

# Configura tunnel VPN da sito a sito basato su route su FTD Gestito da FMC

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Limitazioni e restrizioni](#)

[Procedura di configurazione in FMC](#)

[Verifica](#)

[Dalla GUI FMC](#)

[Da CLI FTD](#)

---

## Introduzione

In questo documento viene descritto come configurare un tunnel VPN da sito a sito basato su route statica su Firepower Threat Defense gestito da Firepower Management Center.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza base del funzionamento di un tunnel VPN.
- Comprendere come spostarsi all'interno del CCP.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Cisco Firepower Management Center (FMC) versione 6.7.0
- Cisco Firepower Threat Defense (FTD) versione 6.7.0

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 su route consente di determinare il traffico interessante da crittografare o inviare tramite tunnel VPN e di utilizzare il routing del traffico anziché policy/elenchi degli accessi, come nella VPN basata su policy o su crypto-map. 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. Ciò significa che tutto il traffico indirizzato nel tunnel IPsec viene crittografato, a prescindere dalla subnet di origine/destinazione.

Nel documento si fa riferimento alla configurazione SVTI (Static Virtual Tunnel Interface). Per la configurazione di Dynamic Virtual Tunnel Interface (DVTI) su Secure Firewall, fare riferimento a questo [documento](#).

## Limitazioni e restrizioni

Di seguito sono riportati i limiti e le restrizioni noti per i tunnel basati su route su FTD:

- Supporta solo IPsec. GRE non supportato.
- Supporta solo interfacce IPv4, IPv4, reti protette o payload VPN (nessun supporto per IPv6).
- Il routing statico e solo il protocollo BGP Dynamic Routing è supportato per le interfacce VTI che classificano il traffico per la VPN (nessun supporto per altri protocolli come OSPF, RIP e così via).
- Sono supportate solo 100 VTI per interfaccia.
- VTI non è supportato in un cluster FTD.
- VTI non è supportato in questi criteri:

QoS


NAT

· Impostazioni piattaforma


Questi algoritmi non sono più supportati in FMC/FTD versione 6.7.0 per i nuovi tunnel VPN (FMC supporta tutte le cifrature rimosse per gestire FTD < 6.7):

- Crittografia 3DES, DES e NULL non supportata nei criteri IKE.
- I gruppi DH 1, 2 e 24 non sono supportati nei criteri IKE e nelle proposte IPsec.

- Integrità MD5 non supportata nei criteri IKE.
- PRF MD5 non è supportato nei criteri IKE.
- Gli algoritmi di crittografia DES, 3DES, AES-GMAC, AES-GMAC-192 e AES-GMAC-256 non sono supportati nella proposta IPsec.

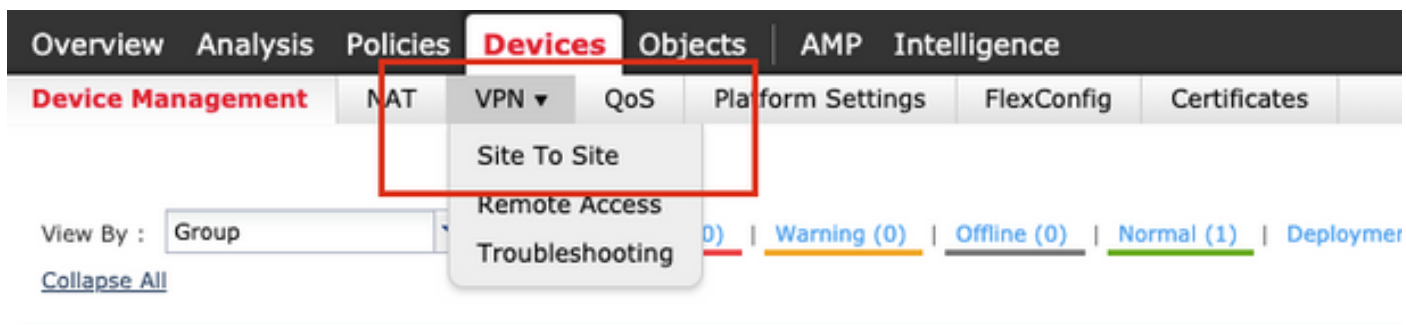
 Nota: ciò vale sia per i tunnel VPN basati su route da sito a sito che per quelli basati su criteri. Per aggiornare un FTD precedente alla versione 6.7 da FMC, viene attivato un controllo di pre-convalida che avvisa l'utente delle modifiche relative alle cifrature rimosse che bloccano l'aggiornamento.

FTD 6.7 gestito tramite FMC 6.7	Configurazione disponibile	Tunnel VPN da sito a sito
Nuova installazione	Sono disponibili cifrari deboli, ma non possono essere utilizzati per configurare il dispositivo FTD 6.7.	Sono disponibili cifrari deboli, ma non possono essere utilizzati per configurare il dispositivo FTD 6.7.
Aggiornamento: FTD configurato solo con cifratura debole	Aggiornamento da FMC 6.7 UI, un controllo di pre-convalida visualizza un errore. L'aggiornamento è bloccato fino alla riconfigurazione.	Dopo l'aggiornamento FTD e presupponendo che il peer non abbia modificato le proprie impostazioni, il tunnel viene terminato.
Aggiornamento: FTD configurato solo con alcune cifrature deboli e alcune cifrature forti	Aggiornamento da FMC 6.7 UI, un controllo di pre-convalida visualizza un errore. L'aggiornamento è bloccato fino alla riconfigurazione.	Dopo l'aggiornamento del FTD e presupponendo che il peer disponga di cifrature efficaci, il tunnel viene ristabilito.
Aggiornamento: paese di classe C (non si dispone di una licenza di crittografia efficace)	Consenti DES è consentito	Consenti DES è consentito

