

# Configurazione VPN da sito a sito su FTD Gestita da FMC

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Passaggio 1. Definire la topologia VPN.](#)

[Passaggio 2. Configurare i parametri IKE.](#)

[Passaggio 3. Configurare i parametri IPsec.](#)

[Passaggio 4. Ignorare il controllo di accesso.](#)

[Passaggio 5. Creare un criterio di controllo dell'accesso.](#)

[Passaggio 6. Configurare l'esenzione NAT.](#)

[Passaggio 7. Configurare l'ASA.](#)

[Verifica](#)

[Risoluzione dei problemi e debug](#)

[Problemi iniziali di connettività](#)

[Problemi specifici del traffico](#)

## Introduzione

Questo documento fornisce un esempio di configurazione per la VPN da sito a sito su Firepower Threat Defense (FTD) gestita da FMC.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di VPN
- Esperienza con Firepower Management Center
- Esperienza con la riga di comando ASA

### Componenti usati

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

- Cisco FTD 6.5
- ASA 9.10(1)32

- IKEv2

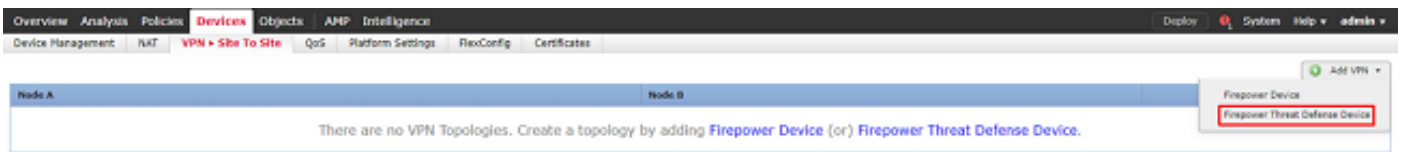
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

## Configurazione

Iniziare con la configurazione su FTD con FirePower Management Center.

### Passaggio 1. Definire la topologia VPN.

1. Passare a **Dispositivi > VPN > Da sito a sito**. In **Aggiungi VPN**, fare clic su **Dispositivo Firepower Threat Defense**, come mostrato in questa immagine.



2. Viene visualizzata la casella **Crea nuova topologia VPN**. Dai a VPN un nome che sia facilmente identificabile.

Topologia della rete: Punto-punto

Versione IKE: IKEv2

In questo esempio, quando si selezionano gli endpoint, il nodo A è l'FTD e il nodo B è l'ASA. Fare clic sul pulsante più verde per aggiungere dispositivi alla topologia, come mostrato nell'immagine.

### Create New VPN Topology

Topology Name:\*

Network Topology:  Point to Point  Hub and Spoke  Full Mesh

IKE Version:\*  IKEv1  IKEv2

**Endpoints** | IKE | IPsec | Advanced

Node A: +

Device Name	VPN Interface	Protected Networks

Node B: +

Device Name	VPN Interface	Protected Networks

**i** Ensure the protected networks are allowed by access control policy of each device.

3. Aggiungere l'FTD come primo endpoint.

Selezionare l'interfaccia su cui deve essere posizionata una mappa crittografica. L'indirizzo IP deve essere popolato automaticamente dalla configurazione del dispositivo.

Fare clic sul segno più verde in Reti protette, come mostrato in questa immagine, per selezionare le subnet da crittografare in questa VPN.

## Add Endpoint




Device:\*

Interface:\*


IP Address:\*

This IP is Private

Connection Type:

Certificate Map:  

