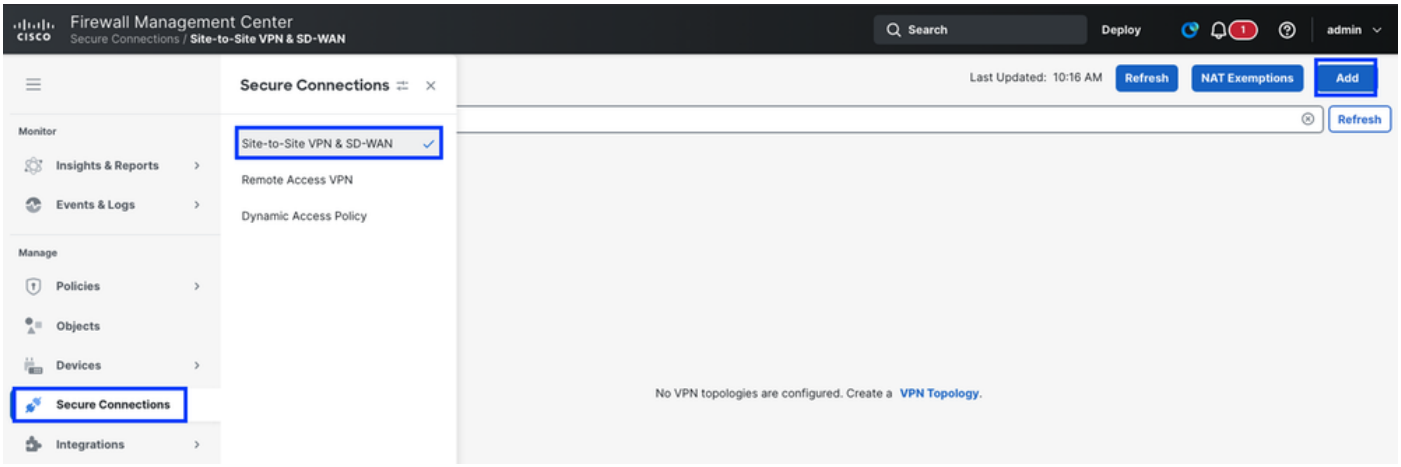


Gestione protetta dei firewall - Configurazione VTI FTD

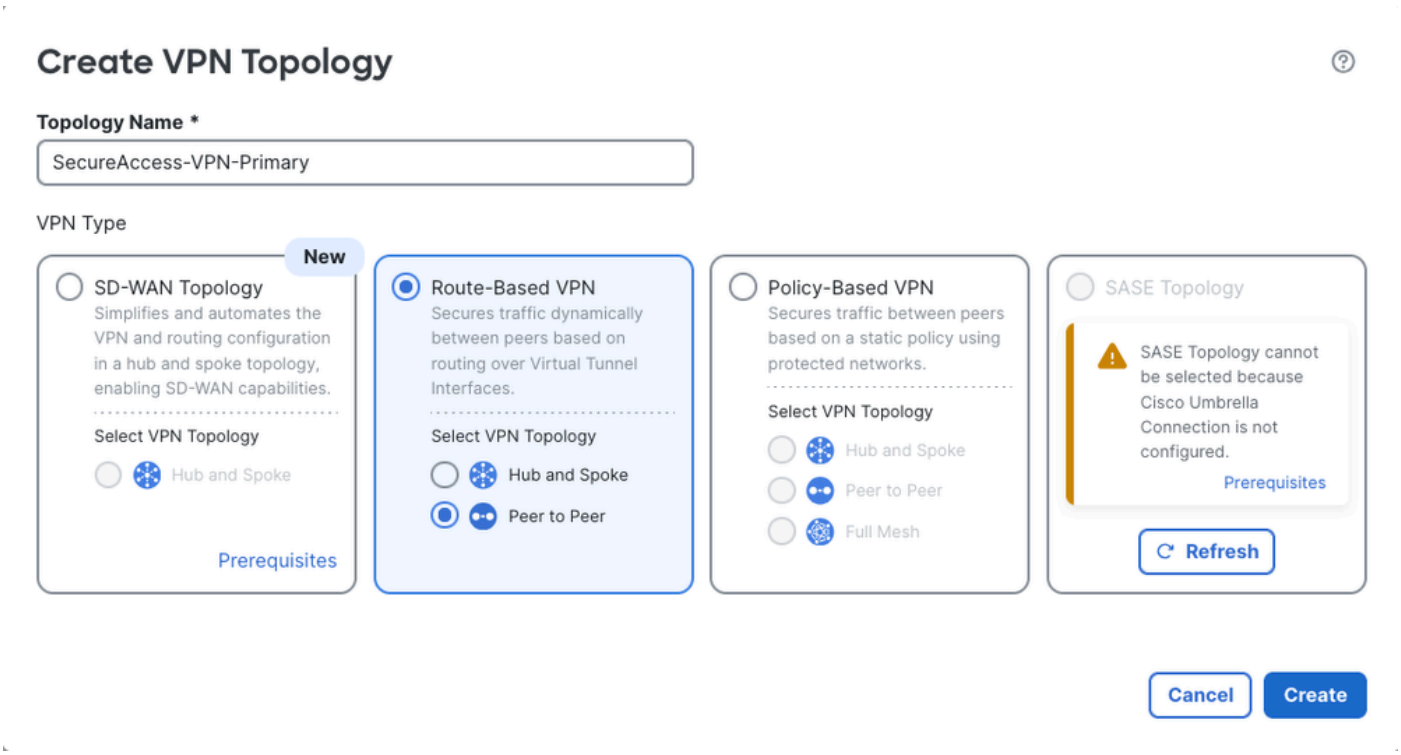
- Configurare anche VTI-2 per la VPN IPsec secondaria con accesso sicuro



3. Selezionare Secure Connections > Site-to-Site VPN & SD-WAN e fare clic su Add per configurare la VPN



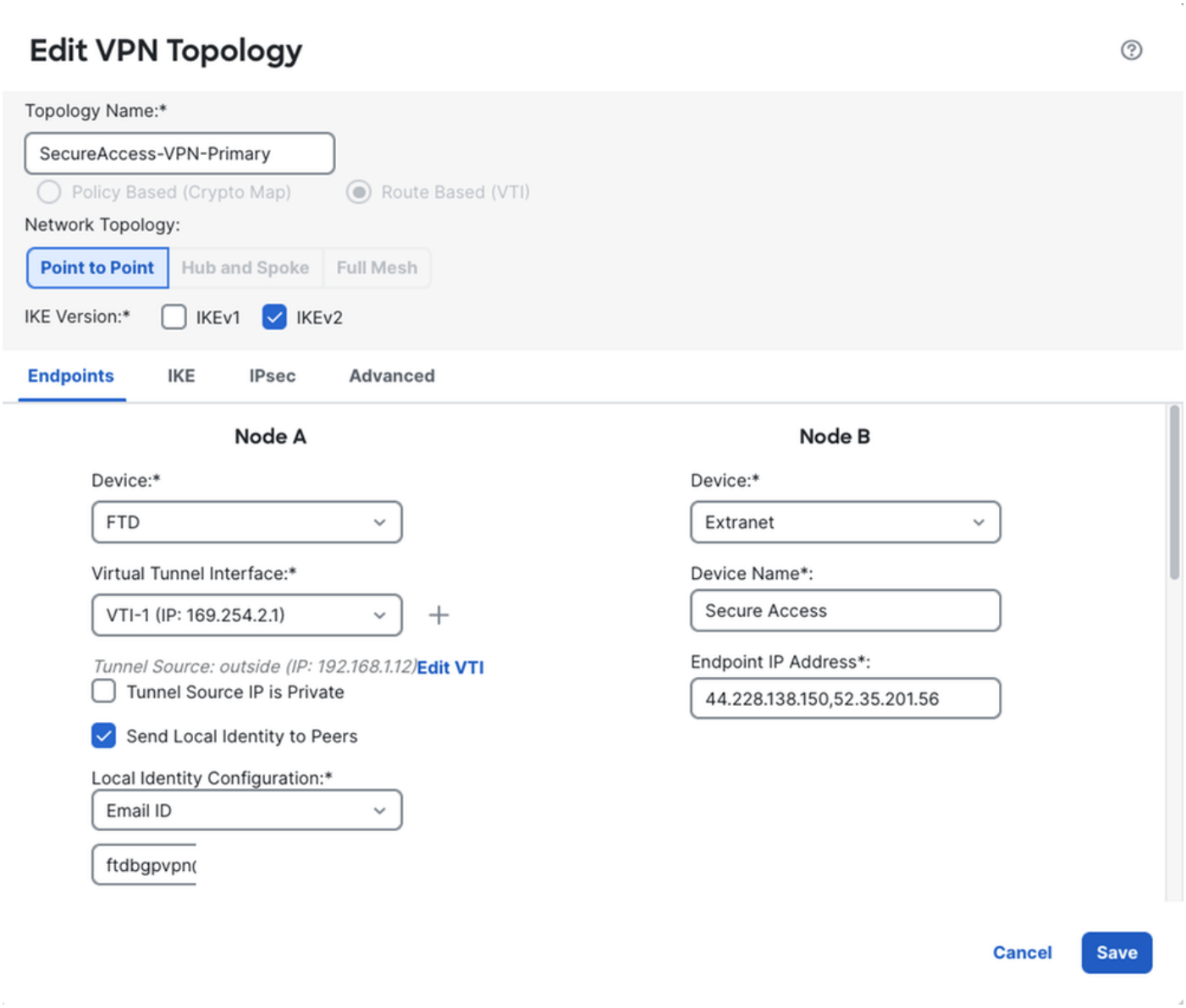
- Crea topologia VPN



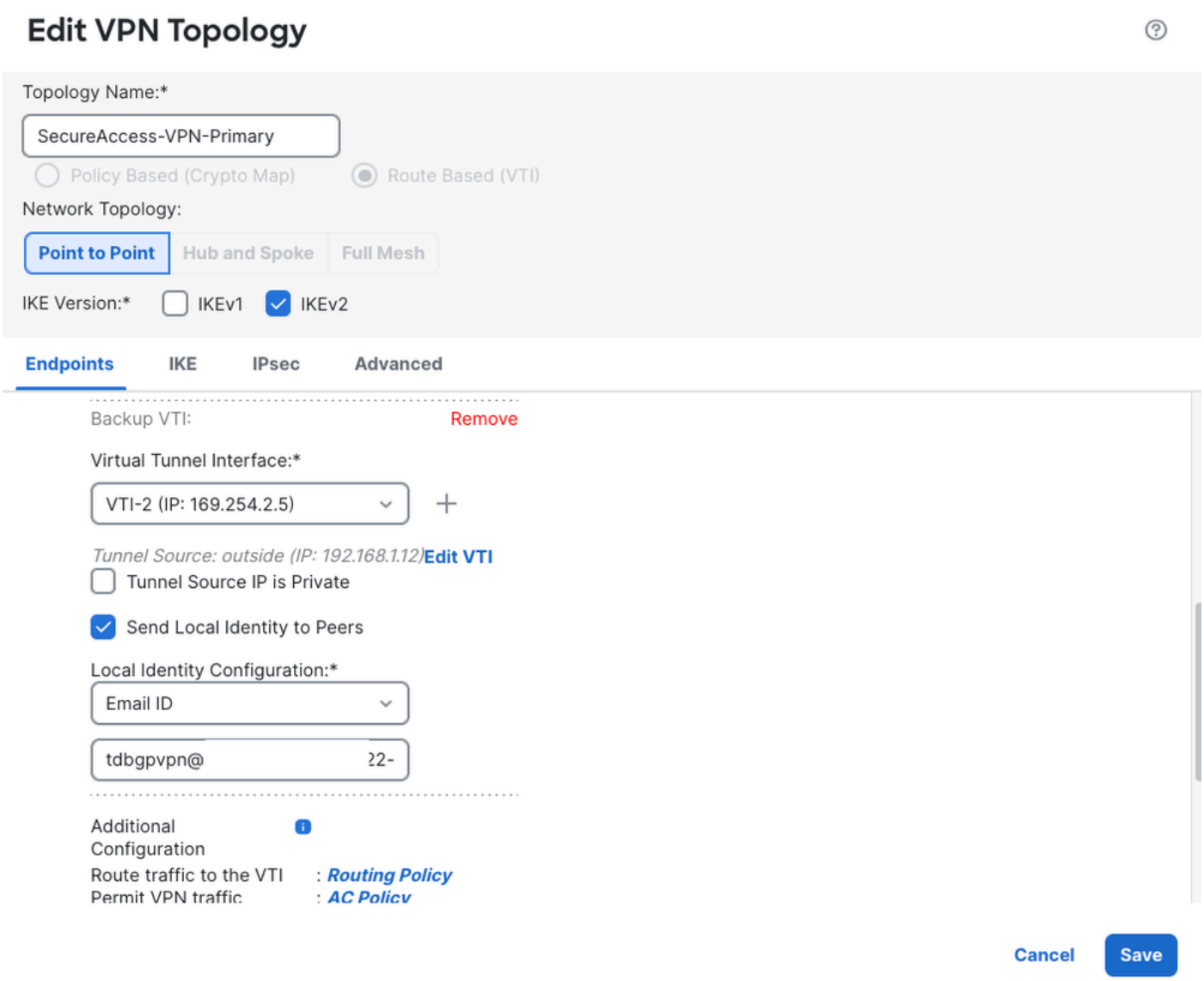
- Dal passaggio 6 di Configurazione del gruppo di tunnel di rete sull'accesso sicuro ottenere

gli ID e gli indirizzi IP del tunnel per i centri dati primario e secondario.