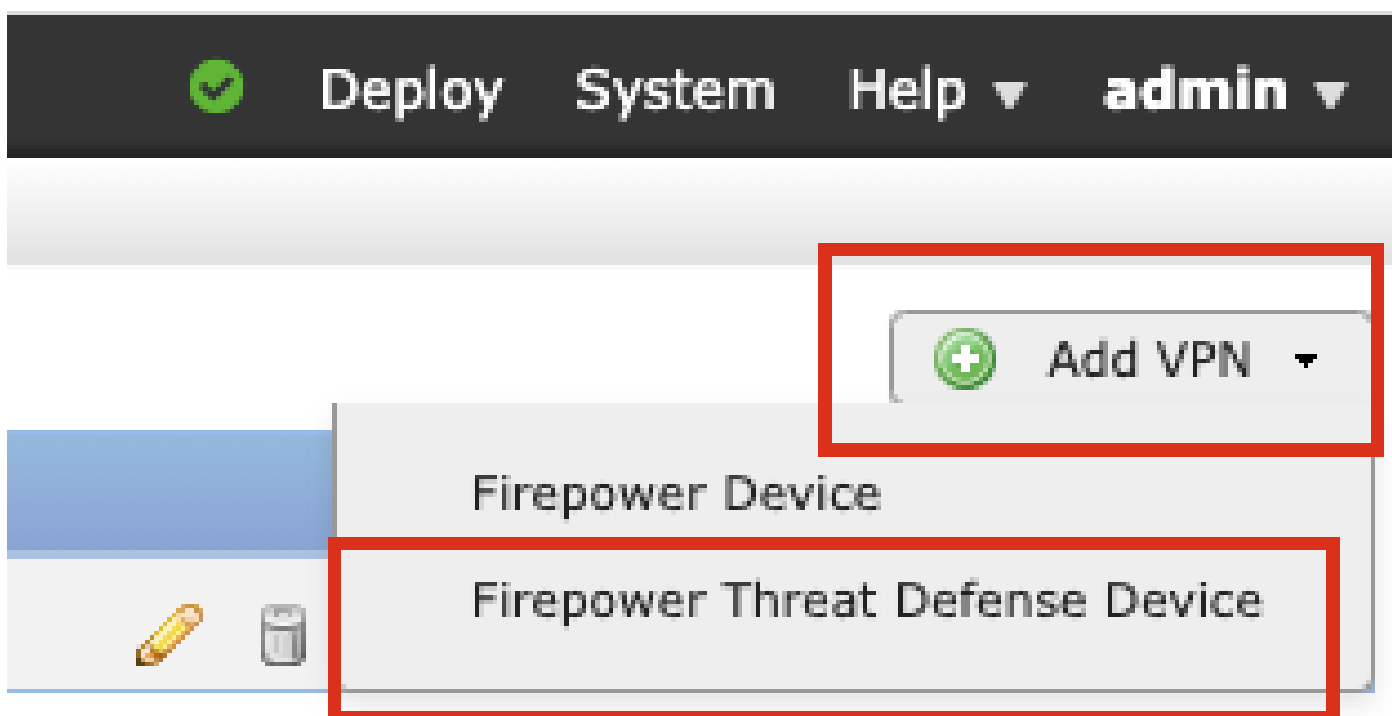
 Nota: non sono necessarie licenze aggiuntive. La VPN basata su route può essere configurata in modalità Licensed e Evaluation. Senza la conformità alla crittografia (funzionalità di esportazione controllate abilitate), solo DES può essere utilizzato come algoritmo di crittografia.

## Procedura di configurazione in FMC

Passaggio 1. Passare a Dispositivi > VPN > Sito-sito.



Passaggio 2. Fare clic su Add VPN (Aggiungi VPN), quindi selezionare Firepower Threat Defense Device, come mostrato nell'immagine.



Passaggio 3. Fornire un nome di topologia e selezionare il tipo di VPN come VTI (Route Based). Scegliere la versione IKE.

Ai fini della presente dimostrazione:

Nome topologia: VTI-ASA

Versione IKE: IKEv2

Topology Name:\*

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:

IKE Version:\*  IKEv1  IKEv2

Passaggio 4. Selezionare il dispositivo su cui configurare il tunnel, scegliere di aggiungere una nuova interfaccia di modello virtuale (fare clic sull'icona +) oppure selezionarne una dall'elenco esistente.

Endpoints | IKE | IPsec | Advanced

**Node A**

Device:\*

Virtual Tunnel Interface:\*

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

Connection Type:\*

Tunnel IP Address :  
Tunnel Source Interface :  
Tunnel Source Interface IP :

**Node B**

Device:\*

Virtual Tunnel Interface:\*

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

Connection Type:\*

Tunnel IP Address :  
Tunnel Source Interface :  
Tunnel Source Interface IP :

Passaggio 5. Definire i parametri della nuova interfaccia del tunnel virtuale. Fare clic su OK.

Ai fini della presente dimostrazione:

Nome: VTI-ASA

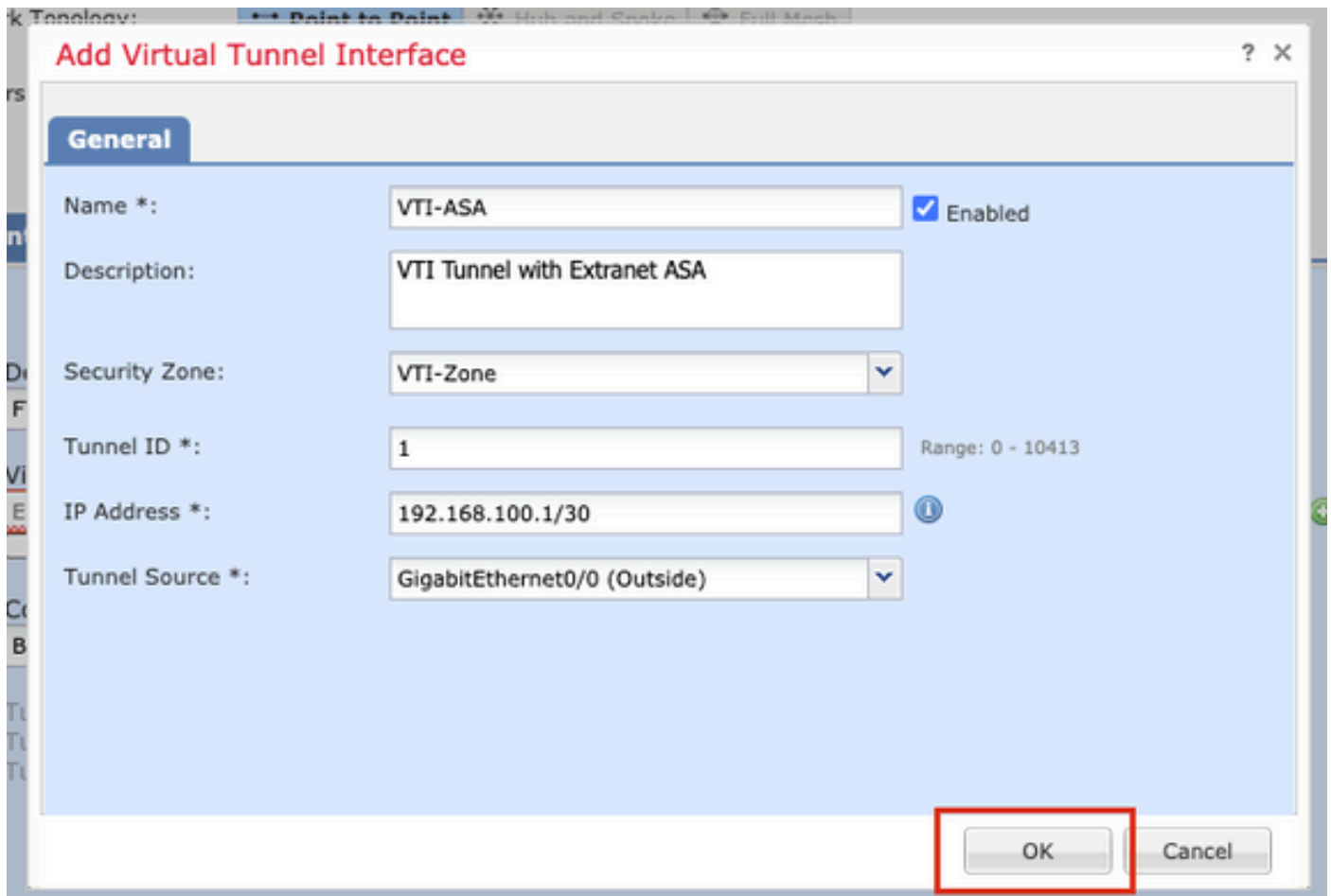
Descrizione (Facoltativa): tunnel VTI con ASA Extranet