Protected Networks:\*

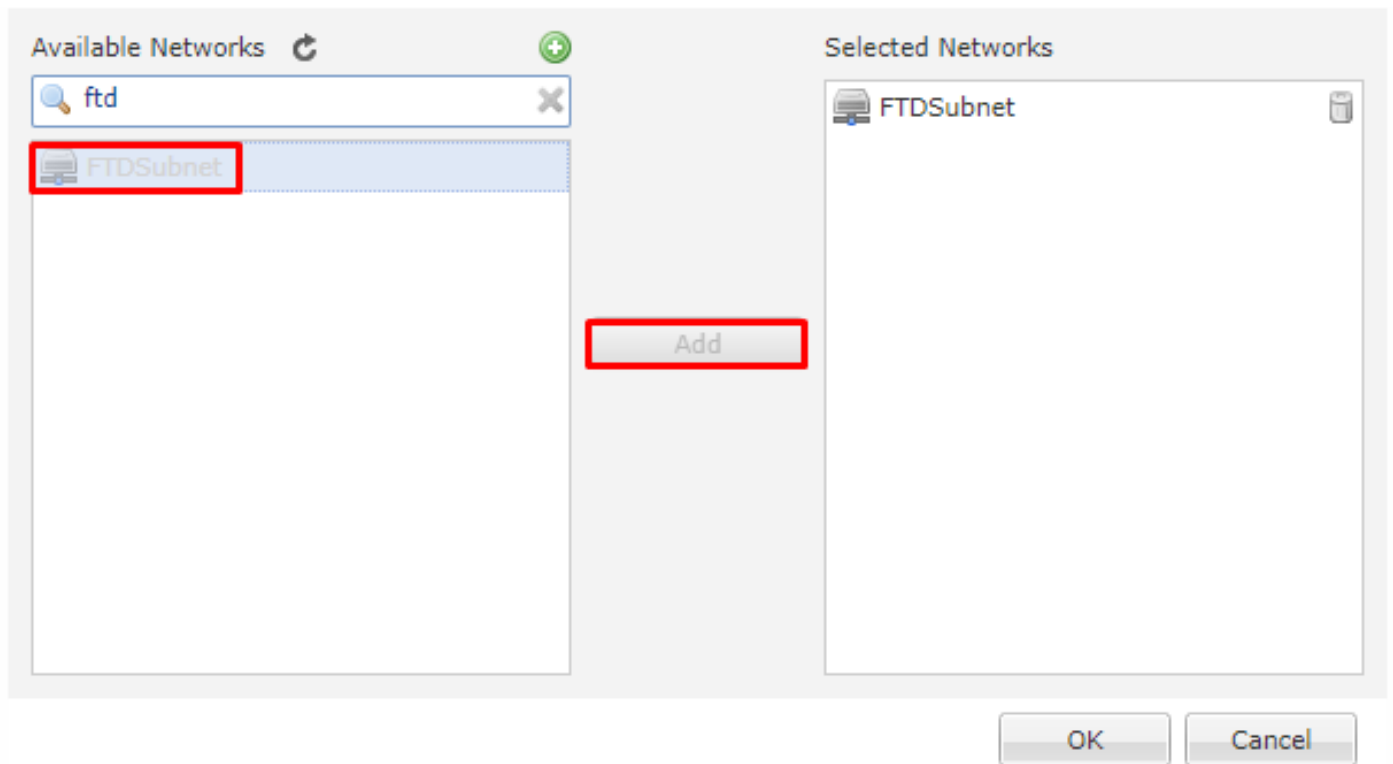
Subnet / IP Address (Network)  Access List (Extended) 

4. Fare clic sul segno più verde per creare un oggetto di rete.

5. Aggiungere all'FTD tutte le subnet locali da cifrare. Fare clic su **Aggiungi** per spostarli nelle reti selezionate. Fare clic su **OK**, come mostrato nell'immagine.

FTDSubnet = 10.10.113.0/24

## Network Objects



Nodo A: (FTD) completato. Fare clic sul segno più verde per il Nodo B, come mostrato nell'immagine.

### Create New VPN Topology

Topology Name: RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:  IKEv1  IKEv2

**Endpoints** IKE IPsec Advanced

Node A:

Device Name	VPN Interface	Protected Networks
FTD	outside/172.16.100.20	FTDSubnet

Node B:

Device Name	VPN Interface	Protected Networks
-------------	---------------	--------------------

ⓘ Ensure the protected networks are allowed by access control policy of each device.

Save Cancel

Il nodo B è un'ASA. I dispositivi non gestiti dal FMC sono considerati Extranet.

6. Aggiungere un nome di dispositivo e un indirizzo IP. Fare clic sul segno più verde per aggiungere reti protette, come mostrato nell'immagine.