- Fare clic sugli endpoint
- In Nodo A, fare clic su Device e selezionare il dispositivo FTD
- Fare clic su Virtual Tunnel Interface e selezionare la prima interfaccia VTI creata nel passaggio precedente
- Fare clic sull'opzione Send Local Identity to Peers (Invia identità locale ai peer) e selezionare Email ID (ID e-mail), immettere l'ID del tunnel primario (da "Save Network Tunnel Group Configuration" (Salva configurazione gruppo tunnel di rete) in Configure Network Tunnel Group on Secure Access (Configura gruppo tunnel di rete su accesso sicuro)
- In Nodo B, fare clic su Device e selezionare Extranet
- Fare clic sul nome del dispositivo e assegnargli un nome
- Fare clic su Indirizzi IP degli endpoint e immettere gli indirizzi IP primari e secondari di Secure Access separati da una virgola (da "Salva configurazione gruppo tunnel di rete" in Configura gruppo tunnel di rete su accesso sicuro)
- Fare clic su Aggiungi VTI di backup
- Fare clic su Virtual Tunnel Interface e selezionare la seconda interfaccia VTI creata nel passaggio precedente
- Fare clic sull'opzione Send Local Identity to Peers (Invia identità locale ai peer) e selezionare Email ID (ID posta elettronica), immettere l'ID del tunnel secondario (da "Save Network Tunnel Group Configuration" (Salva configurazione gruppo tunnel di rete) in Configure Network Tunnel Group on Secure Access (Configura gruppo tunnel di rete su accesso sicuro)
- Fare clic su Salva

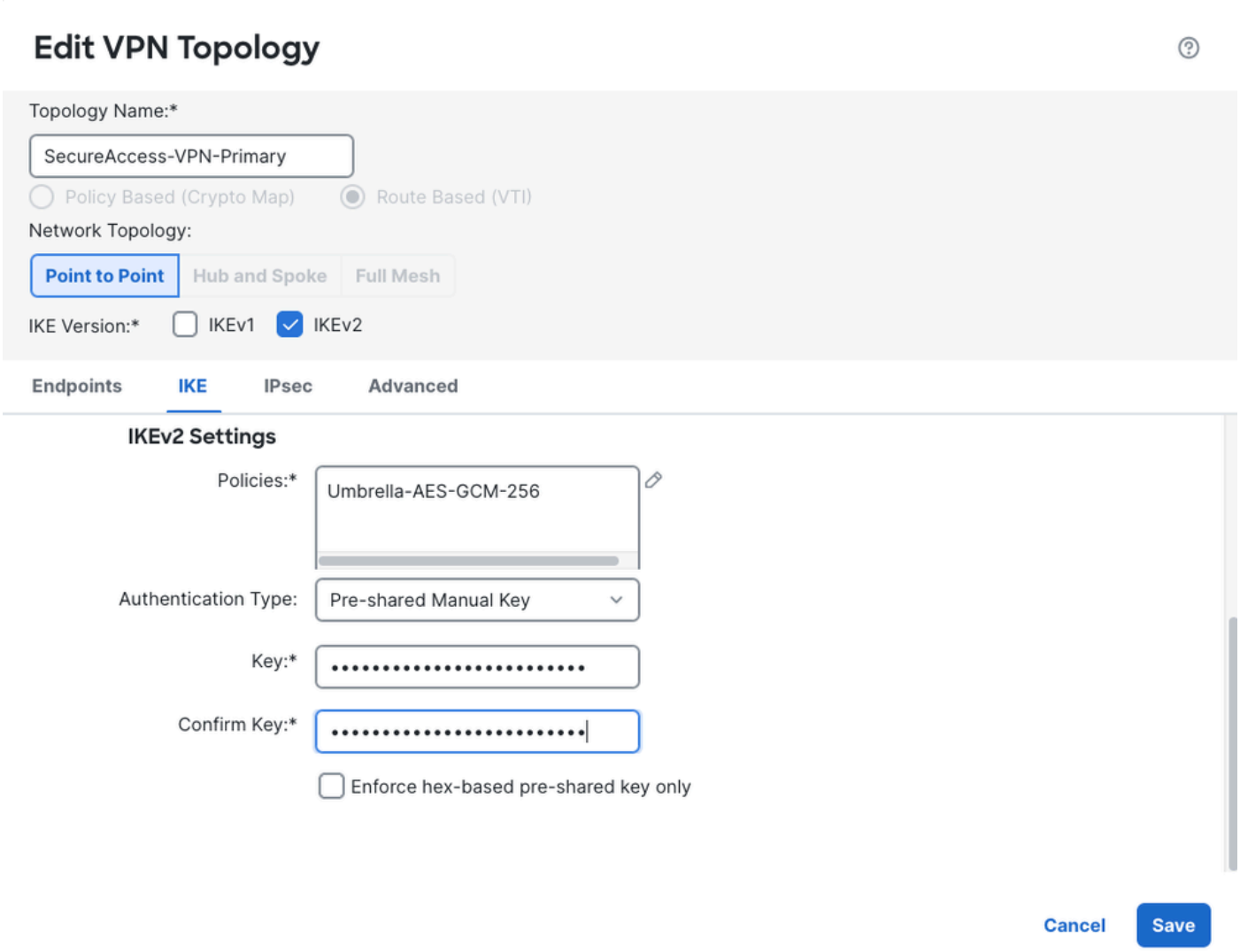


Secure FTD - Configurazione endpoint VPN



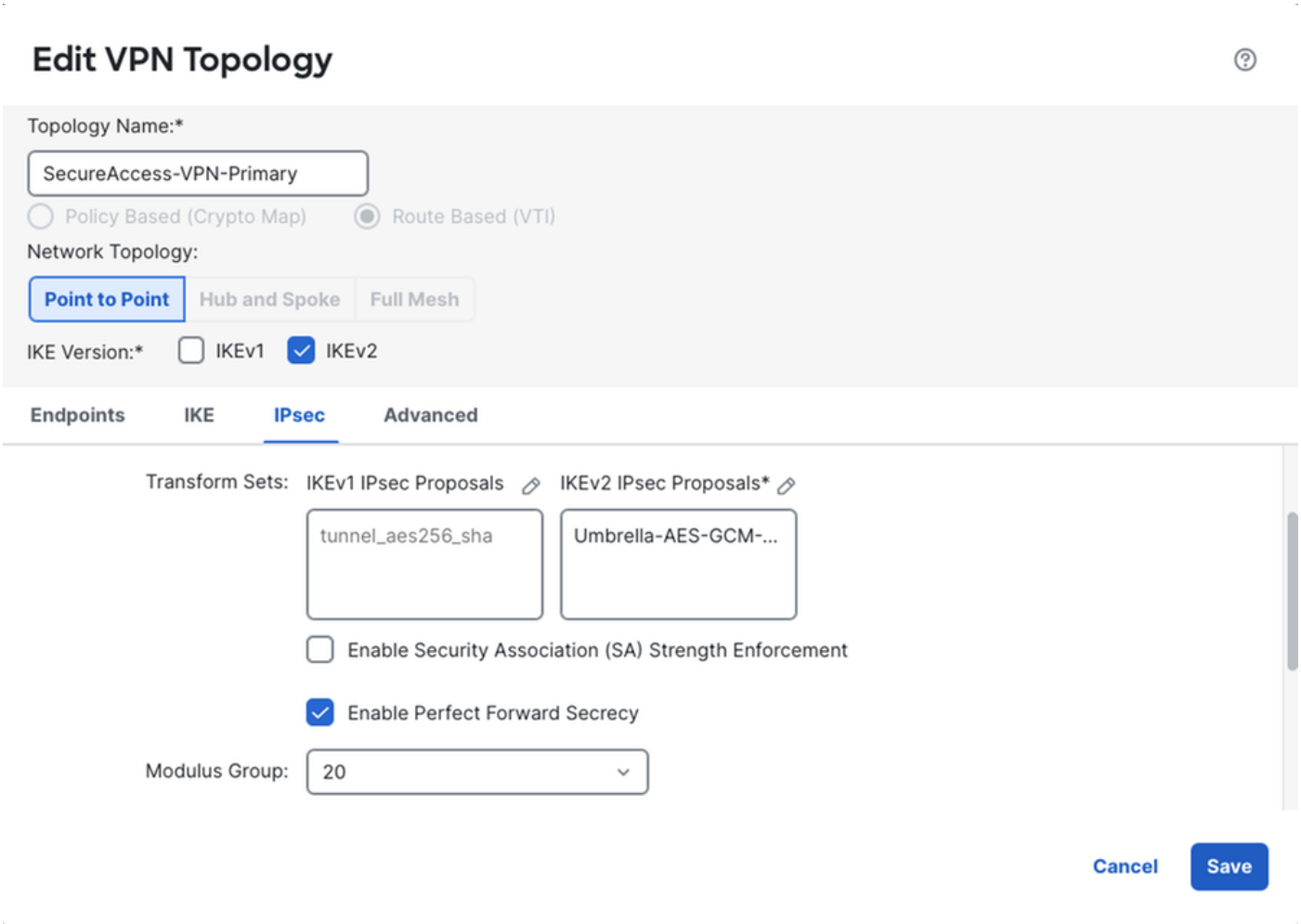
Secure FTD - Configurazione endpoint VPN

- Configurare le impostazioni IKEv2 in base ai parametri IPSec supportati
  - Seleziona criteri come Umbrella-AES-GCM-256
  - Selezionare il tipo di autenticazione come chiave manuale già condivisa