Area di sicurezza: VTI-Zone

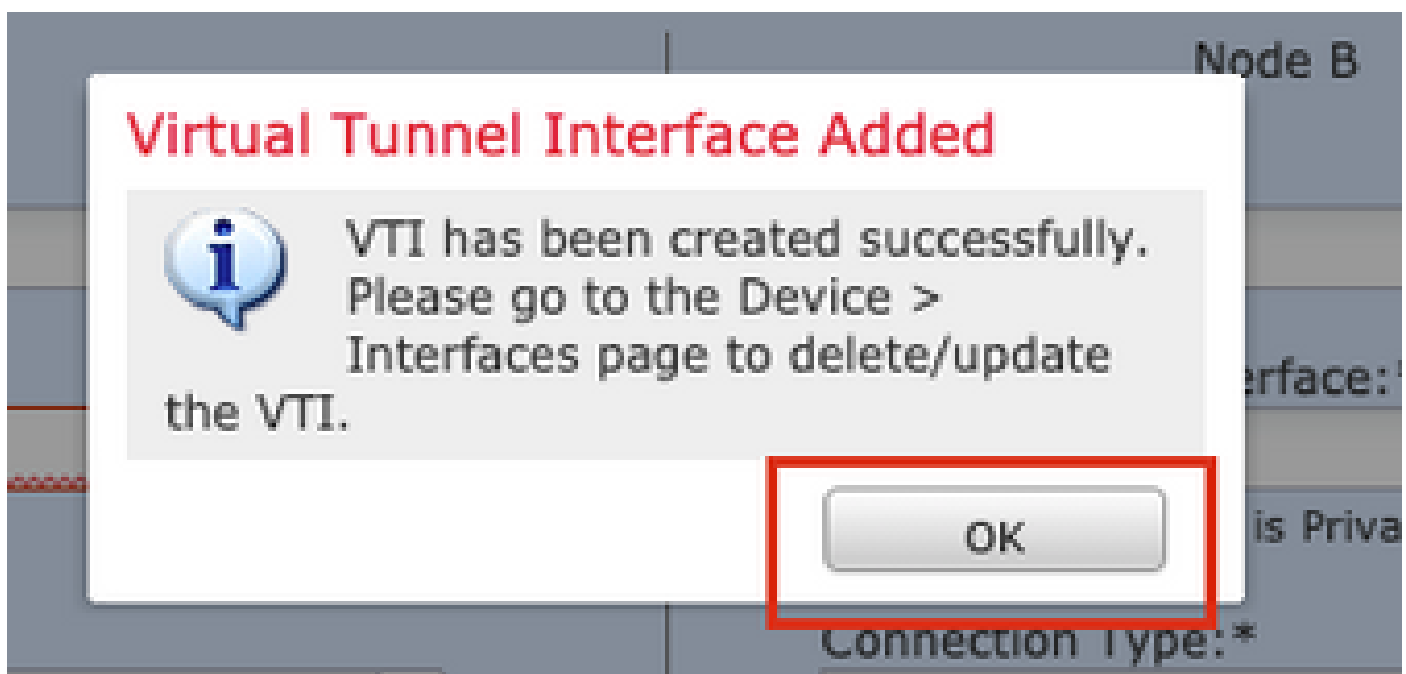
ID tunnel: 1

Indirizzo IP: 192.168.100.1/30

Origine tunnel: Gigabit Ethernet0/0 (esterna)



Passaggio 6. Fare clic su OK nel popup per indicare che la nuova VTI è stata creata.



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

Ai fini della presente dimostrazione:

Dispositivo: Extranet

Nome dispositivo: ASA-Peer

Indirizzo IP endpoint: 10.106.67.252

**Create New 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 IP is Private [Edit VTI](#)

Connection Type: \*

Tunnel IP Address : 192.168.100.1  
Tunnel Source Interface : Outside  
Tunnel Source Interface IP : 10.197.224.90

Additional Configuration ⓘ  
Route traffic to the VTI : [Routing Policy](#)  
Permit VPN traffic : [AC Policy](#)

**Node B**


Device: \*

Device Name: \*

Endpoint IP Address: \*

Passaggio 8. Passare alla scheda IKE. È possibile scegliere di utilizzare un criterio predefinito oppure fare clic sul pulsante + accanto alla scheda Criterio per crearne uno nuovo.

**IKEv2 Settings**

Policy:\* AES-GCM-NULL-SHA-LATEST 

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:\* 24 Characters (Range 1-127)

Passaggio 9. (Facoltativo, se si crea un nuovo criterio IKEv2.) Fornire un nome per il criterio e selezionare gli algoritmi da utilizzare nel criterio. Fare clic su Save (Salva).