## Edit Endpoint



Device:\*

Device Name:\*

IP Address:\*  Static  Dynamic

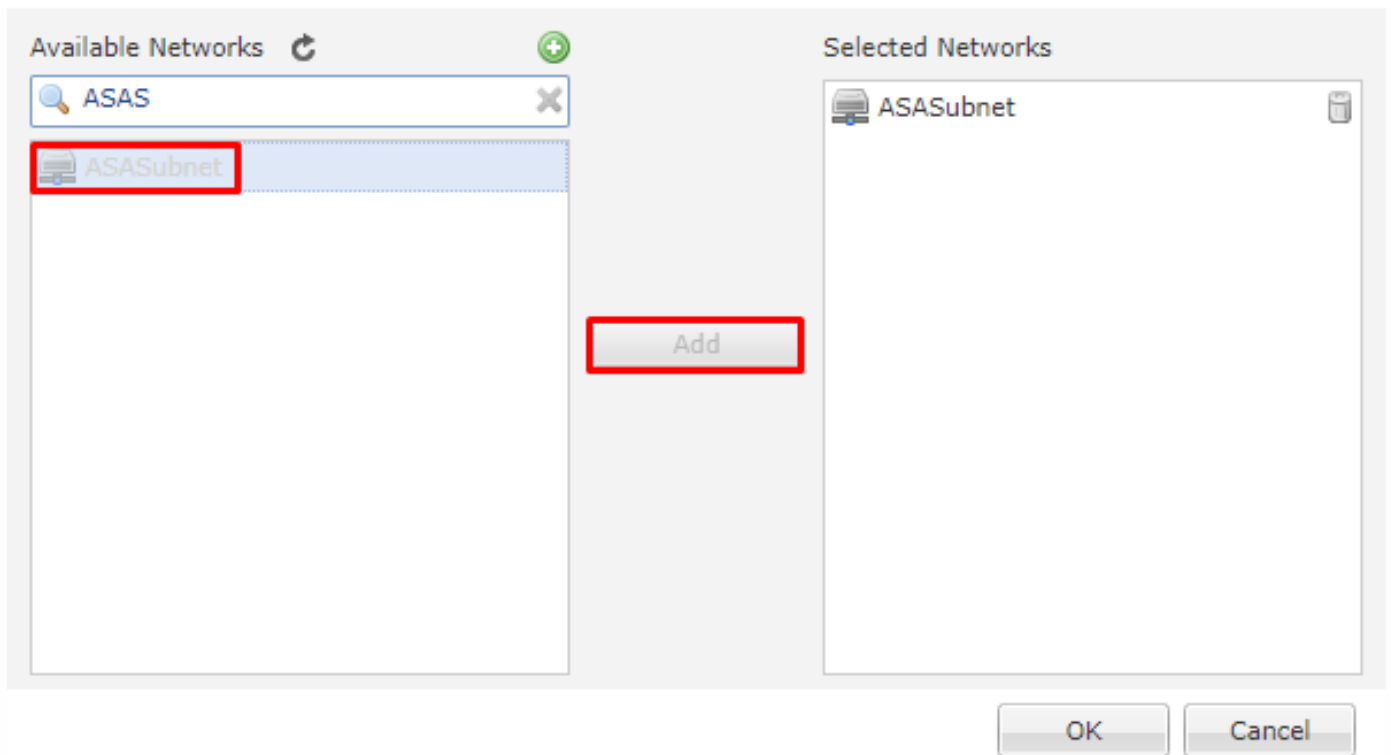
Certificate Map:

Protected Networks:\*  
 Subnet / IP Address (Network)  Access List (Extended)

7. Come mostrato in questa immagine, selezionare le **subnet ASA** da crittografare e aggiungerle alle reti selezionate.

Subnet ASA = 10.10.110.0/24

## Network Objects



### Passaggio 2. Configurare i parametri IKE.

A questo punto, entrambi gli endpoint vengono configurati tramite IKE/IPSEC.

1. Nella scheda **IKE** specificare i parametri utilizzati per lo scambio iniziale di IKEv2. Fare clic sul segno più verde per creare un nuovo criterio IKE, come mostrato nell'immagine.



### Create New VPN Topology

Topology Name:\* RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:\*  IKEv1  IKEv2

Endpoints **IKE** IPsec Advanced

**IKEv1 Settings**

Policy:\* preshared\_sha\_aes256\_dh5\_5

Authentication Type: Pre-shared Automatic Key

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

**IKEv2 Settings**

Policy:\* AES-GCM-NULL-SHA

Authentication Type: Pre-shared Automatic Key

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

Save Cancel

2. Nella nuova regola IKE, specificare un numero di priorità e la durata della fase 1 della connessione. Questo documento utilizza questi parametri per lo scambio iniziale: Integrità (SHA256), Crittografia (AES-256), PRF (SHA256) e Gruppo Diffie-Hellman (Gruppo 14)

**Nota:** Tutti i criteri IKE nel dispositivo vengono inviati al peer remoto indipendentemente dal contenuto della sezione criteri selezionata. Per la connessione VPN verrà selezionato il primo criterio IKE corrispondente al peer remoto. Scegliere il criterio da inviare per primo utilizzando il campo Priorità. La priorità 1 verrà inviata per prima.