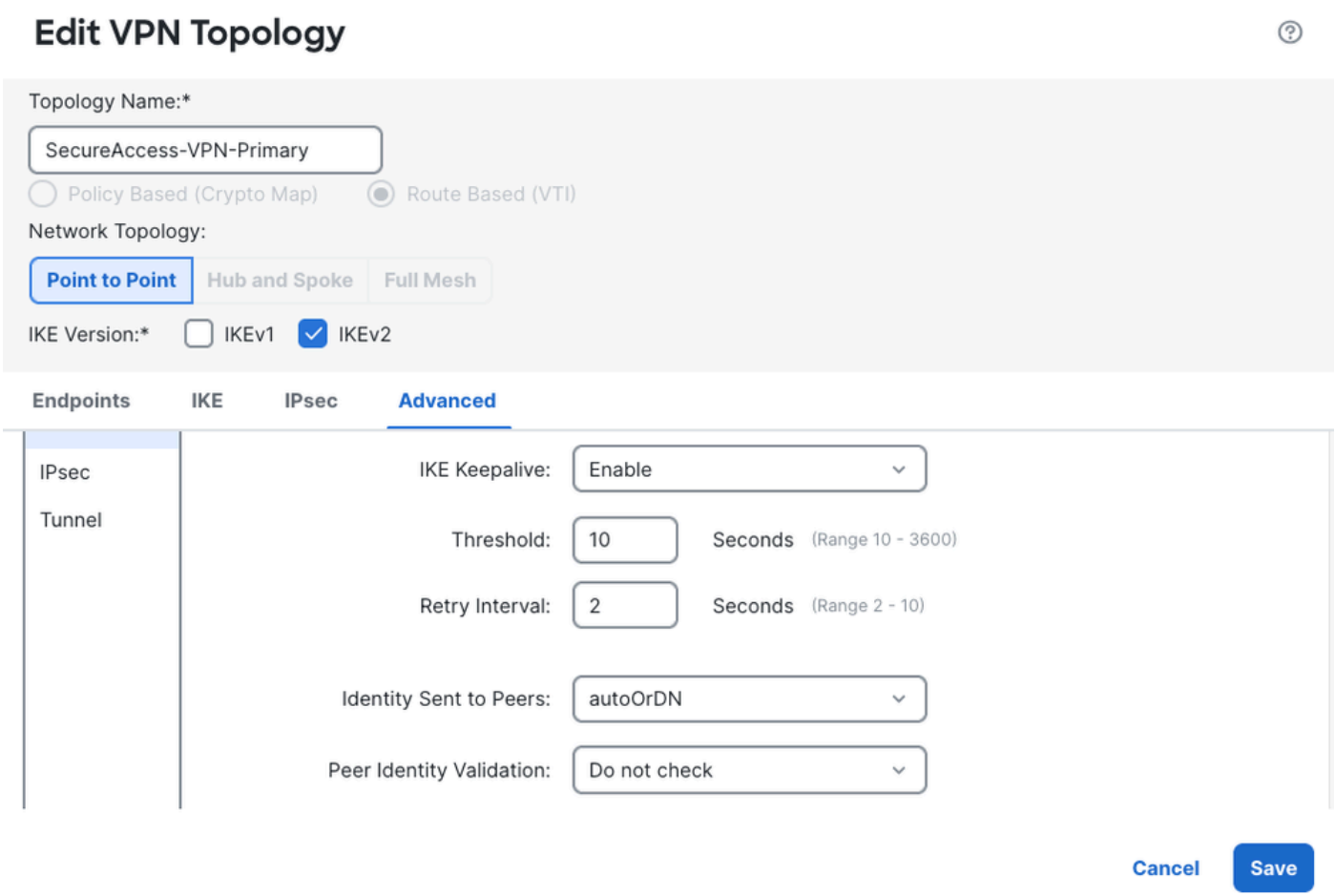
Secure FTD - Impostazioni VPN IKE

- Configura impostazioni IPSec
  - Seleziona proposte IPsec IKEv2 come Umbrella-AES-GCM-256
  - Abilita PFS come gruppo di moduli selezionato come 20



Secure FTD - Impostazioni IPsec VPN

- Impostazioni avanzate
- Fare clic su Salva.



Secure FTD - Impostazioni avanzate VPN

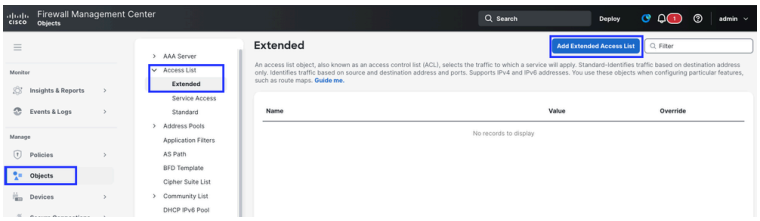
FTD Policy Based Routing

Nel routing tradizionale, i pacchetti vengono instradati in base all'indirizzo IP di destinazione. Modificare il routing di un traffico specifico in un sistema di routing basato sulla destinazione è difficile. Il Policy Based Routing (PBR) estende e integra i meccanismi forniti dai protocolli di routing, offrendo un maggiore controllo su quest'ultimo.

PBR consente di impostare la precedenza IP. Consente inoltre di specificare un percorso per determinati traffici, ad esempio il traffico di priorità su un collegamento costoso. Con PBR, è possibile definire il routing in base a criteri diversi dalla rete di destinazione, ad esempio porta di origine, indirizzo di destinazione, porta di destinazione, protocollo, applicazioni o una combinazione di questi oggetti. Per ulteriori informazioni, fare riferimento al documento Policy Based Routing

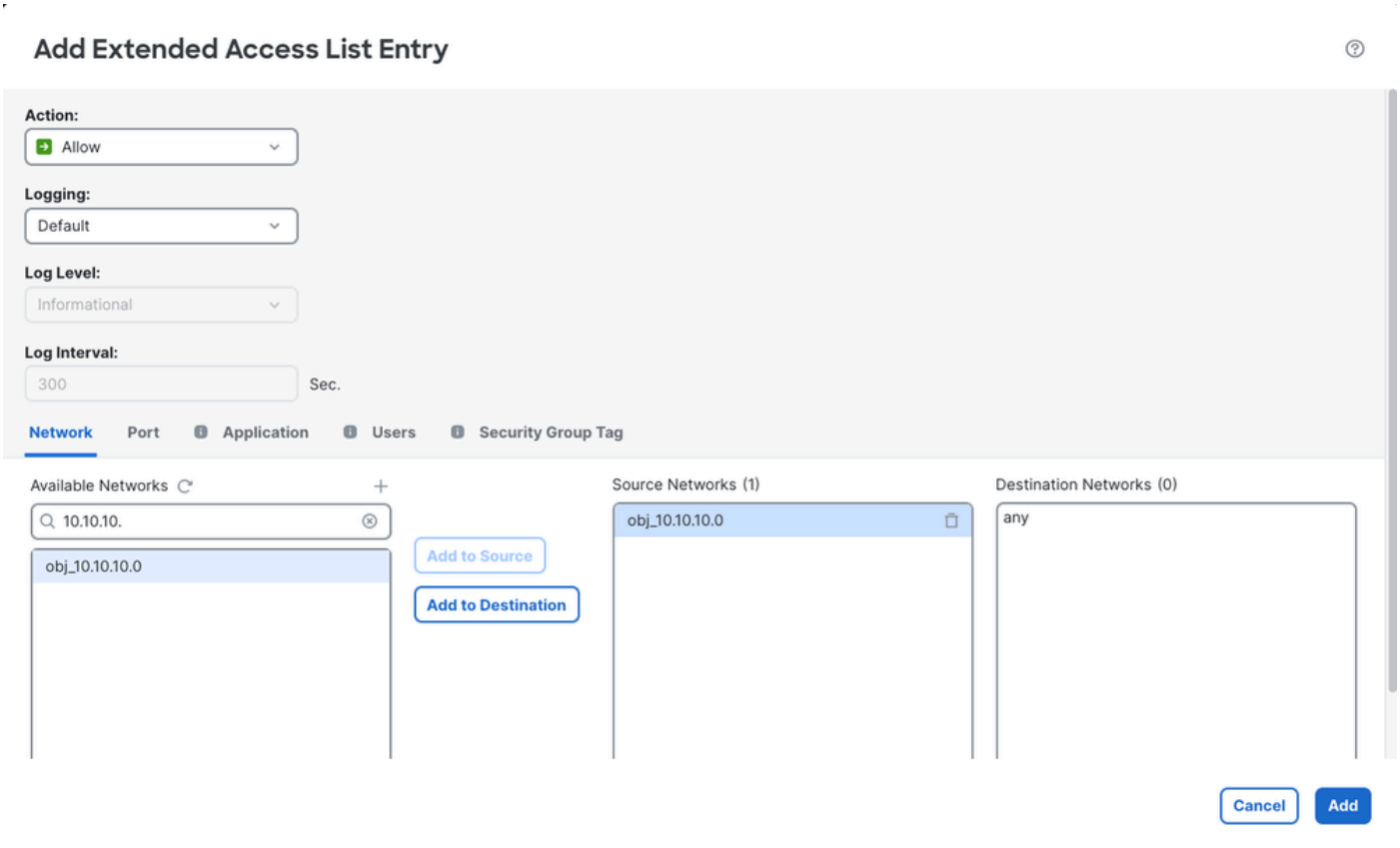
1. Configura elenco accessi

- Selezionare Oggetti > Elenco accessi > Estesi

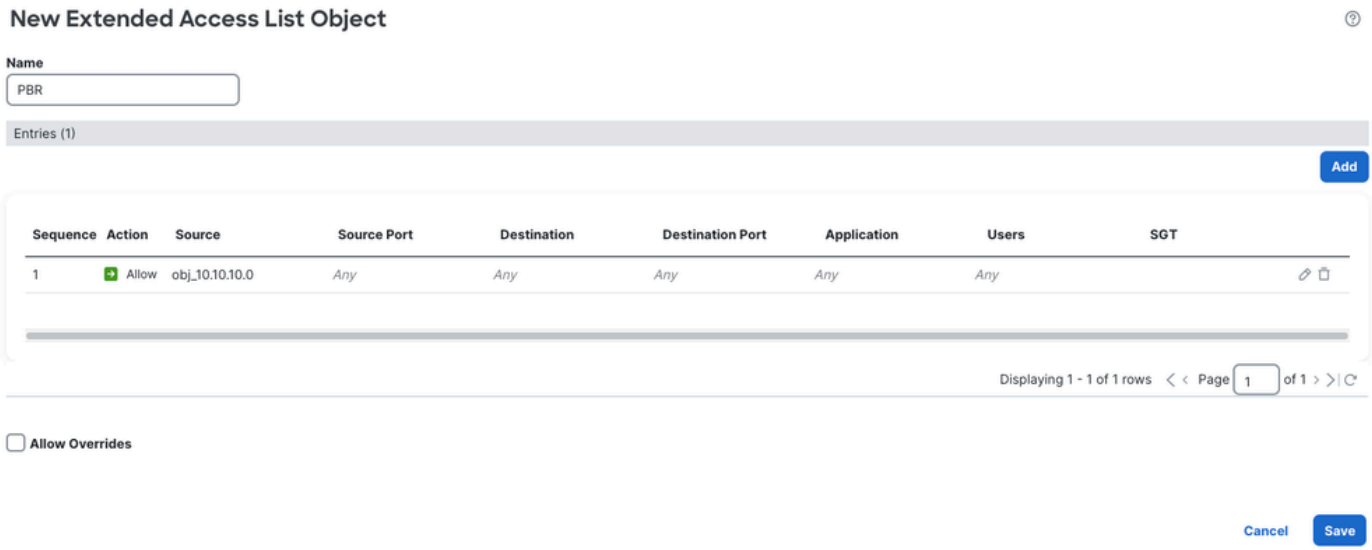
- Fare clic su Add Extended Access List 

Secure FTD - Elenco accessi esteso

- Assegnare un nome all'elenco accessi
- Definizione dell'azione
  - Consenti. - Il traffico definito verrà inviato al tunnel IPsec
  - Blocco - Il traffico verrà ignorato dal tunnel IPSec
  - La regola verrà confrontata in base al numero di sequenza (dal più basso al più alto)
  - Fare clic su Add
  - Fare clic su Salva.



