Configura VPN da sito a sito su FTD Gestito da FDM

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Configurazione](#)
[Definizione di reti protette](#)
[Configura VPN da sito a sito](#)
[Configurazione ASA](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Problemi iniziali di connettività](#)
[Problemi specifici del traffico](#)
[Informazioni correlate](#)

Introduzione

Questo documento descrive come configurare la VPN da sito a sito su Firepower Threat Defense (FTD) gestito da FirePower Device Manager (FDM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di VPN
- Esperienza con FDN
- Esperienza con la riga di comando di Adaptive Security Appliance (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.

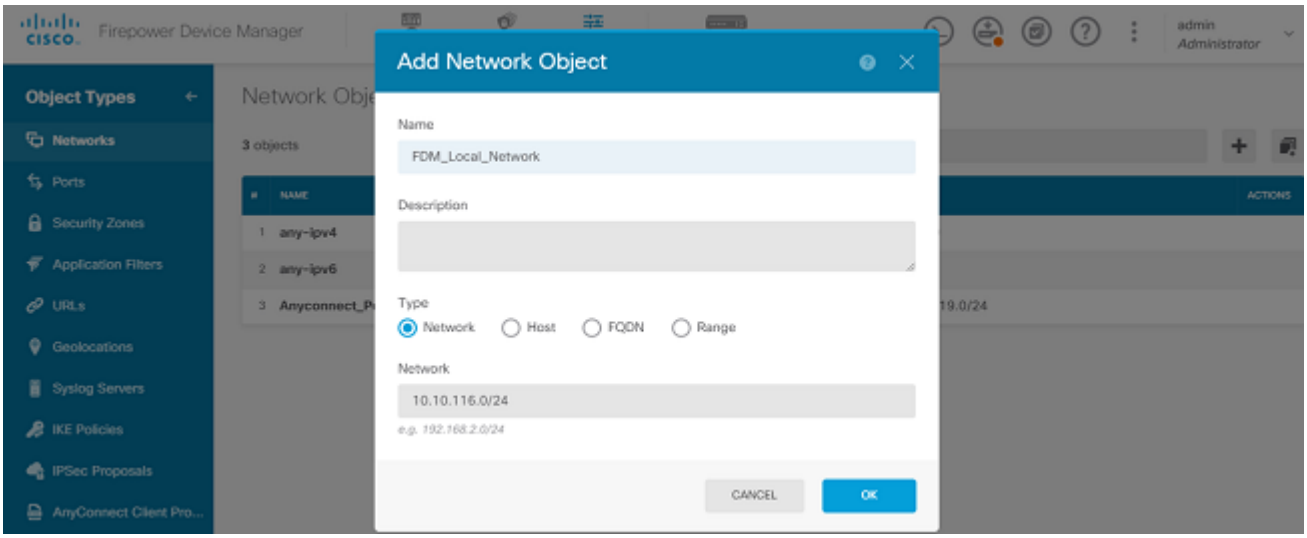
Configurazione

Iniziare con la configurazione su FTD con FDM.

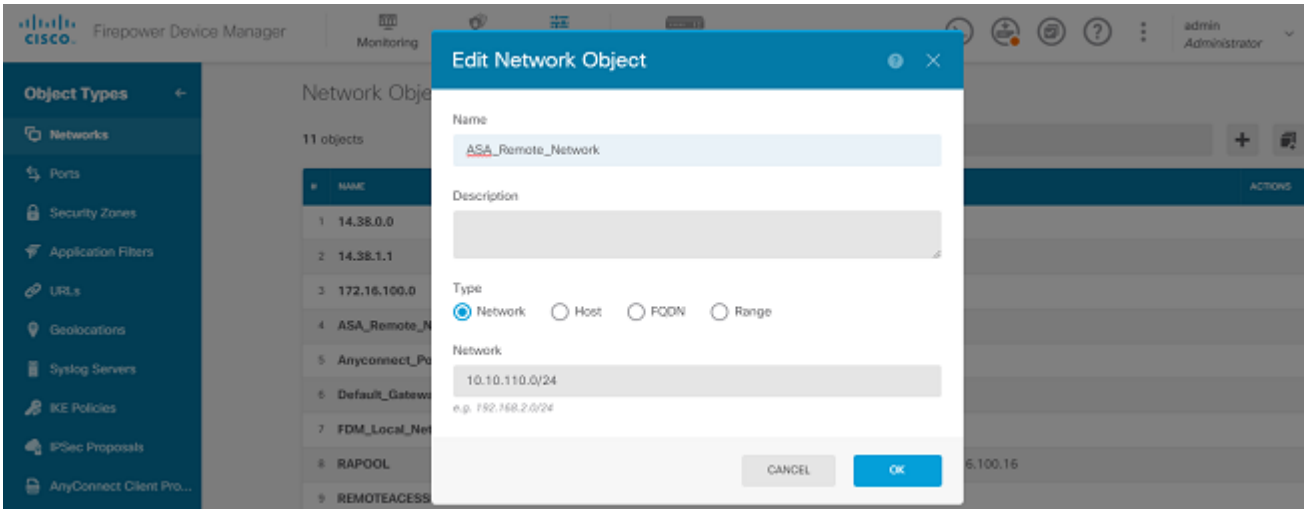
Definizione di reti protette

Selezionare **Oggetti > Reti > Aggiungi nuova rete**.