Ai fini della presente dimostrazione:

Nome: ASA-IKEv2-Policy

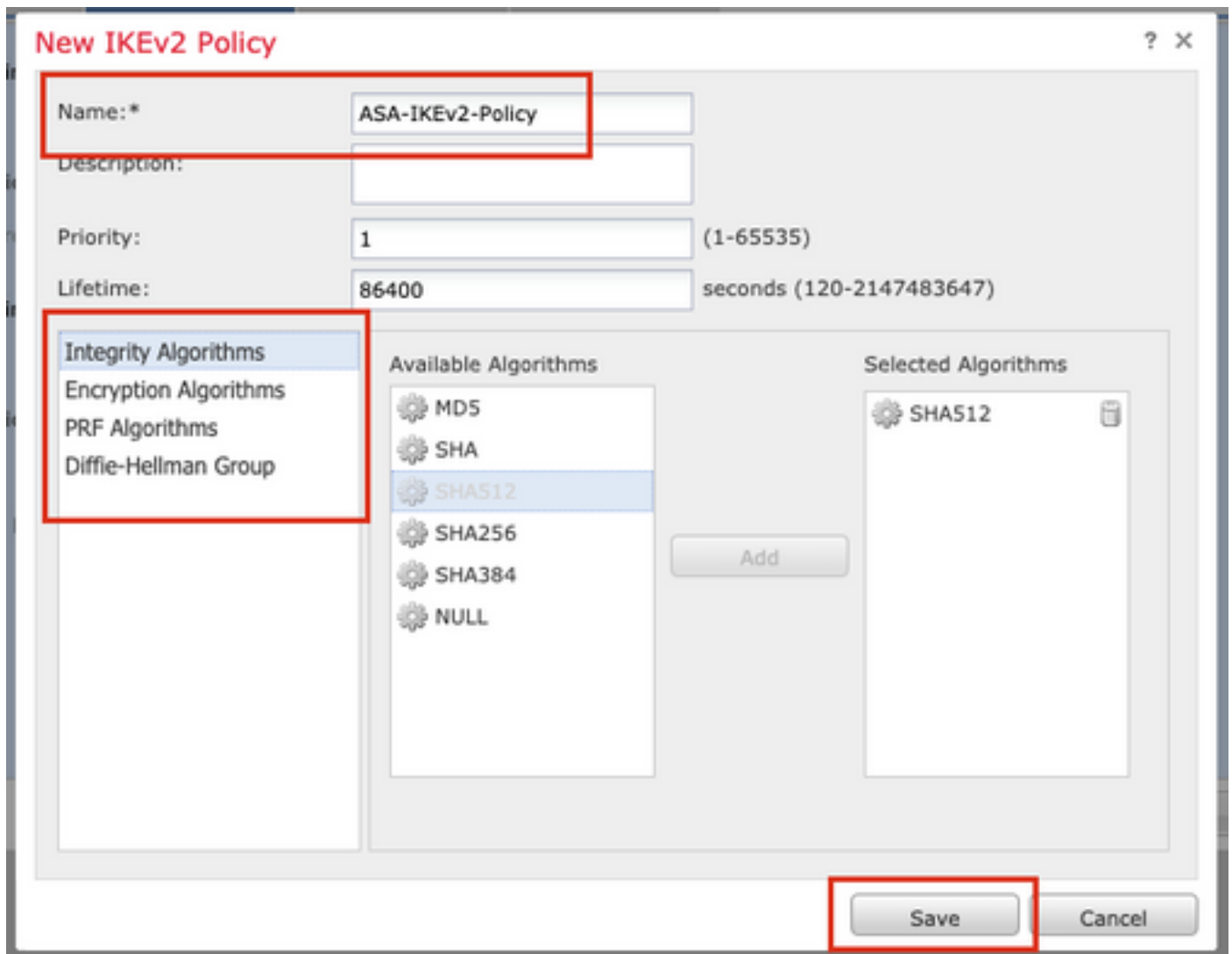
Algoritmi di integrità: SHA-512

Algoritmi di crittografia: AES-256

Algoritmi PRF: SHA-512

Gruppo Diffie-Hellman: 21





Passaggio 10. Scegliere il nuovo criterio o il criterio esistente. Selezionare il tipo di autenticazione. Se si utilizza una chiave manuale già condivisa, specificare la chiave nelle caselle Chiave e Conferma chiave.

Ai fini della presente dimostrazione:

Criterio: ASA-IKEv2-Policy


Tipo di autenticazione: chiave manuale già condivisa


Chiave: cisco123

Chiave di conferma: cisco123

Endpoints **IKE** IPsec Advanced

**IKEv1 Settings**


Policy:\* preshared\_sha\_aes256\_dh14\_3 


Authentication Type: Pre-shared Automatic Key 

Pre-shared Key Length:\* 24 Characters (Range 1-127)

---

**IKEv2 Settings**


Policy:\* ASA-IKEv2-Policy 

Authentication Type: Pre-shared Manual Key 

Key:\*


Confirm Key:\*

Enforce hex-based pre-shared key only


 Nota: se entrambi gli endpoint sono registrati sullo stesso FMC, è possibile utilizzare anche l'opzione di chiave automatica precondivisa.


Passaggio 11. Passare alla scheda IPsec. È possibile scegliere di utilizzare una proposta IPsec IKEv2 predefinita o crearne una nuova. Fare clic sul pulsante Modifica accanto alla scheda Proposta IPsec IKEv2.

Crypto Map Type:  Static  Dynamic

IKEv2 Mode: Tunnel 

Transform Sets:

IKEv1 IPsec Proposals  tunnel\_aes256\_sha

IKEv2 IPsec Proposals\*  AES-GCM

Enable Security Association (SA) Strength Enforcement

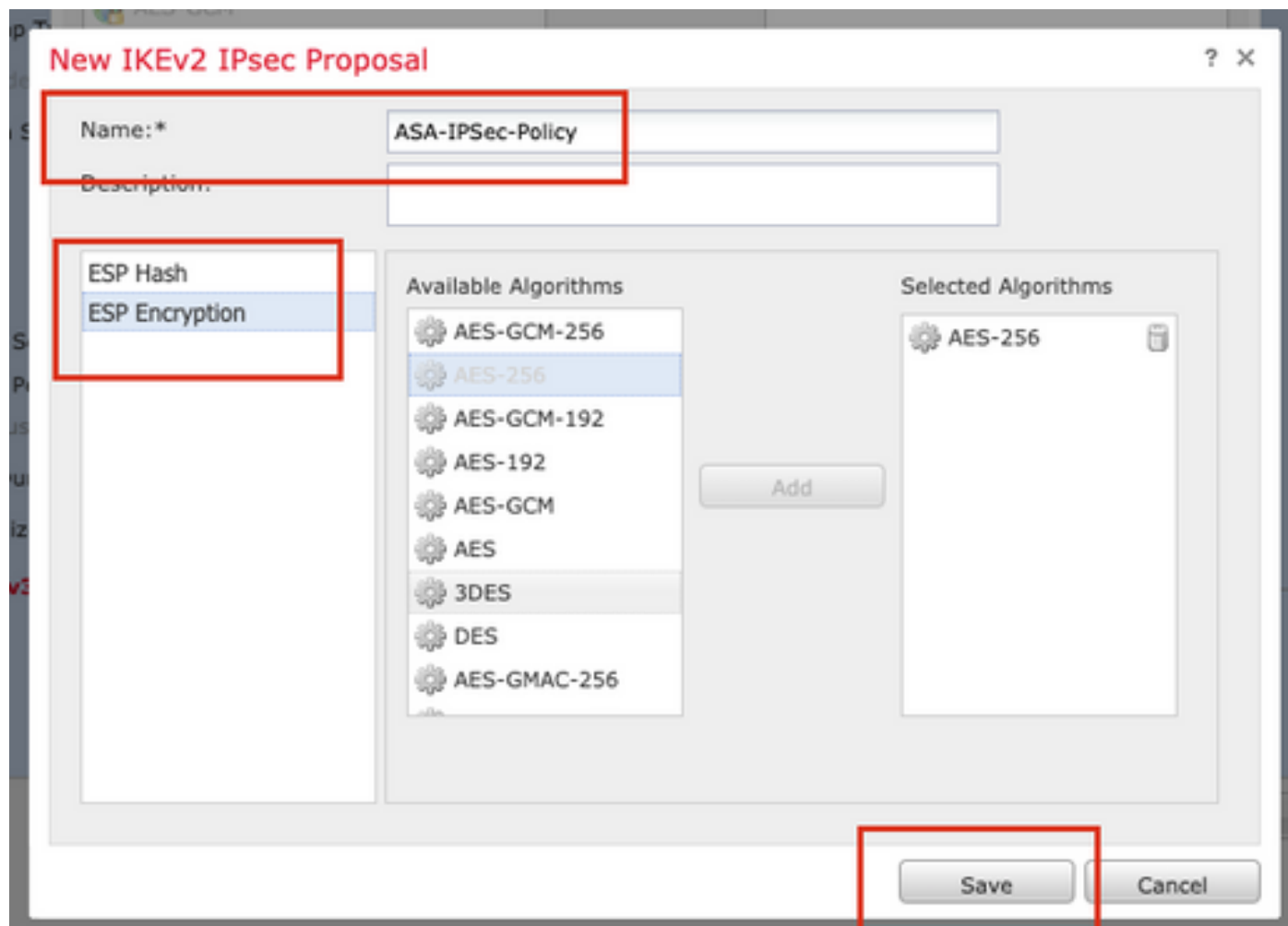
Passaggio 12. (Facoltativo, se si crea una nuova proposta IPsec IKEv2.) Fornire un nome per la proposta e selezionare gli algoritmi da utilizzare nella proposta. Fare clic su Save (Salva).

Ai fini della presente dimostrazione:

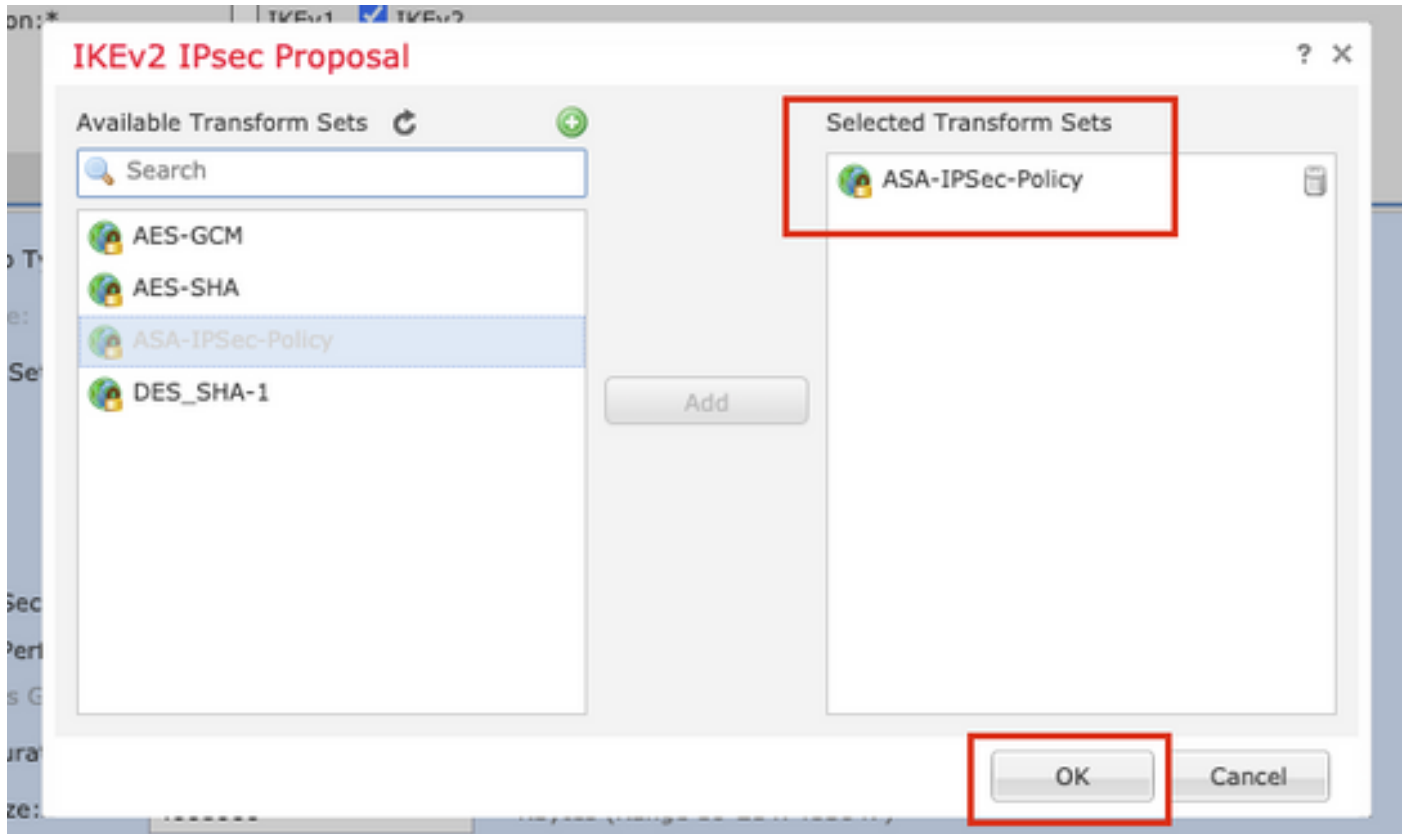
Nome: ASA-IPSec-Policy

Hash ESP: SHA-512

Crittografia ESP: AES-256



Passaggio 13. Scegliere la proposta o la proposta appena creata dall'elenco delle proposte disponibili. Fare clic su OK.