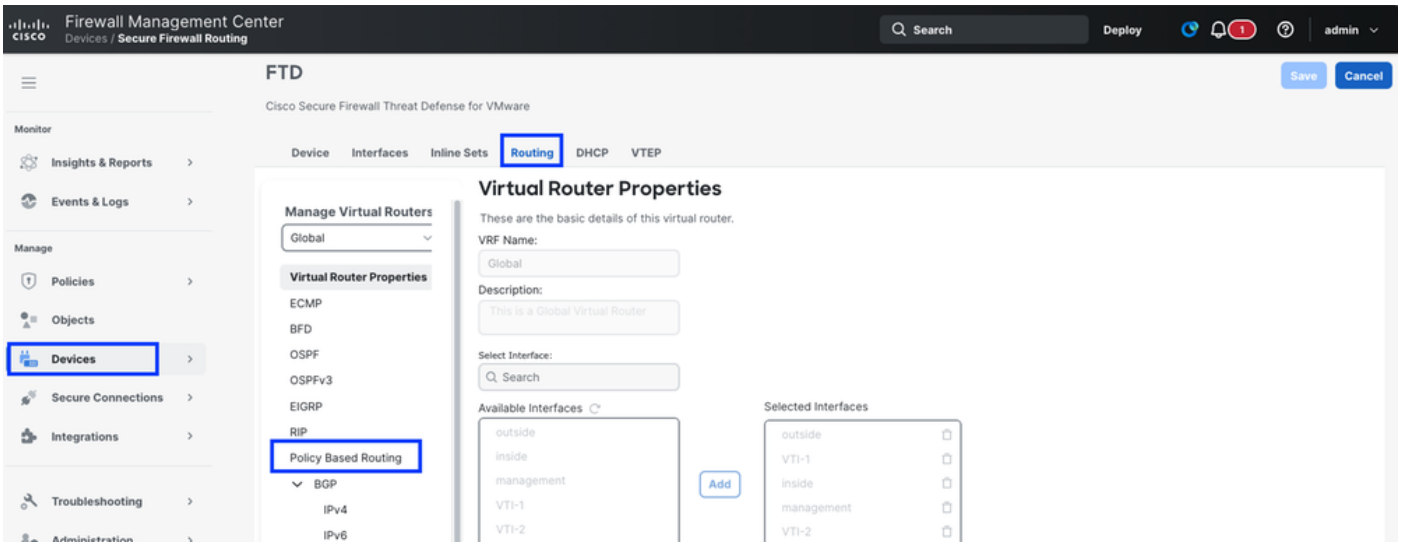
Secure FTD - Elenco accessi esteso



Secure FTD - Elenco accessi esteso

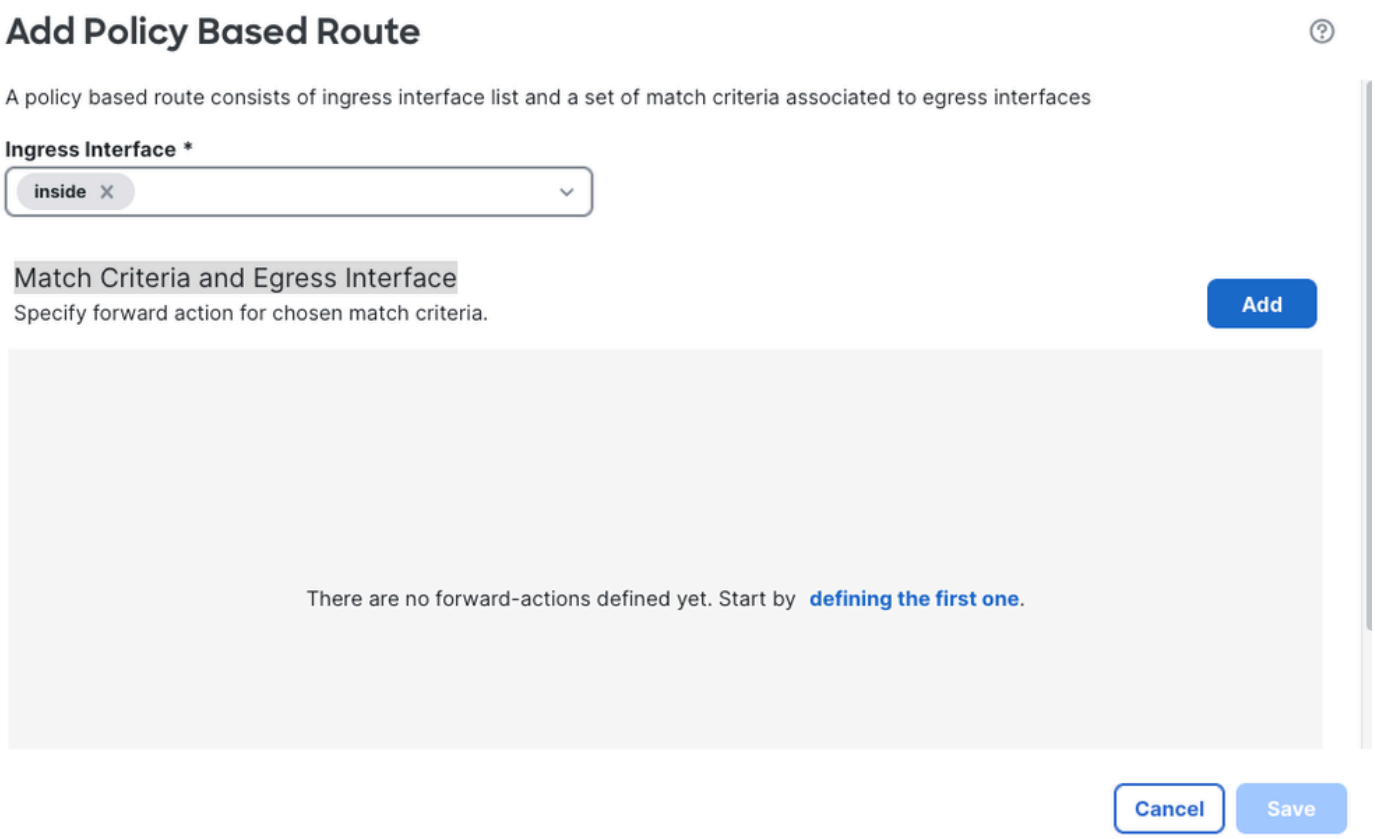
2. Configurare il routing basato su criteri

- Selezionare Dispositivi > Gestione dispositivi > FTD > Instradamento



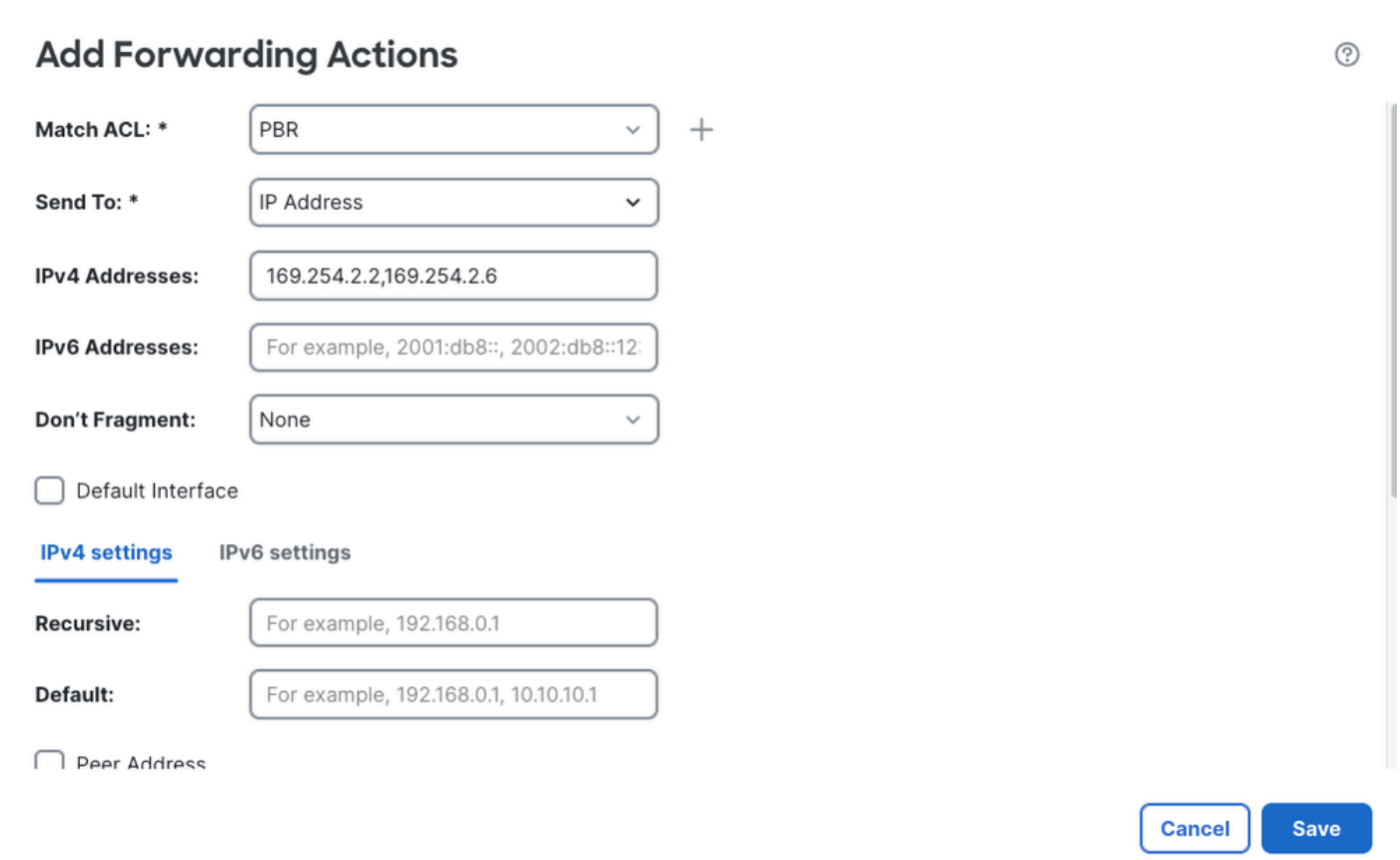
Secure FTD - Policy Based Routing

- Fare clic su Aggiungi
- Selezionare Interfaccia in ingresso - Interfaccia in ingresso per la subnet definita nell'elenco degli accessi

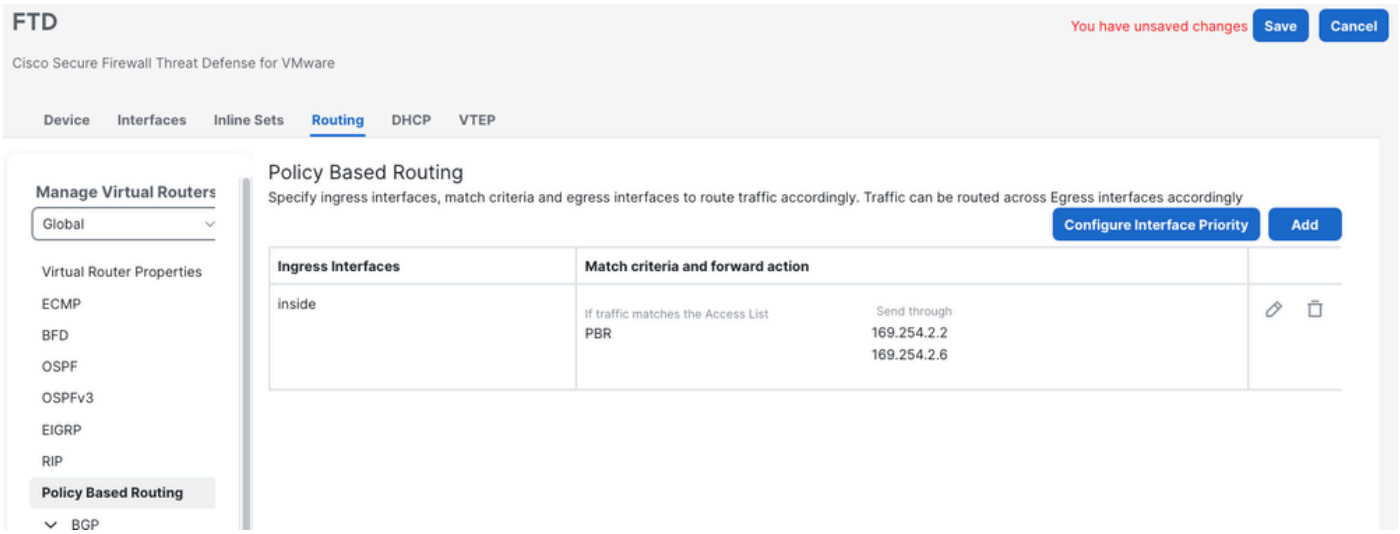


Secure FTD - Policy Based Routing

- Definizione dei criteri di corrispondenza e dell'interfaccia in uscita
  - Fare clic su Add
  - Selezionare l'ACL corrispondente
  - Selezionare Invia a come indirizzo IP
  - Aggiungi indirizzo IP hop successivo. - Gli indirizzi IP dell'interfaccia VTI sono. 169.254.2.130 e. 169.254.2.5/30. Quindi, gli indirizzi IP dell'hop successivo per VTI -1 e VTI-2 saranno 169.254.2.2 e 169.254. 169 254 2.6
  - Fare clic su Salva