# New IKEv2 Policy

Name:\*

Description:

Priority:  (1-65535)

Lifetime:  seconds (120-2147483647)

- Integrity Algorithms**
- Encryption Algorithms
- PRF Algorithms
- Diffie-Hellman Group

- Available Algorithms
- MD5
  - SHA
  - SHA512
  - SHA256**
  - SHA384
  - NULL

Add

- Selected Algorithms
- SHA256

Save Cancel

# New IKEv2 Policy

Name:\*

Description:

Priority:  (1-65535)

Lifetime:  seconds (120-2147483647)

Integrity Algorithms

**Encryption Algorithms**

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- AES
- AES-256
- DES
- 3DES
- AES-192
- AES-GCM
- AES-GCM-192
- AES-GCM-256
- NULL

Add

Selected Algorithms

- AES-256

## New IKEv2 Policy



Name:\*

Description:

Priority:  (1-65535)

Lifetime:  seconds (120-2147483647)

- Integrity Algorithms
- Encryption Algorithms
- PRF Algorithms**
- Diffie-Hellman Group

### Available Algorithms

- MD5
- SHA
- SHA512
- SHA256
- SHA384

Add

### Selected Algorithms

- SHA256

Save Cancel

## New IKEv2 Policy



Name:\*

Description:

Priority:  (1-65535)

Lifetime:  seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

**Diffie-Hellman Group**

Available Groups

- 1
- 2
- 5
- 14**
- 15
- 16
- 19
- 20
- 21

Add

Selected Groups

- 14

Save Cancel

- Una volta aggiunti i parametri, selezionare questo criterio e scegliere il **tipo di autenticazione**.
- Scegliere manuale **pre-chiave condivisa**. Per questo documento viene usato PSK cisco123.

### Create New VPN Topology

Topology Name:\* RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:\*  IKEv1  IKEv2

Endpoints **IKE** IPsec Advanced

**IKEv1 Settings**

Policy:\* preshared\_sha\_aes256\_dh5\_5

Authentication Type: Pre-shared Automatic Key

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

**IKEv2 Settings**

Policy:\* **ASA**

Authentication Type: **Pre-shared Manual Key**

Key:\* .....

Confirm Key:\* .....

Enforce hex-based pre-shared key only

Save Cancel

### Passaggio 3. Configurare i parametri IPsec.

1. In **IPsec**, fare clic sulla matita per modificare il set di trasformazioni e creare una nuova proposta IPsec, come mostrato nell'immagine.

## Create New VPN Topology

? x

Topology Name:\* RTPVPN-ASA


Network Topology: **Point to Point** Hub and Spoke Full Mesh


IKE Version:\*  IKEv1  IKEv2

Endpoints IKE **IPsec** Advanced

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

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group: 14

Lifetime Duration\*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

— **ESPv3 Settings**

Save Cancel

2. Per creare una nuova proposta IPsec IKEv2, fare clic sul segno più verde e immettere i parametri della fase 2.

Selezionare **Crittografia ESP > AES-GCM-256**. Quando si utilizza l'algoritmo GCM per la crittografia, non è necessario utilizzare un algoritmo Hash. Con GCM la funzione hash è integrata.

## Edit IKEv2 IPsec Proposal



Name:\* ASA

Description:

ESP Hash

ESP Encryption

Available Algorithms

- AES-GCM-256
- AES-256
- AES-GCM-192
- AES-192
- AES-GCM
- AES
- 3DES
- DES
- AES-GMAC-25

Add

Selected Algorithms

- AES-GCM-256

Save Cancel

3. Dopo aver creato la nuova proposta IPsec, aggiungerla ai set di trasformazioni selezionati.

## IKEv2 IPsec Proposal



Available Transform Sets

Search

- AES-GCM
- AES-SHA
- ASA
- DES\_SHA-1

Add

Selected Transform Sets

- ASA

OK Cancel

La nuova proposta IPsec selezionata viene ora elencata in Proposte IPsec IKEv2.



Se necessario, è possibile modificare la durata della fase 2 e l'opzione PFS. Per questo esempio, la durata verrà impostata come predefinita e PFS verrà disattivato.

**Create New VPN Topology**

Topology Name: RTPVPN-ASA

Network Topology: Point to Point | Hub and Spoke | Full Mesh

IKE Version:  IKEv1  IKEv2

Endpoints | IKE | **IPsec** | Advanced

Crypto Map Type:  Static  Dynamic

IKEv2 Mode: Tunnel

Transform Sets:

- IKEv1 IPsec Proposals: tunnel\_aes256\_sha
- IKEv2 IPsec Proposals: ASA

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group: 14

Lifetime Duration\*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

ESPv3 Settings

Save Cancel

Facoltativo: è necessario completare l'opzione Ignora controllo di accesso o Crea criteri di controllo di accesso.

#### Passaggio 4. Ignorare il controllo di accesso.

Facoltativamente, è possibile abilitare `sysopt allow-vpn` in **Advanced > Tunnel**.