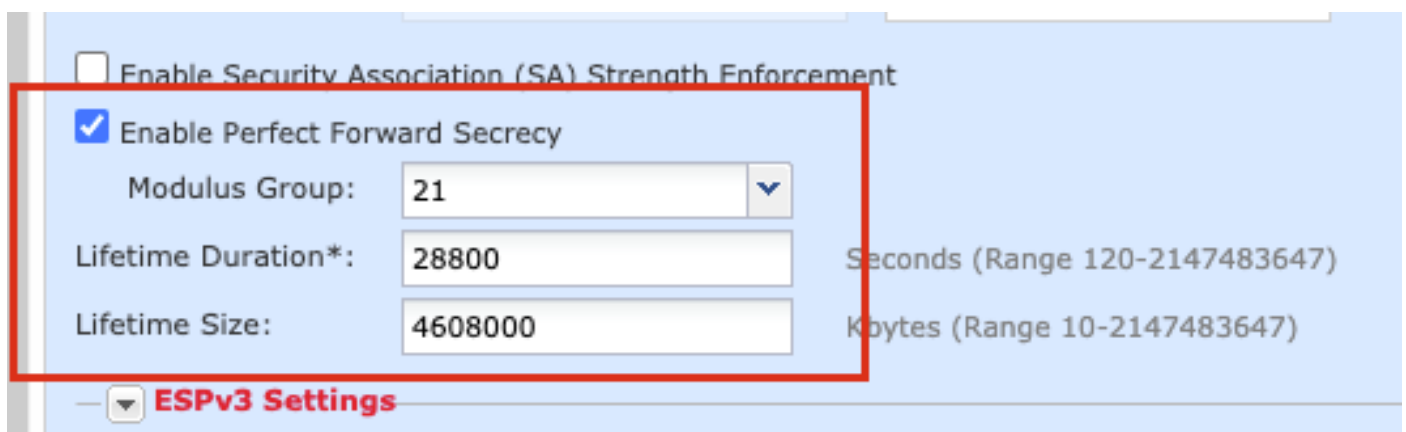
Passaggio 14. (Facoltativo) Scegliere le impostazioni Perfect Forward Secrecy. Configurare Durata IPsec e Dimensione durata.

Ai fini della presente dimostrazione:

Perfect Forward Secrecy: Gruppo di moduli 21

Durata: 28800 (predefinita)

Dimensione durata: 4608000 (predefinita)



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

Topology Name:\*

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:

IKE Version:\*  IKEv1  IKEv2

---

Endpoints | IKE | **IPsec** | Advanced

Crypto Map Type:  Static  Dynamic

IKEv2 Mode:

Transform Sets: **IKEv1 IPsec Proposals**  **IKEv2 IPsec Proposals\***

Enable Security Association (SA) Strength Enforcement

Enable Perfect Forward Secrecy


Modulus Group:

Lifetime Duration\*:  Seconds (Range 120-2147483647)

Lifetime Size:  Kbytes (Range 10-2147483647)

— **ESPv3 Settings** —

Passaggio 16. Configurare i criteri di controllo di accesso. Passare a Policy > Controllo accesso > Controllo accesso. Modificare il criterio applicato all'FTD.

 Nota: il protocollo allow-vpn della connessione syspot non funziona con tunnel VPN basati su route. Le regole di controllo d'accesso devono essere configurate sia per le zone IN->OUT che per le zone OUT -> IN.

Specificare le zone di origine e di destinazione nella scheda Zone.

Specificare le reti di origine e di destinazione nella scheda Reti. Fare clic su Add.

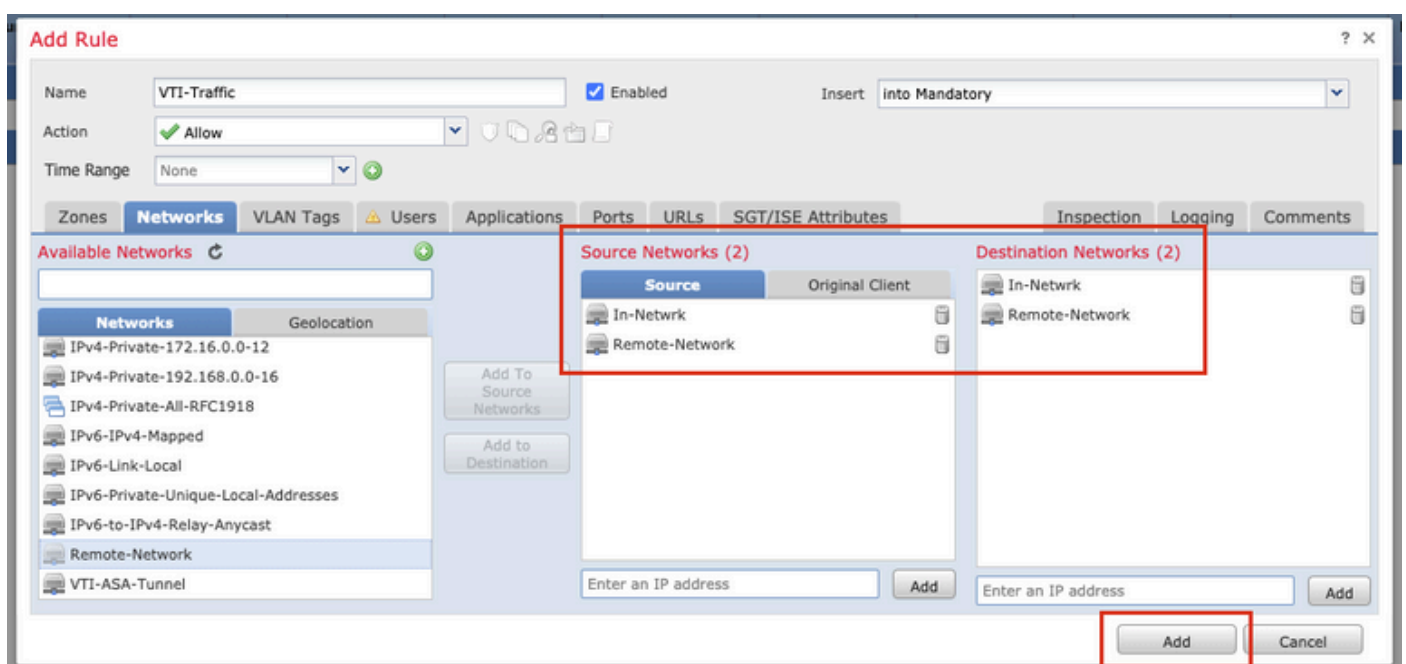
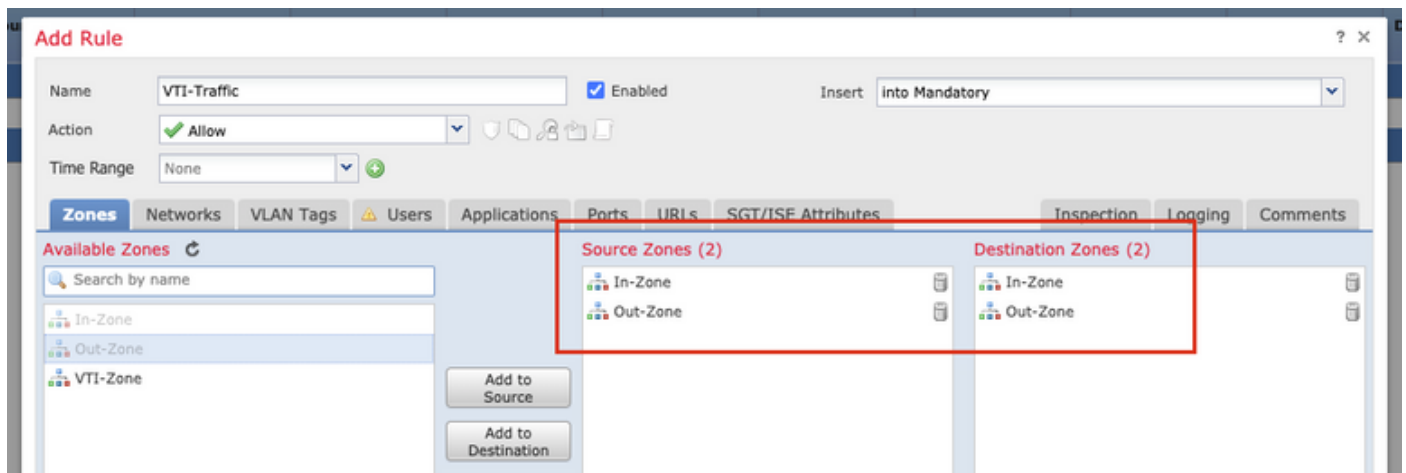
Ai fini della presente dimostrazione:

Zone di origine: zona interna e zona esterna

Zone di destinazione: zona esterna e zona interna

Reti di origine: in rete e rete remota

Reti di destinazione: rete remota e in rete



Passaggio 17. Aggiungere il routing sul tunnel VTI. Selezionare Dispositivi > Gestione dispositivi. Modificare il dispositivo su cui è configurato il tunnel VTI.

Passare a Instradamento statico nella scheda Instradamento. Fare clic su Aggiungi instradamento.

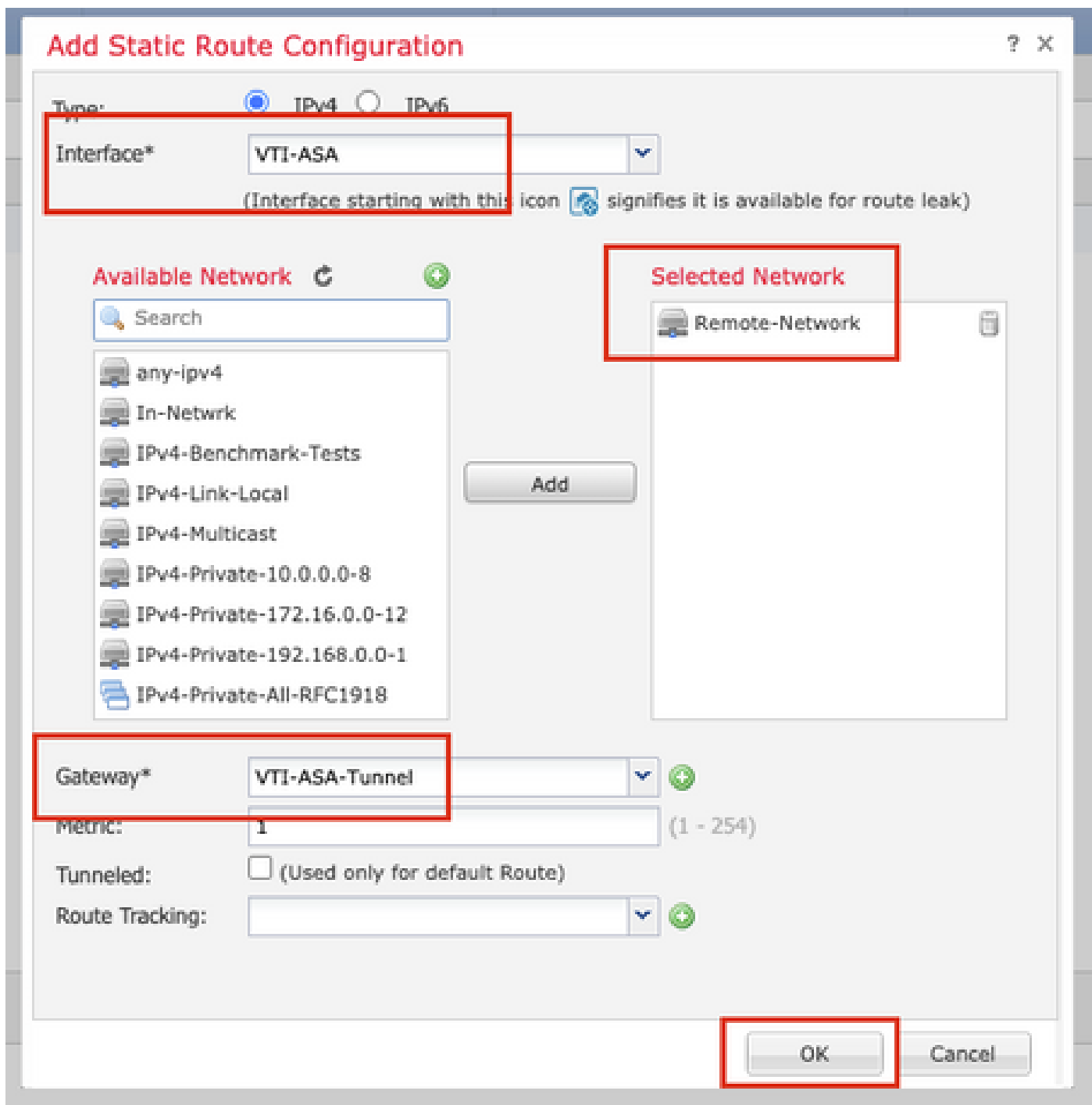
Fornire l'interfaccia, scegliere la rete, fornire il gateway. Fare clic su OK.

Ai fini della presente dimostrazione:

Interfaccia: VTI-ASA

Rete: rete remota

Gateway: tunnel VTI-ASA



Passaggio 18. Passare a Distribuisce > Distribuzione. Selezionare l'FTD in cui distribuire la configurazione e fare clic su Distribuisce.