Secure FTD - Policy Based Routing

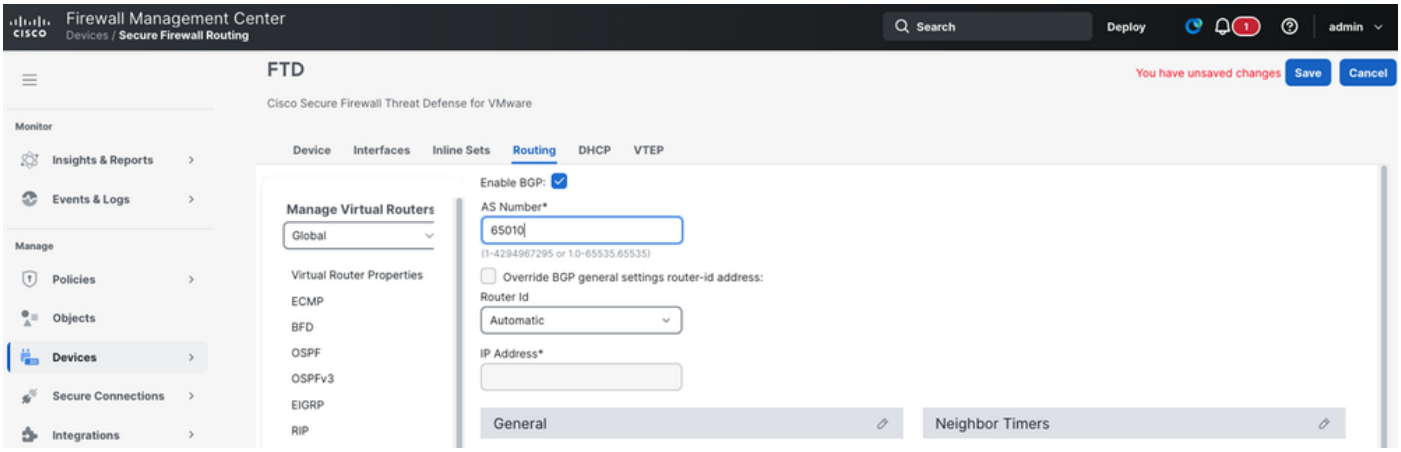


Secure FTD - Policy Based Routing

Configurazione di BGP su FTD

1. Abilitare BGP

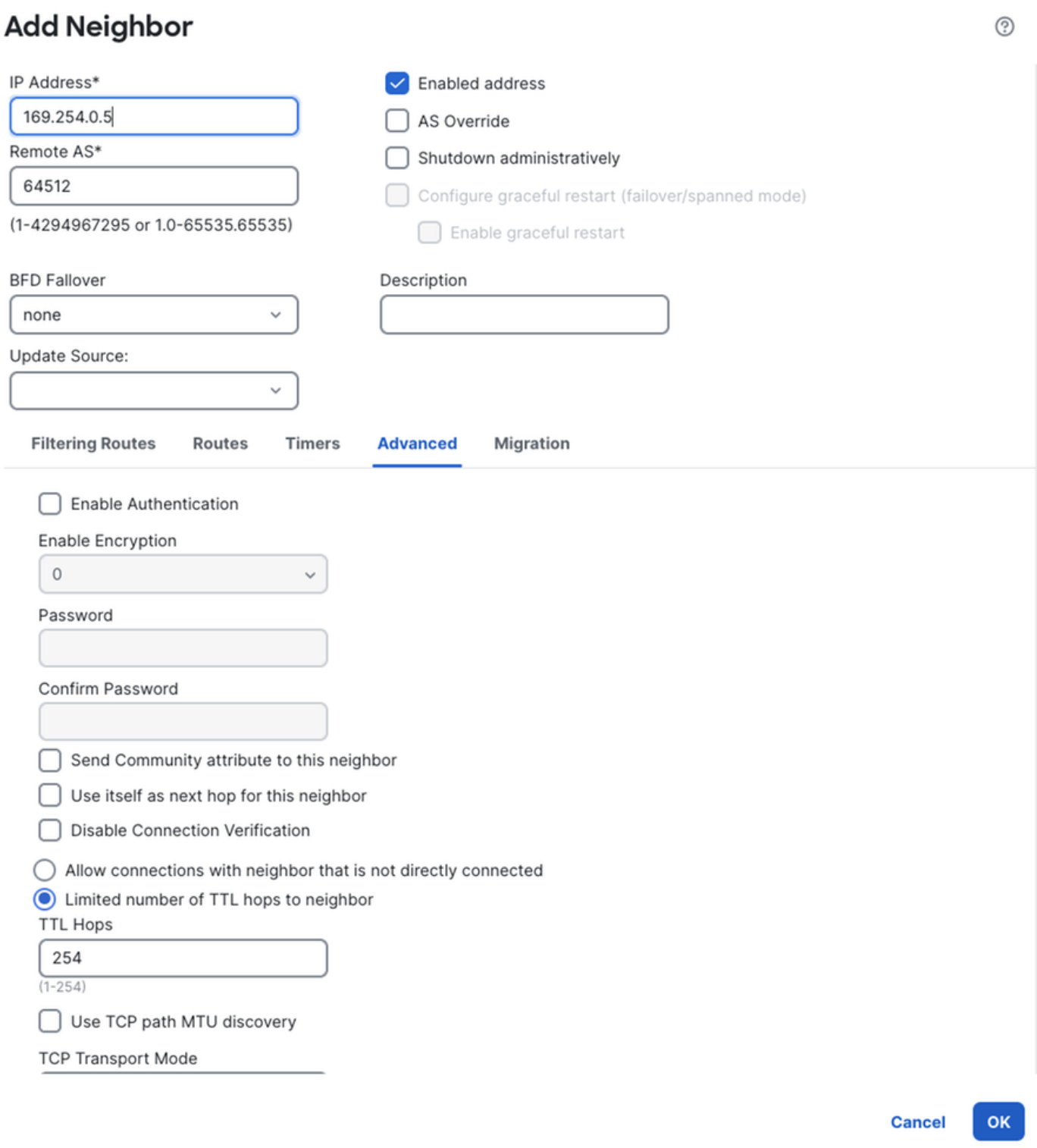
- Selezionare Dispositivi > Gestione dispositivi > FTD > Routing > Impostazioni generali > BGP
- Abilitare BGP e aggiungere il numero AS (numero AS locale FTD)
- Fare clic su Salva.

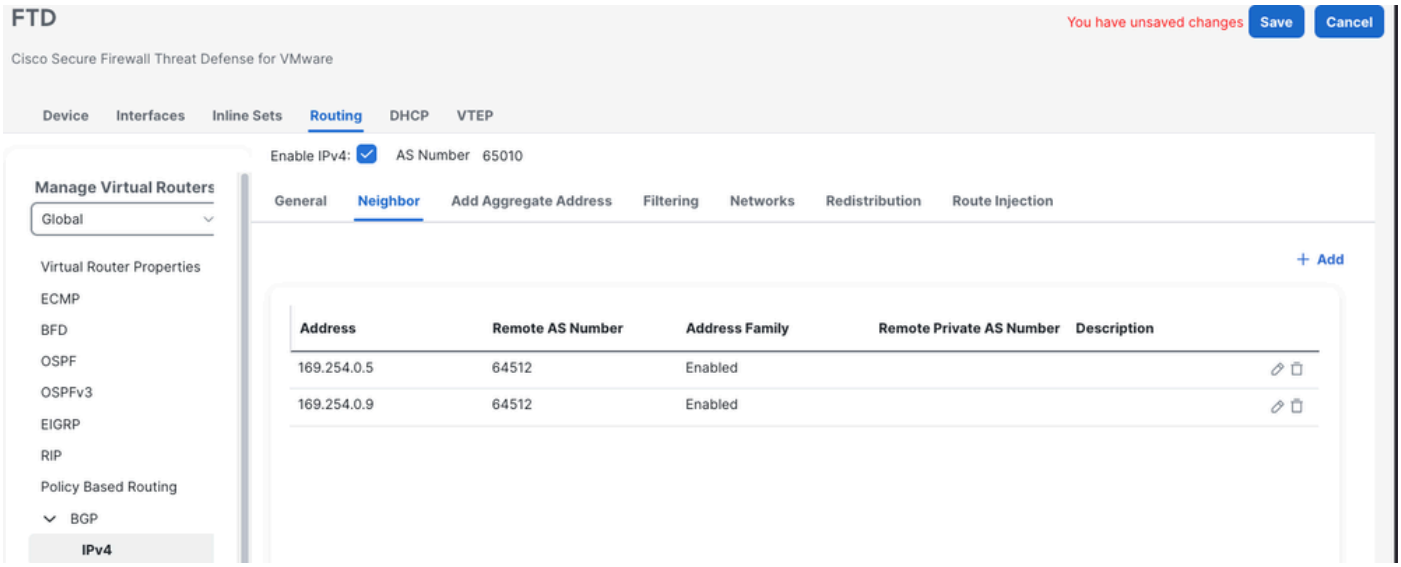


Secure FTD - Routing BGP

- Selezionare BGP > IPv4

2. Aggiunta router adiacente BGP: i peer BGP con accesso sicuro sono 169.254.0.5 e 169.254.0.5. 169.254.0.9

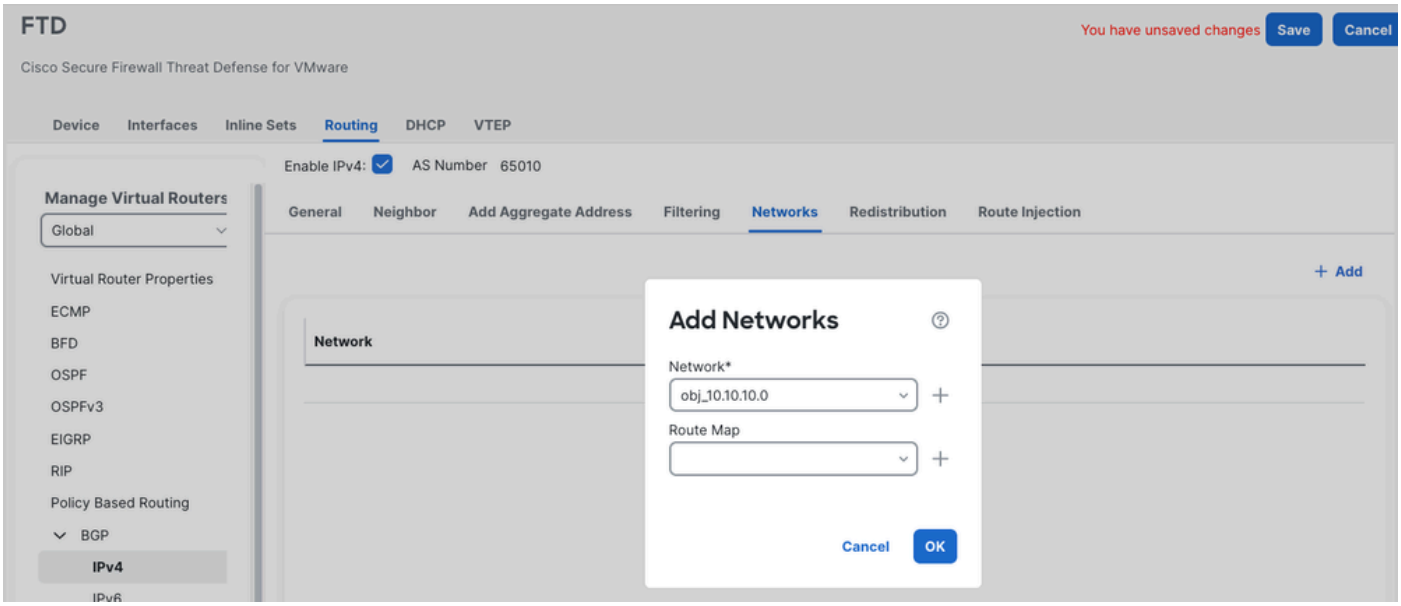

Add Neighbor
IP Address*
169.254.0.5
Remote AS*
64512
(1-4294967295 or 1.0-65535.65535)
Enabled address
AS Override
Shutdown administratively
Configure graceful restart (failover/spanned mode)
Enable graceful restart
BFD Fallover
none
Description
Update Source:
Filtering Routes
Routes
Timers
Advanced
Migration
Enable Authentication
Enable Encryption
0
Password
Confirm Password
Send Community attribute to this neighbor
Use itself as next hop for this neighbor
Disable Connection Verification
Allow connections with neighbor that is not directly connected
Limited number of TTL hops to neighbor
TTL Hops
254
(1-254)
Use TCP path MTU discovery
TCP Transport Mode
Cancel
OK



Secure FTD - Routing BGP

3. Aggiungere le reti - Reti che devono essere pubblicizzate per Secure Access

- Fare clic su OK.