In questo modo non è più possibile utilizzare i criteri di controllo di accesso per ispezionare il traffico proveniente dagli utenti. Per filtrare il traffico degli utenti, è comunque possibile usare filtri VPN o ACL scaricabili. Questo è un comando globale e verrà applicato a tutte le VPN se questa casella di controllo è abilitata.

**Create New VPN Topology** ? X

Topology Name:\*

Network Topology:  Point to Point  Hub and Spoke  Full Mesh

IKE Version:\*  IKEv1  IKEv2

Endpoints    IKE    IPsec    **Advanced**

IKE  
IPsec  
**Tunnel**

**NAT Settings**

Keepalive Messages Traversal  
Interval:  Seconds (Range 10 - 3600)

**Access Control for VPN Traffic**

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)  
*Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.*

**Certificate Map Settings**

Use the certificate map configured in the Endpoints to determine the tunnel

Use the certificate OU field to determine the tunnel

Use the IKE identity to determine the tunnel

Use the peer IP address to determine the tunnel

Se **sysopt allow-vpn** non è abilitato, è necessario creare una policy di controllo dell'accesso per consentire il traffico VPN attraverso il dispositivo FTD. Se l'opzione **sysopt allow-vpn** è abilitata, ignorare la creazione di criteri di controllo di accesso.

### Passaggio 5. Creare un criterio di controllo dell'accesso.

In Criteri di controllo d'accesso, passare a **Criteri > Controllo d'accesso > Controllo d'accesso** e selezionare il criterio che interessa il dispositivo FTD. Per aggiungere una regola, fare clic su **Aggiungi regola**, come mostrato nell'immagine.

Deve essere consentito il traffico dalla rete interna verso l'esterno e dalla rete esterna verso la rete interna. Creare una regola per eseguire entrambe le operazioni o creare due regole per mantenerle separate. In questo esempio viene creata una regola per entrambe le operazioni.

## Editing Rule - VPN\_Traffic

Name: VPN\_Traffic  Enabled [Move](#)

Action:  Allow

Zones: **Networks** | VLAN Tags | Users | Applications | Ports | URLs | SGT/ISE Attributes | Inspection | Logging | Comments

Available Networks:

Source Networks (2):

Source	Original Client
ASASubnet	
FTDSubnet	

Destination Networks (2):

ASASubnet
FTDSubnet

Buttons: Add To Source Networks, Add to Destination, Save, Cancel

Rules | Security Intelligence | HTTP Responses | Logging | Advanced

Filter by Device | Show Rule Conflicts | Add Category | Add Rule | Search Rules

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VL...	Us...	Ap...	So...	De...	URLs	So...	De...	A...
1 VPN_Traffic	Inside Outside	Inside Outside	ASASubnet FTDSubnet	ASASubnet FTDSubnet	Any	Any	Any	Any	Any	Any	Any	Any	Allow

Default Action: Access Control: Block All Traffic

## Passaggio 6. Configurare l'esenzione NAT.

Configurare un'istruzione di esenzione NAT per il traffico VPN. L'esenzione NAT deve essere in atto per evitare che il traffico VPN colpisca un'altra istruzione NAT e traduca in modo errato il traffico VPN.

1. Passare a **Dispositivi > NAT**, selezionare il criterio NAT che ha come destinazione l'FTD. Creare una nuova regola facendo clic sul pulsante **Aggiungi regola**.

Overview | Analysis | Policies | **Devices** | Objects | AMP | Intelligence

Device Management | **NAT** | VPN | QoS | Platform Settings | FlexConfig | Certificates