Push della configurazione nella CLI FTD dopo la corretta distribuzione:

```
<#root>
```

```
crypto ikev2 policy 1
```

```
encryption aes-256  
integrity sha512  
group 21  
prf sha512  
lifetime seconds 86400
```

```
crypto ikev2 enable Outside

crypto ipsec ikev2 ipsec-proposal CSM_IP_1

  protocol esp encryption aes-256
  protocol esp integrity sha-512

crypto ipsec profile FMC_IPSEC_PROFILE_1

  set ikev2 ipsec-proposal CSM_IP_1
  set pfs group21

group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
  vpn-idle-timeout 30
  vpn-idle-timeout alert-interval 1
  vpn-session-timeout none
  vpn-session-timeout alert-interval 1
  vpn-filter none
  vpn-tunnel-protocol ikev1 ikev2

tunnel-group 10.106.67.252 type ipsec-l2l
tunnel-group 10.106.67.252 general-attributes
  default-group-policy .DefaultS2SGroupPolicy
tunnel-group 10.106.67.252 ipsec-attributes
  ikev2 remote-authentication pre-shared-key *****
  ikev2 local-authentication pre-shared-key *****

interface Tunnel1

  description VTI Tunnel with Extranet ASA
  nameif VTI-ASA

  ip address 192.168.100.1 255.255.255.252
  tunnel source interface Outside
  tunnel destination 10.106.67.252
  tunnel mode ipsec ipv4

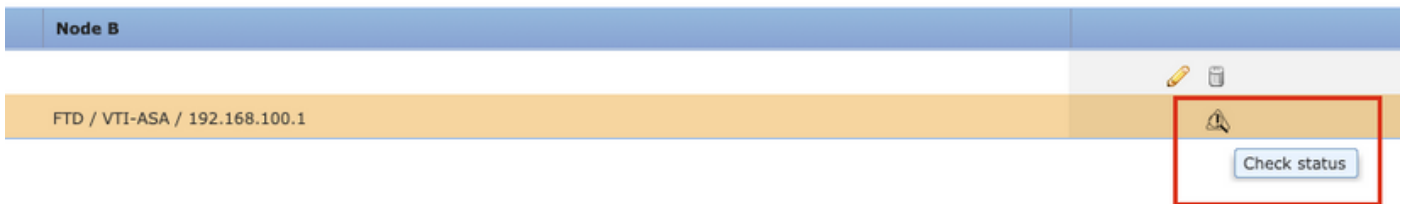
  tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

## Verifica

### Dalla GUI FMC

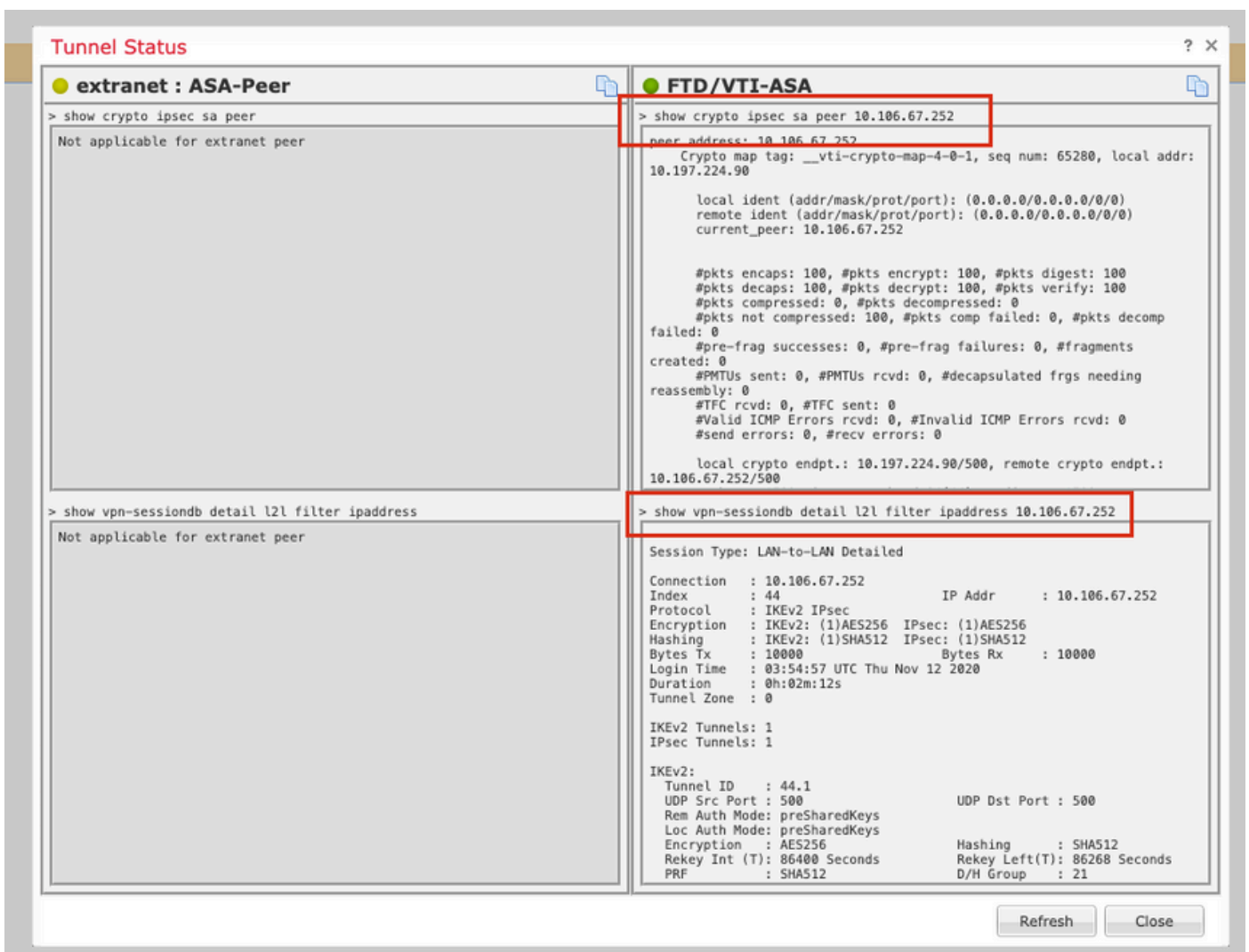
Fare clic sull'opzione Check Status (Verifica stato) per monitorare lo stato del tunnel VPN dalla GUI stessa





Ciò include questi comandi presi dalla CLI FTD:

- show crypto ipsec sa peer <Indirizzo IP peer>
- show vpn-sessiondb detail l2l filter ipaddress <Indirizzo IP peer>



Da CLI FTD

Questi comandi possono essere usati dalla CLI di FTD per visualizzare la configurazione e lo stato dei tunnel VPN.

```
show running-config crypto
show running-config nat
```

```
show running-config route
show crypto ikev1 sa detailed
show crypto ikev2 sa detailed
show crypto ipsec sa detailed
show vpn-sessiondb detail 121
```

## 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).