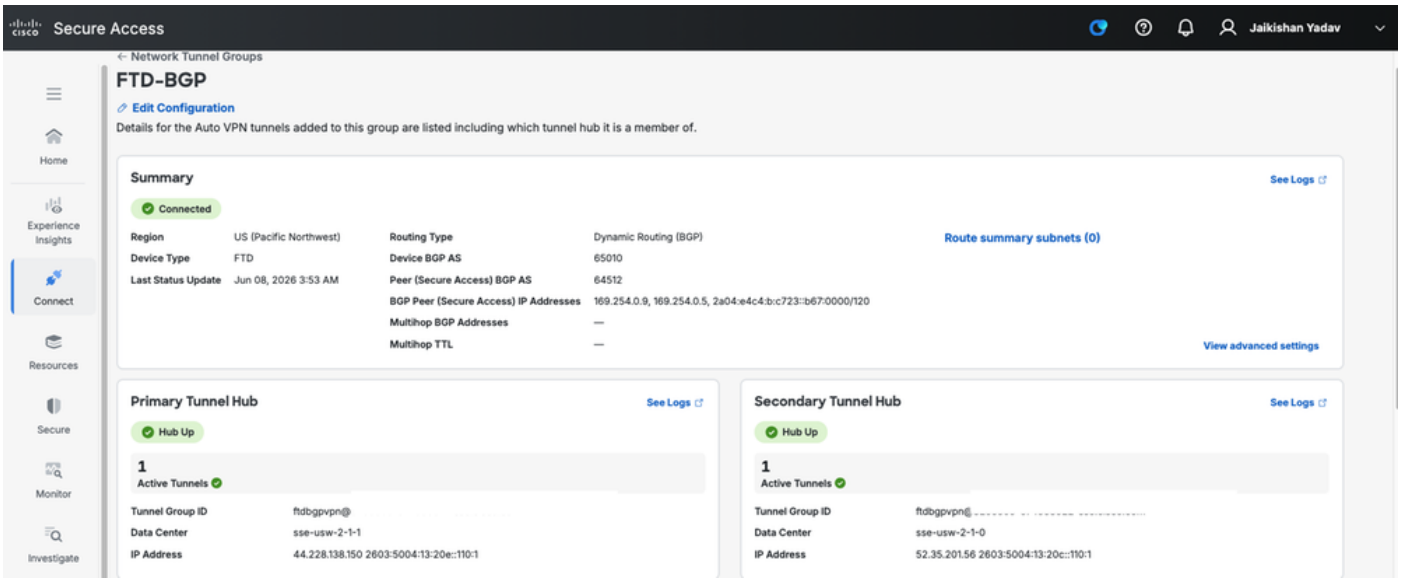


Secure FTD - Routing BGP

- Salvare e distribuire le modifiche

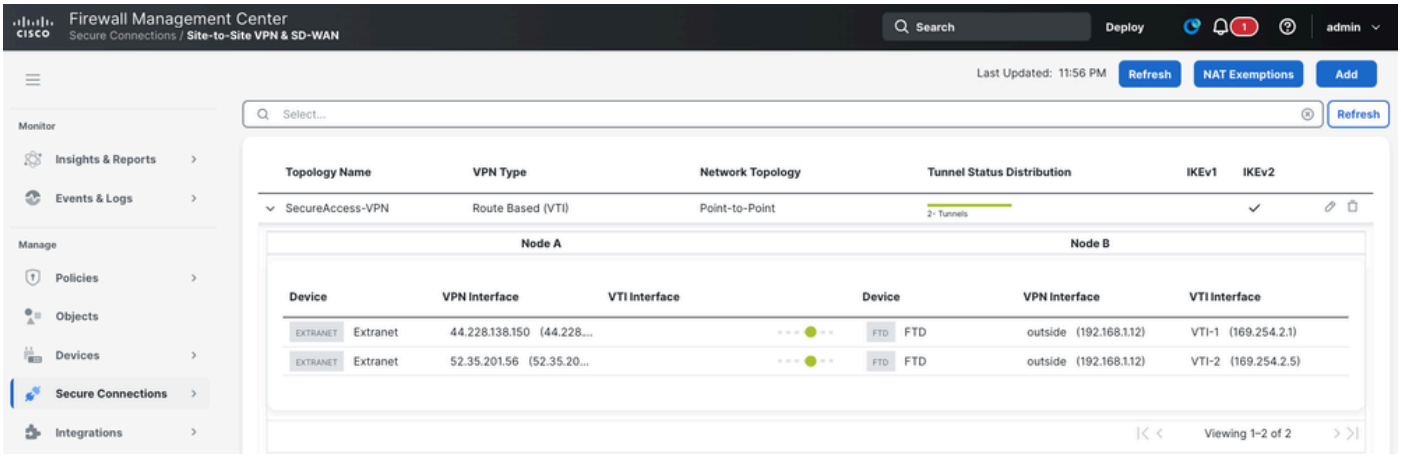
Verifica stato tunnel

Su accesso sicuro



Stato tunnel IPSec - FTD sicuro

Sul CCP



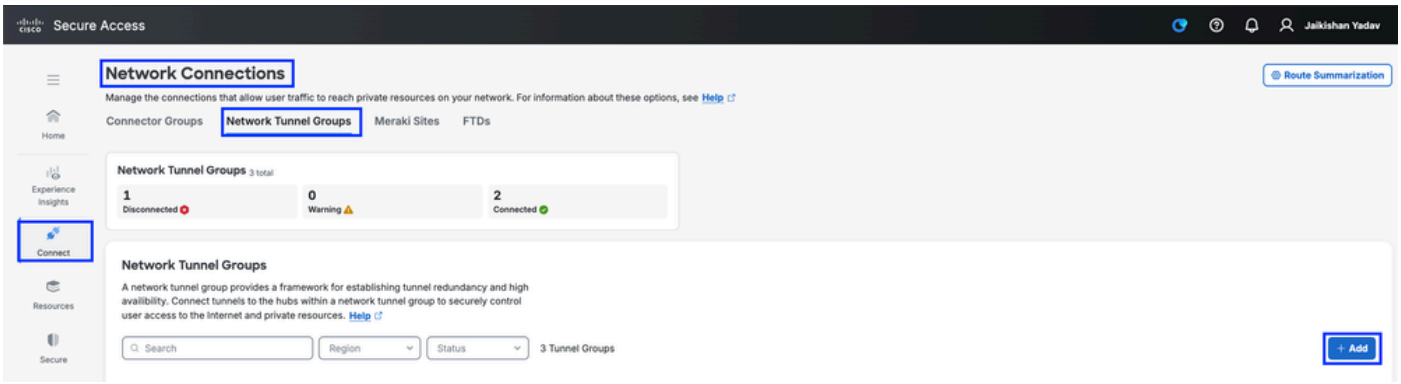
Stato tunnel IPSec - FMC protetto

Configurazione della VPN IPsec basata su route statica su ASA (Adaptive Security Appliance) con PBR

Configurazione VPN su accesso sicuro

1. Accesso al dashboard Accesso sicuro Accesso sicuro
2. Passare a Connetti > Connessioni di rete > Gruppi di tunnel di rete e fare clic su +Aggiungi per

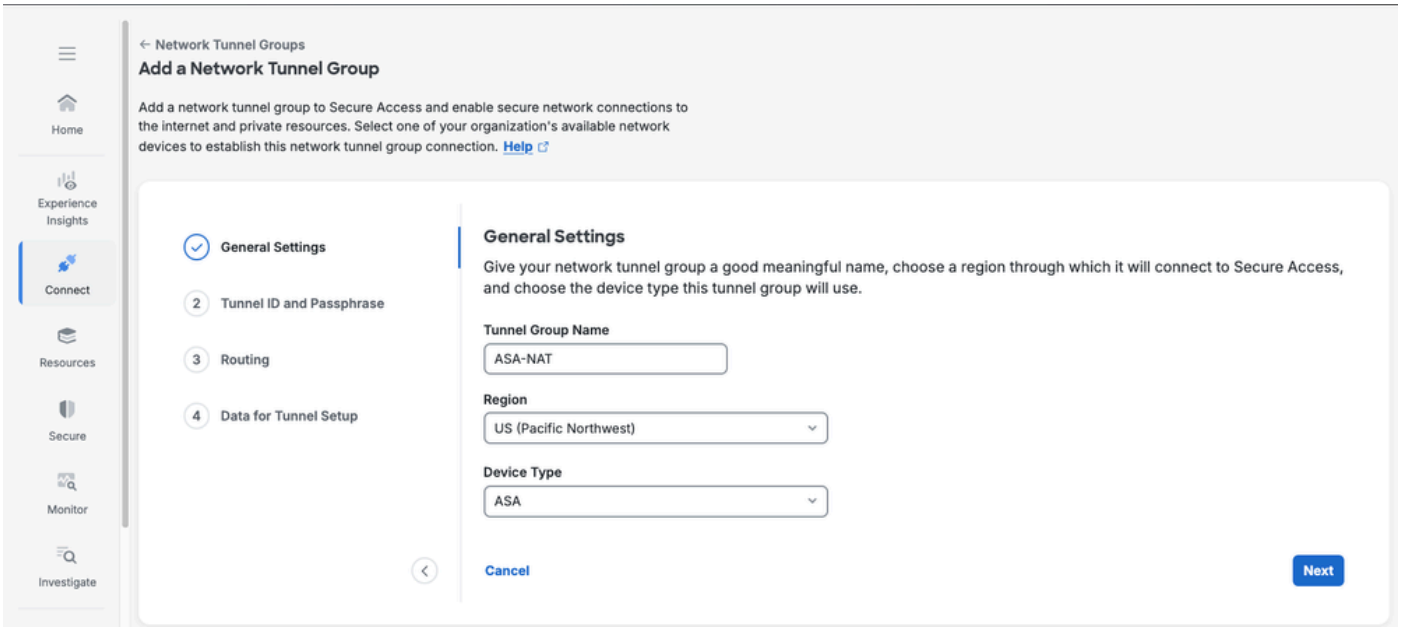
configurare il gruppo di tunnel di rete



Accesso sicuro - Gruppi di tunnel di rete

3. Configurare il gruppo di tunnel di rete - Impostazioni generali

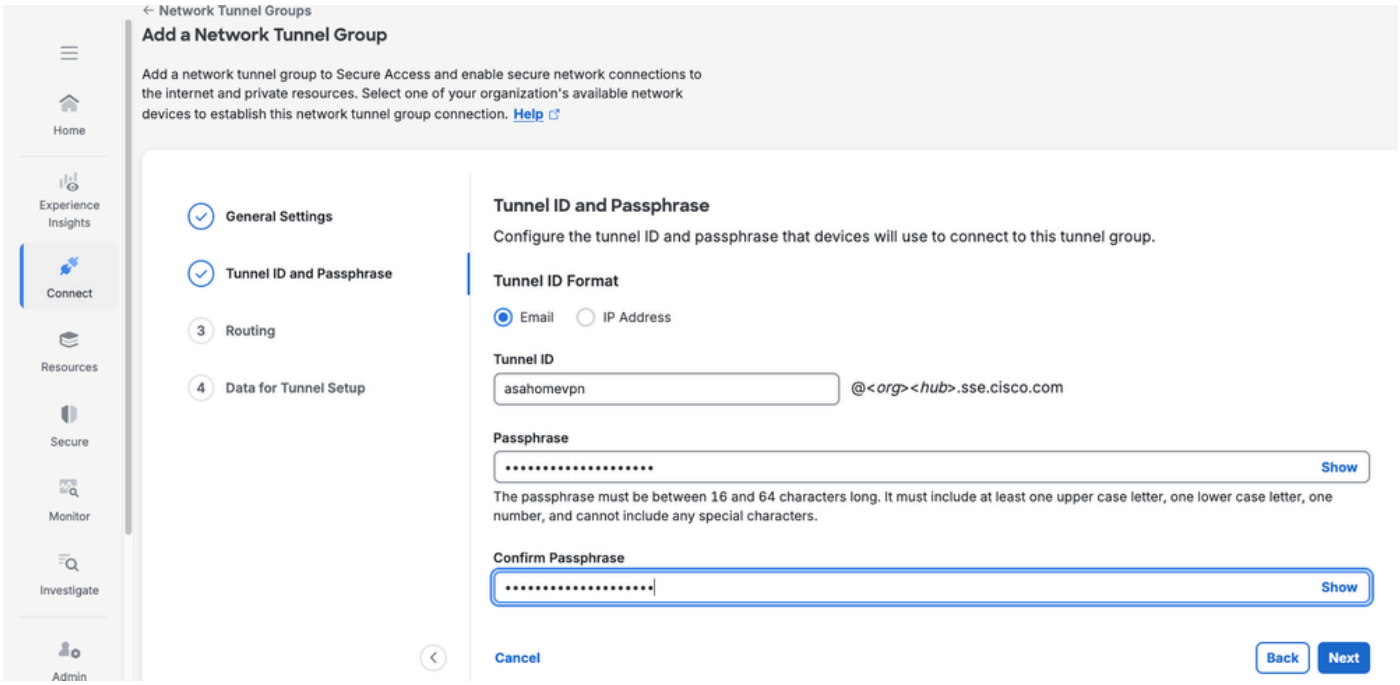
- Configura nome gruppo tunnel, area e tipo di dispositivo
- Fare clic su Avanti.