VirtualFTDNAT

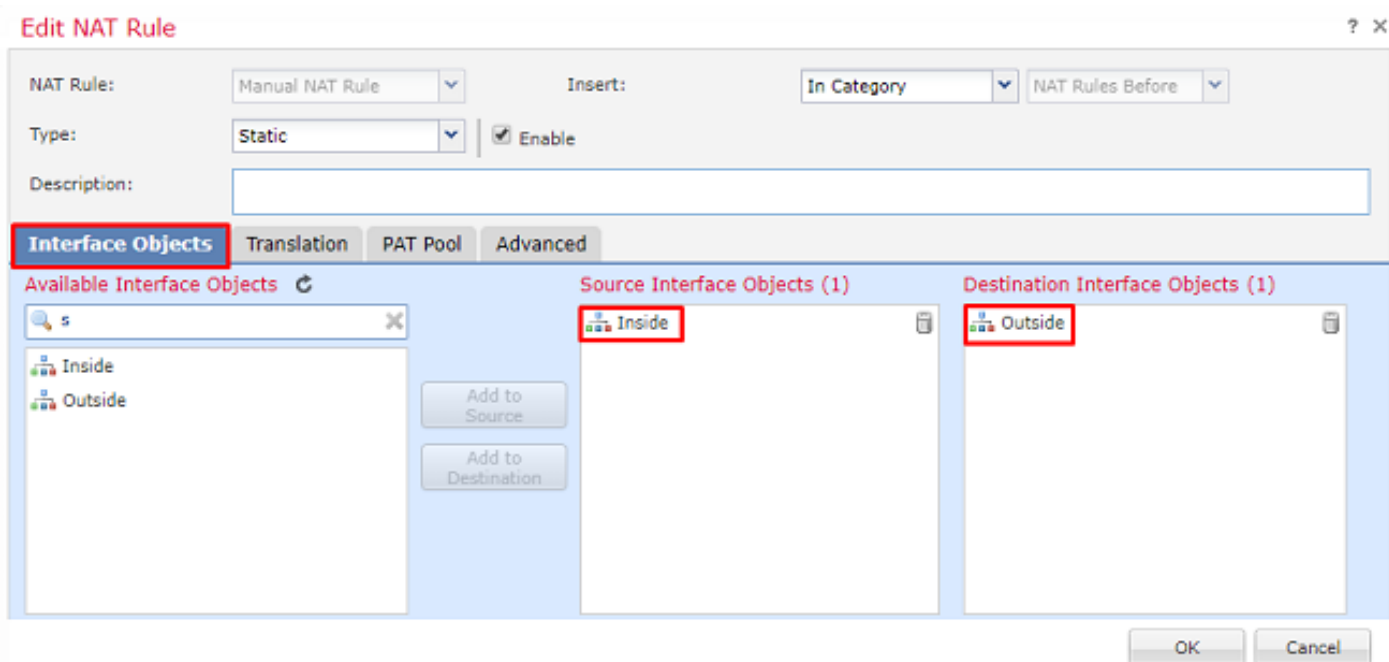
Enter Description

Policy Assignments (1)

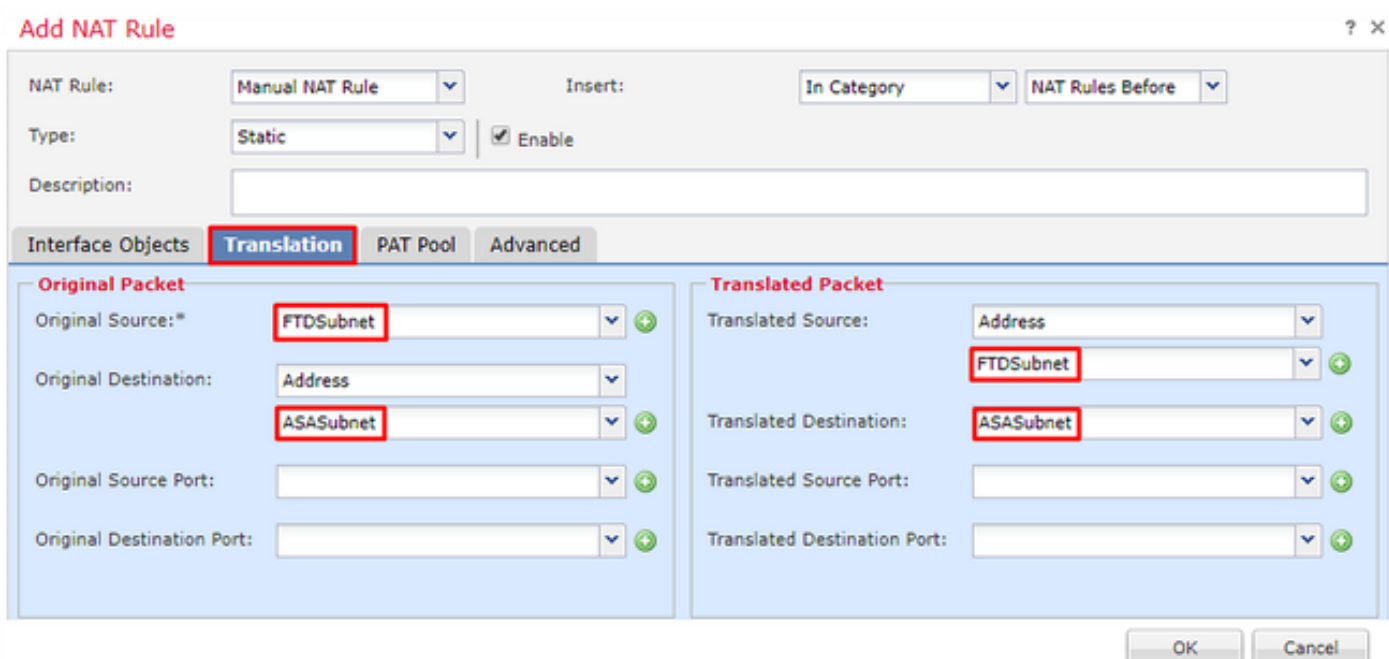
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
NAT Rules Before											
Auto NAT Rules											