Accesso sicuro - Impostazioni generali gruppi tunnel di rete

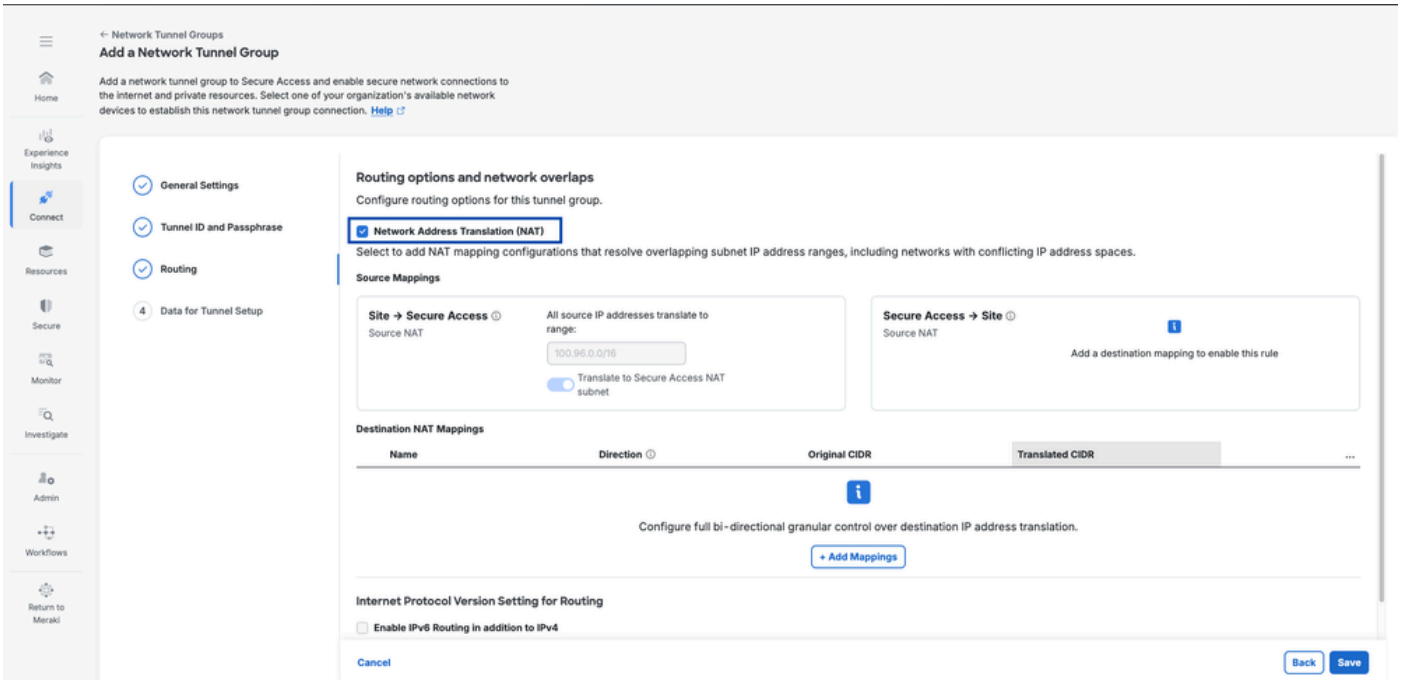
4. Configurare l'ID tunnel e la passphrase.

- Configurare l'ID del tunnel e la passphrase.
- Fare clic su Avanti



Accesso sicuro - Gruppi di tunnel di rete

5. Abilitare NAT (Network Address Translation)

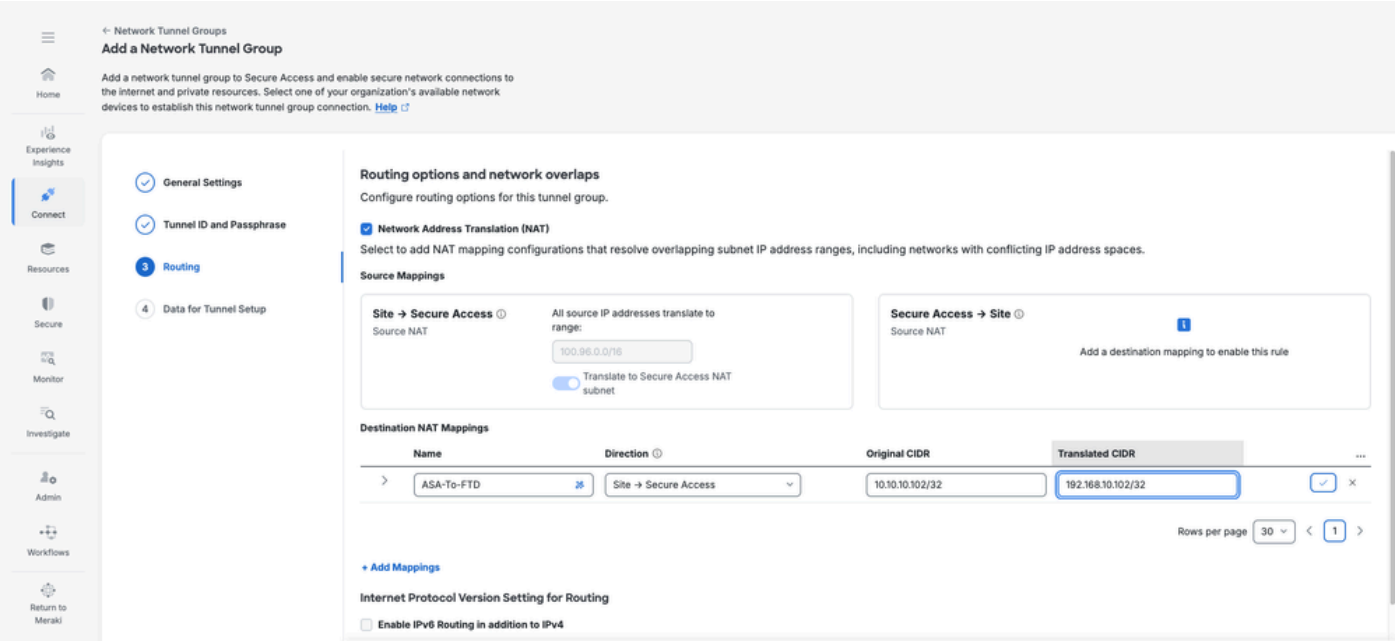


Accesso sicuro - Impostazioni NAT gruppi tunnel di rete

6. Aggiungi mapping NAT di destinazione

Flusso 1 - Da router 1 a router 2 (da sito ad accesso sicuro)

Flusso 2 - Da router 2 a router 1 (accesso sicuro al sito)

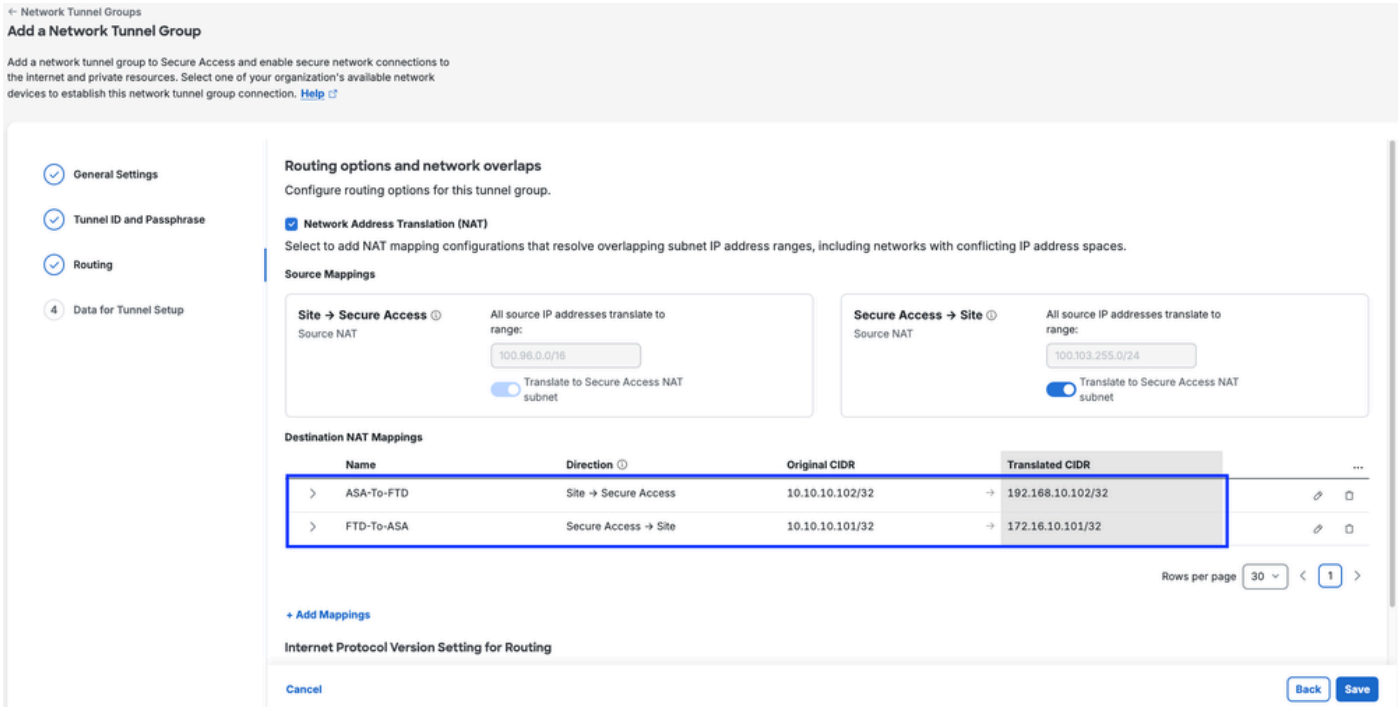


Accesso sicuro - Impostazioni NAT gruppi tunnel di rete

Attenzione: Quando NAT è abilitato, BGP non è possibile. Configurare inoltre la VPN statica sui dispositivi Customer Edge

---

Suggerimento: Ricordarsi sempre di eseguire il ping di un indirizzo IP tradotto.
L'IP tradotto va in CIDR tradotto e l'IP reale va in CIDR originale.



Accesso sicuro - Impostazioni NAT gruppi tunnel di rete

Fare clic su Salva

Suggerimento: Per il traffico che va dal 'Sito A' al 'Sito B', dalla direzione del punto di vista di CNHE-1 è 'Sito-> SecureAccess'

Per il traffico che va dal 'sito B' al 'sito A', dalla direzione del punto di vista di CNHE-1 è 'SecureAccess -> Sito'

Configurazione VPN su ASA

1. Accedere alla CLI di ASA, accedere alla modalità abilitazione e verificare la connettività IP di base verso Internet

ASA# sh ip
Indirizzi IP di sistema:
Nome interfaccia Indirizzo IP Subnet mask, metodo
Gigabit Ethernet0/0 esterno a 192.168.1.40 255.255.255.0 manuale
Gigabit Ethernet0/1 all'interno del manuale 10.10.1.255.255.255.0

Indirizzi IP correnti:
Nome interfaccia Indirizzo IP Subnet mask, metodo
Gigabit Ethernet0/0 esterno a 192.168.1.40 255.255.255.0 manuale

Gigabit Ethernet0/1 all'interno del manuale 10.10.1.255.255.255.0

ASA# ping 8.8.8.8
Digitare la sequenza di escape da interrompere.
Invio di 5 echo ICMP da 100 byte a 8.8.8.8, il timeout è di 2 secondi:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/28/30 ms
N. ASA

2. Configurare il criterio IKEv2 e abilitare IKEv2 sull'interfaccia esterna

criterio crypto ikev2 10
crittografia aes-gcm-256
integrità null
gruppo 19
secondi durata 86400
crypto ikev2 abilitare per l'esterno

3. Configurare la proposta IPSec

crypto ipsec ikev2 ipsec-proposta Ipsec-proposta-primary
protocollo esp encryption aes-gcm-256

4. Configurare il profilo IPSec

crypto ipsec profile csa-profile-primary
set ikev2 ipsec-proposta Ipsec-proposta-primario
set ikev2 local-identity email-id <id tunnel primario>

5. Configurare Criteri di gruppo e abilitare il protocollo IKEv2 nell'attributo.

criteri di gruppo csa-policy-primary internal
attributi primari csa-policy-criteri-gruppo
vpn-tunnel-protocol ikev2

6. Configurare il gruppo di tunnel.

tunnel group 44.228.138.150 tipo ipsec-l2l
tunnel group 44.228.138.150 general-attributes
default-group-policy csa-policy-primary

attributi ipsec tunnel group 44.228.138.150
chiave pre-condivisa <pre-shared-key> di autenticazione remota ikev2
chiave precondivisa di autenticazione locale ikev2 <chiave precondivisa>

7. Configurazione della VTI (Virtual Tunnel Interface)

- Nameif può essere se lo si desidera
- L'indirizzo IP assegnato alla VTI non deve essere sovrapposto ad altre interfacce sull'appliance ASA
- L'origine del tunnel deve essere l'interfaccia esterna del firewall
- La destinazione del tunnel deve essere l'indirizzo IP del data center

interface Tunnel1
nameif VTI-1
indirizzo ip 169.254.2.1 255.255.255.252
interfaccia di origine tunnel esterna
destinazione del tunnel 44.228.138.150
modalità tunnel ipsec ipv4
protezione tunnel profilo ipsec profilo csa-profilo-primario

8. Configurare il routing in modo che il traffico diretto all'indirizzo IP o alla subnet mappati venga instradato all'interno dell'interfaccia VTI. L'hop successivo deve passare attraverso l'IP entro la gamma VTI.

route VTI-1 0.0.0.0 0.0.0.0 169.254.2.2.5. (per traffico basato su Internet, pool RAVPN o CGNAT)

o

rotta VTI-1 172.16.10.101 255.255.255.255 169.254.2.2 5

Policy Based Routing

1. Elenco accessi

access-list PBR extended allow ip 10.10.10.0 255.255.255.0 any

2. Percorso-mappa

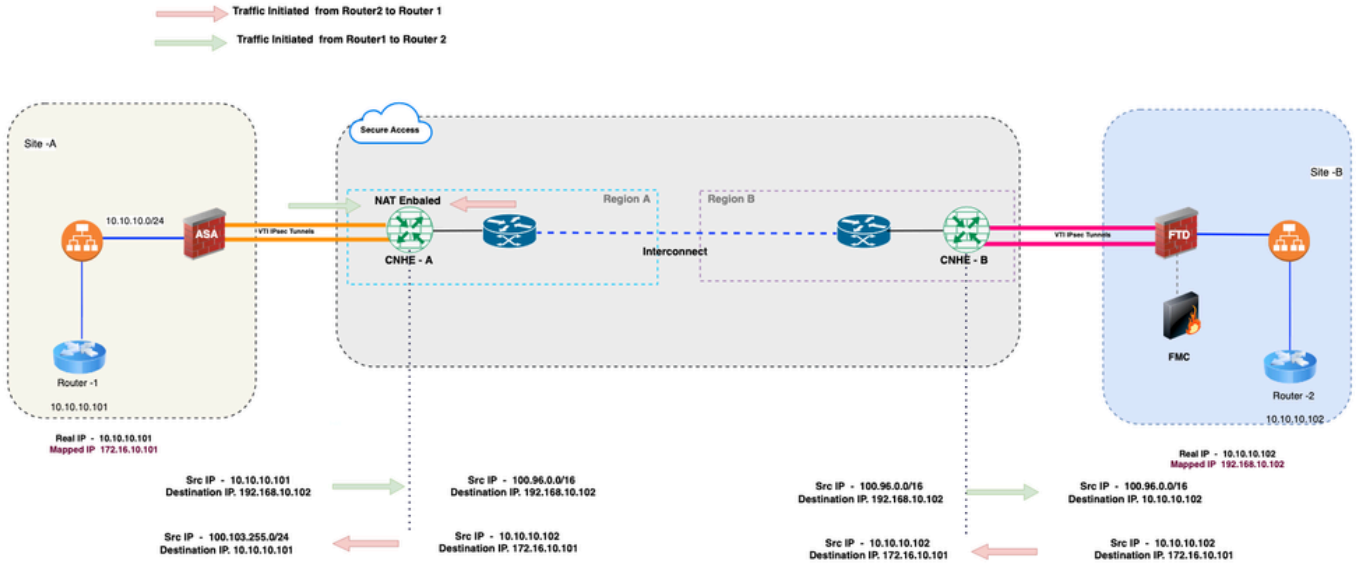
route-map autorizzazione RM-CSA 10
corrispondenza indirizzo ip PBR

set ip next-hop 169.254.2.2 169.254.2.6

3. Applicare la mappa del percorso sull'interfaccia in entrata

interfaccia Gigabit Ethernet0/1
nameif inside
livello di protezione 100
indirizzo ip 10.10.10.1 255.255.255.0
policy-route route-map RM-CSA

Verifica



Stato dell'interfaccia del router e della raggiungibilità del GW

```
Router1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       192.168.1.101   YES NVRAM  down                  down
GigabitEthernet2       10.10.10.101    YES NVRAM  up                    up
GigabitEthernet3       unassigned      YES NVRAM  administratively down down
GigabitEthernet9       unassigned      YES unset  administratively down down
Router1#ping  10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Test 1- Router2 —> Router1. - Test Ping

```
Router1#ping 192.168.10.102
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.102, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 207/211/223 ms
Router1#
```

Acquisizione dei pacchetti sull'appliance ASA (firmware locale)

```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA#
ASA#
ASA# ter pag 20
ASA# sh cap capin

10 packets captured

   1: 10:56:45.024244       10.10.10.101 > 192.168.10.102 icmp: echo request
   2: 10:56:45.231143       192.168.10.102 > 10.10.10.101 icmp: echo reply
   3: 10:56:45.232470       10.10.10.101 > 192.168.10.102 icmp: echo request
   4: 10:56:45.441856       192.168.10.102 > 10.10.10.101 icmp: echo reply
   5: 10:56:45.443122       10.10.10.101 > 192.168.10.102 icmp: echo request
   6: 10:56:45.652477       192.168.10.102 > 10.10.10.101 icmp: echo reply
   7: 10:56:45.653423       10.10.10.101 > 192.168.10.102 icmp: echo request
   8: 10:56:45.875397       192.168.10.102 > 10.10.10.101 icmp: echo reply
   9: 10:56:45.876450       10.10.10.101 > 192.168.10.102 icmp: echo request
  10: 10:56:46.082301       192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

   1: 10:56:45.024458       10.10.10.101 > 192.168.10.102 icmp: echo request
   2: 10:56:45.230914       192.168.10.102 > 10.10.10.101 icmp: echo reply
   3: 10:56:45.232516       10.10.10.101 > 192.168.10.102 icmp: echo request
   4: 10:56:45.441795       192.168.10.102 > 10.10.10.101 icmp: echo reply
   5: 10:56:45.443153       10.10.10.101 > 192.168.10.102 icmp: echo request
   6: 10:56:45.652432       192.168.10.102 > 10.10.10.101 icmp: echo reply
   7: 10:56:45.653454       10.10.10.101 > 192.168.10.102 icmp: echo request
   8: 10:56:45.875351       192.168.10.102 > 10.10.10.101 icmp: echo reply
   9: 10:56:45.876480       10.10.10.101 > 192.168.10.102 icmp: echo request
  10: 10:56:46.082240       192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
```

Acquisizione pacchetti su FTD (Remote FW)

```
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd# sh cap vti

10 packets captured

   1: 16:06:41.122292       100.96.2.0 > 10.10.10.102 icmp: echo request
   2: 16:06:41.124856       10.10.10.102 > 100.96.2.0 icmp: echo reply
   3: 16:06:41.329557       100.96.2.0 > 10.10.10.102 icmp: echo request
   4: 16:06:41.330442       10.10.10.102 > 100.96.2.0 icmp: echo reply
   5: 16:06:41.546327       100.96.2.0 > 10.10.10.102 icmp: echo request
   6: 16:06:41.547106       10.10.10.102 > 100.96.2.0 icmp: echo reply
   7: 16:06:41.752036       100.96.2.0 > 10.10.10.102 icmp: echo request
   8: 16:06:41.752814       10.10.10.102 > 100.96.2.0 icmp: echo reply
   9: 16:06:41.967891       100.96.2.0 > 10.10.10.102 icmp: echo request
  10: 16:06:41.968501       10.10.10.102 > 100.96.2.0 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

   1: 16:06:41.123299       100.96.2.0 > 10.10.10.102 icmp: echo request
   2: 16:06:41.124825       10.10.10.102 > 100.96.2.0 icmp: echo reply
   3: 16:06:41.330000       100.96.2.0 > 10.10.10.102 icmp: echo request
   4: 16:06:41.330396       10.10.10.102 > 100.96.2.0 icmp: echo reply
   5: 16:06:41.546800       100.96.2.0 > 10.10.10.102 icmp: echo request
   6: 16:06:41.547090       10.10.10.102 > 100.96.2.0 icmp: echo reply
   7: 16:06:41.752448       100.96.2.0 > 10.10.10.102 icmp: echo request
   8: 16:06:41.752783       10.10.10.102 > 100.96.2.0 icmp: echo reply
   9: 16:06:41.968242       100.96.2.0 > 10.10.10.102 icmp: echo request
  10: 16:06:41.968486       10.10.10.102 > 100.96.2.0 icmp: echo reply
10 packets shown
```

Prova 2. - Router 2 —> Test ping del router 1

```
Router2#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       unassigned      YES NVRAM  administratively down down
GigabitEthernet2       10.10.10.102    YES NVRAM  up                    up
GigabitEthernet3       unassigned      YES NVRAM  administratively down down
Router2#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Acquisizione pacchetti FTD (FW locale)

```
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd#
ftd#
ftd#
ftd# sh cap vti

10 packets captured

   1: 16:11:45.622450       10.10.10.102 > 172.16.10.101 icmp: echo request
   2: 16:11:45.823825       172.16.10.101 > 10.10.10.102 icmp: echo reply
   3: 16:11:45.825762       10.10.10.102 > 172.16.10.101 icmp: echo request
   4: 16:11:46.045667       172.16.10.101 > 10.10.10.102 icmp: echo reply
   5: 16:11:46.046857       10.10.10.102 > 172.16.10.101 icmp: echo request
   6: 16:11:46.252321       172.16.10.101 > 10.10.10.102 icmp: echo reply
   7: 16:11:46.253572       10.10.10.102 > 172.16.10.101 icmp: echo request
   8: 16:11:46.453803       172.16.10.101 > 10.10.10.102 icmp: echo reply
   9: 16:11:46.454764       10.10.10.102 > 172.16.10.101 icmp: echo request
  10: 16:11:46.664119       172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

   1: 16:11:45.622083       10.10.10.102 > 172.16.10.101 icmp: echo request
   2: 16:11:45.823886       172.16.10.101 > 10.10.10.102 icmp: echo reply
   3: 16:11:45.825442       10.10.10.102 > 172.16.10.101 icmp: echo request
   4: 16:11:46.045697       172.16.10.101 > 10.10.10.102 icmp: echo reply
   5: 16:11:46.046582       10.10.10.102 > 172.16.10.101 icmp: echo request
   6: 16:11:46.252352       172.16.10.101 > 10.10.10.102 icmp: echo reply
   7: 16:11:46.253313       10.10.10.102 > 172.16.10.101 icmp: echo request
   8: 16:11:46.453849       172.16.10.101 > 10.10.10.102 icmp: echo reply
   9: 16:11:46.454596       10.10.10.102 > 172.16.10.101 icmp: echo request
  10: 16:11:46.664150       172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
```

Acquisizione pacchetti ASA (Remote FW)

```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA# sh cap capin

10 packets captured

   1: 11:08:30.288391       100.103.255.195 > 10.10.10.101 icmp: echo request
   2: 11:08:30.289123       10.10.10.101 > 100.103.255.195 icmp: echo reply
   3: 11:08:30.504566       100.103.255.195 > 10.10.10.101 icmp: echo request
   4: 11:08:30.504963       10.10.10.101 > 100.103.255.195 icmp: echo reply
   5: 11:08:30.710992       100.103.255.195 > 10.10.10.101 icmp: echo request
   6: 11:08:30.711404       10.10.10.101 > 100.103.255.195 icmp: echo reply
   7: 11:08:30.917112       100.103.255.195 > 10.10.10.101 icmp: echo request
   8: 11:08:30.917402       10.10.10.101 > 100.103.255.195 icmp: echo reply
   9: 11:08:31.128243       100.103.255.195 > 10.10.10.101 icmp: echo request
  10: 11:08:31.128640       10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

   1: 11:08:30.287964       100.103.255.195 > 10.10.10.101 icmp: echo request
   2: 11:08:30.289322       10.10.10.101 > 100.103.255.195 icmp: echo reply
   3: 11:08:30.504505       100.103.255.195 > 10.10.10.101 icmp: echo request
   4: 11:08:30.505009       10.10.10.101 > 100.103.255.195 icmp: echo reply
   5: 11:08:30.710961       100.103.255.195 > 10.10.10.101 icmp: echo request
   6: 11:08:30.711434       10.10.10.101 > 100.103.255.195 icmp: echo reply
   7: 11:08:30.917066       100.103.255.195 > 10.10.10.101 icmp: echo request
   8: 11:08:30.917417       10.10.10.101 > 100.103.255.195 icmp: echo reply
   9: 11:08:31.128197       100.103.255.195 > 10.10.10.101 icmp: echo request
  10: 11:08:31.128685       10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
```

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).