Buttons: Show Warnings, Save, Cancel, Add Rule

2. Creare una nuova regola NAT manuale statica. Fare riferimento alle interfacce interne ed esterne.



3. Sotto la scheda **Traduzione** e selezionare le subnet di origine e di destinazione. Poiché si tratta di una regola di esenzione NAT, rendere uguali l'origine/destinazione originale e l'origine/destinazione tradotta, come mostrato nella seguente immagine:



4. Infine, passare alla scheda **Avanzate** e abilitare la funzione no-proxy-arp e route-lookup.

**Add NAT Rule** ? X

NAT Rule:  Insert:

Type:   Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Fallthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

5. Salva questa regola e guarda i risultati finali nell'elenco NAT.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates

**VirtualFTDNAT** Show Warnings Save Cancel

Enter Description Policy Assignments

**Rules** Filter by Device Add Rule

#	Direction	Type	Source Interface...	Destination Interface...	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
<b>NAT Rules Before</b>											
1	↔	Static	Inside	Outside	FTDSubnet	ASASubnet		FTDSubnet	ASASubnet		Dns:fal route-k no-pro
<b>Auto NAT Rules</b>											
#	↔	Dynamic	Inside	Outside	any-obj			Interface			Dns:fal
<b>NAT Rules After</b>											

6. Al termine della configurazione, salvare e distribuire la configurazione nell'FTD.

## Passaggio 7. Configurare l'ASA.

1. Abilitare IKEv2 sull'interfaccia esterna dell'appliance ASA:

```
Crypto ikev2 enable outside
```

2. Creare il criterio IKEv2 che definisce gli stessi parametri configurati nell'FTD:

```
Crypto ikev2 policy 1
Encryption aes-256
Integrity sha256
Group 14
Prf sha256
Lifetime seconds 86400
```

3. Creare un criterio di gruppo che consenta il protocollo ikev2:

```
Group-policy FTD_GP internal
Group-policy FTD_GP attributes
Vpn-tunnel-protocol ikev2
```

4. Creare un gruppo di tunnel per l'indirizzo IP pubblico FTD peer. Fare riferimento ai criteri di gruppo e specificare la chiave già condivisa:

```
Tunnel-group 172.16.100.20 type ipsec-l2l
Tunnel-group 172.16.100.20 general-attributes
Default-group-policy FTD_GP
Tunnel-group 172.16.100.20 ipsec-attributes
ikev2 local-authentication pre-shared-key cisco123
ikev2 remote-authentication pre-shared-key cisco123
```

5. Creare un elenco degli accessi che definisca il traffico da crittografare: (FTDSubnet 10.10.113.0/24) (ASASubnet 10.10.110.0/24)

```
Object network FTDSUBNET
Subnet 10.10.113.0 255.255.255.0
Object network ASASUBNET
Subnet 10.10.110.0 255.255.255.0
Access-list ASAToFTD extended permit ip object ASASUBNET object FTDSUBNET
```

6. Creare una proposta ipsec ikev2 che faccia riferimento agli algoritmi specificati nell'FTD:

```
Crypto ipsec ikev2 ipsec-proposal FTD
Protocol esp encryption aes-gcm-256
```

7. Creare una voce della mappa crittografica che colleghi la configurazione:

```
Crypto map outside_map 10 set peer 172.16.100.20
Crypto map outside_map 10 match address ASAToFTD
Crypto map outside_map 10 set ikev2 ipsec-proposal FTD
Crypto map outside_map 10 interface outside
```

8. Creare una dichiarazione di esenzione NAT che impedisca al traffico VPN di essere NATTED dal firewall:

```
Nat (inside,outside) 1 source static ASASUBNET ASASUBNET destination static FTDSUBNET FTDSUBNET
no-proxy-arp route-lookup
```

## Verifica

**Nota:** Al momento non è possibile verificare lo stato del tunnel VPN dal FMC. È necessario apportare un miglioramento a questa funzionalità [CSCvh7603](#).

Tentativo di avviare il traffico attraverso il tunnel VPN. Per accedere alla riga di comando dell'ASA o dell'FTD, usare il comando packet tracer. Quando si usa il comando packet-tracer per attivare il tunnel VPN, deve essere eseguito due volte per verificare che il tunnel venga attivato. La prima volta che il comando viene emesso, il tunnel VPN è inattivo, quindi il comando packet-tracer non riuscirà con VPN encrypt DROP. Non utilizzare l'indirizzo IP interno del firewall come indirizzo IP di origine nel packet-tracer, in quanto si verificheranno sempre errori.

```
firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10
```

```
Phase: 10
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:
```

```
firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10
```

```
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.100.1 using egress ifc outside
```

```
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet
no-proxy-arp route-lookup
Additional Information:
NAT divert to egress interface outside
Untranslate 10.10.110.10/0 to 10.10.110.10/0
```

```
Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip ifc Inside object-group FMC_INLINE_src_rule_268436483
ifc outside object-group FMC_INLINE_dst_rule_268436483 rule-id 268436483
access-list CSM_FW_ACL_ remark rule-id 268436483: ACCESS POLICY: FTD-Access-Control-Policy -
Mandatory
access-list CSM_FW_ACL_ remark rule-id 268436483: L7 RULE: VPN_Traffic
object-group network FMC_INLINE_src_rule_268436483
description: Auto Generated by FMC from src of UnifiedNGFWRule# 1 (FTD-Access-Control-
Policy/mandatory)
network-object object ASASubnet
network-object object FTDSubnet
object-group network FMC_INLINE_dst_rule_268436483
description: Auto Generated by FMC from dst of UnifiedNGFWRule# 1 (FTD-Access-Control-
Policy/mandatory)
network-object object ASASubnet
network-object object FTDSubnet
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached
```

```
Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet
no-proxy-arp route-lookup
Additional Information:
Static translate 10.10.113.10/0 to 10.10.113.10/0
```

Phase: 10  
Type: VPN  
Subtype: encrypt  
Result: ALLOW  
Config:  
Additional Information:

Result:  
input-interface: Inside  
input-status: up  
input-line-status: up  
output-interface: outside  
output-status: up  
output-line-status: up  
Action: allow

Per monitorare lo stato del tunnel, accedere alla CLI dell'FTD o dell'ASA.

Dalla CLI dell'FTD verificare la fase 1 e la fase 2 con questo comando:

## Mostra sa crypto ikev2

```
> show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local
Remote                               Status          Role
9528731 172.16.100.20/500
192.168.200.10/500                    READY          INITIATOR
    Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
    Life/Active Time: 86400/118 sec
Child sa: local selector 10.10.113.0/0 - 10.10.113.255/65535
         remote selector 10.10.110.0/0 - 10.10.110.255/65535
         ESP spi in/out: 0x66be357d/0xb74c8753
```

## Risoluzione dei problemi e debug

### Problemi iniziali di connettività

Quando si costruisce una VPN, ci sono due lati che negoziano il tunnel. Pertanto, è meglio ottenere entrambi i lati della conversazione quando si risolvono i problemi relativi a qualsiasi tipo di errore del tunnel. Una guida dettagliata su come eseguire il debug dei tunnel IKEv2 è disponibile qui: [Come eseguire il debug delle VPN IKEv2](#)

La causa più comune degli errori del tunnel è un problema di connettività. Il modo migliore per determinare questa condizione è acquisire i pacchetti sul dispositivo. Usare questo comando per acquisire i pacchetti sul dispositivo:

```
Capture capout interface outside match ip host 172.16.100.20 host 192.168.200.10
```

Una volta eseguita l'acquisizione, provare a inviare il traffico sulla VPN e verificare la presenza di traffico bidirezionale nell'acquisizione dei pacchetti.

Esaminare l'acquisizione dei pacchetti con questo comando:



## mostra capout

```
firepower# show cap capout
```

```
4 packets captured
```

```
1: 11:51:12.059628      172.16.100.20.500 > 192.168.200.10.500:  udp 690
2: 11:51:12.065243      192.168.200.10.500 > 172.16.100.20.500:  udp 619
3: 11:51:12.066692      172.16.100.20.500 > 192.168.200.10.500:  udp 288
4: 11:51:12.069835      192.168.200.10.500 > 172.16.100.20.500:  udp 240
```

## Problemi specifici del traffico

I problemi più comuni che si possono verificare sono:

- Problemi di routing dietro l'FTD — la rete interna non è in grado di indirizzare i pacchetti agli indirizzi IP e ai client VPN assegnati.
- Elenchi di controllo di accesso che bloccano il traffico.
- Non è possibile ignorare Network Address Translation per il traffico VPN.

Per ulteriori informazioni sulle VPN sull'FTD gestito da FMC, è possibile consultare la guida alla configurazione completa qui: [Guida alla configurazione di FTD gestito da FMC](#)