Configurare gli oggetti per le reti LAN dalla GUI di FDM. Creare un oggetto per la rete locale dietro il dispositivo FDM come mostrato nell'immagine.



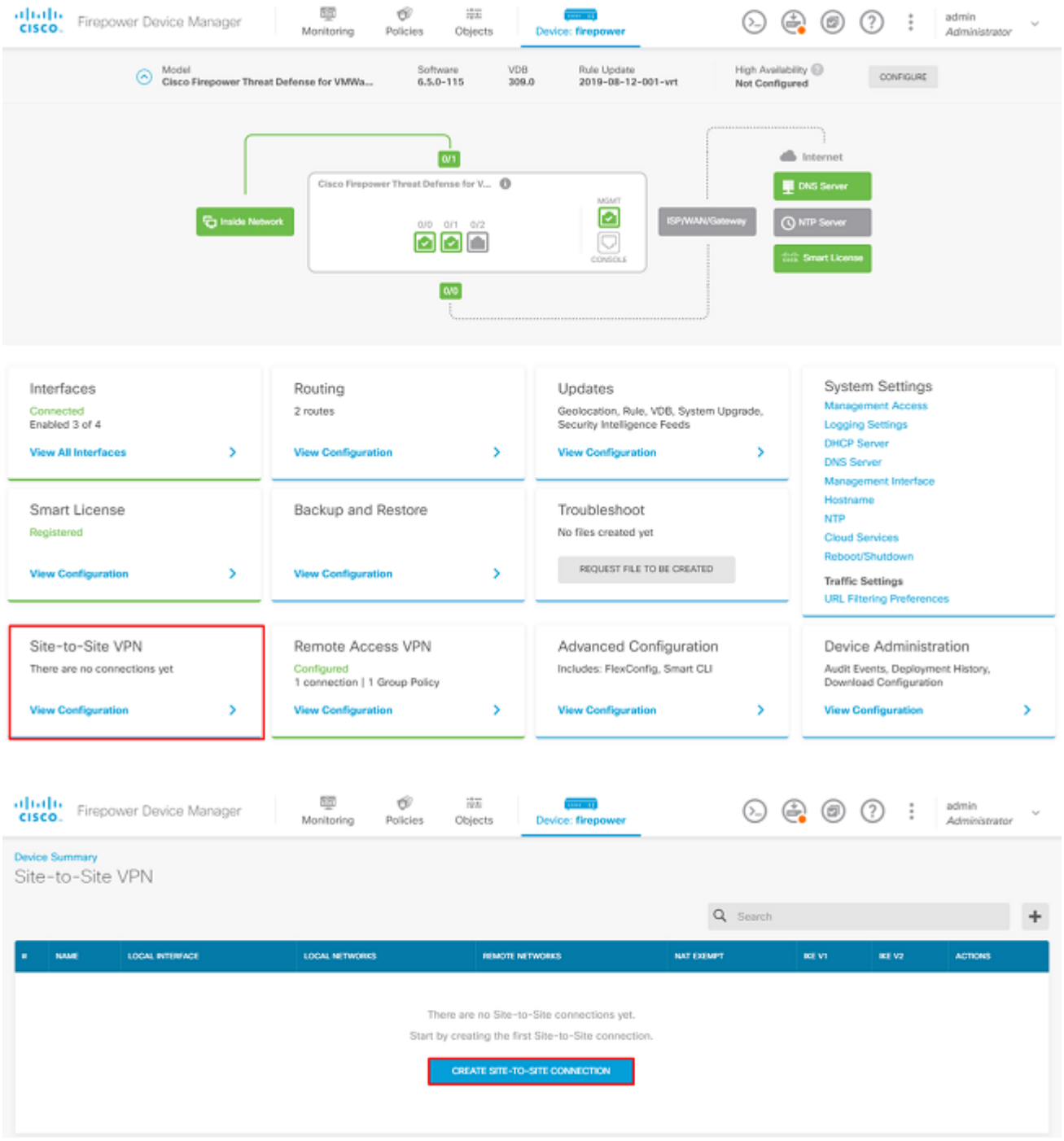
Creare un oggetto per la rete remota dietro la periferica ASA, come mostrato nell'immagine.



Configura VPN da sito a sito

Passare a **VPN da sito a sito > Crea connessione da sito a sito**.

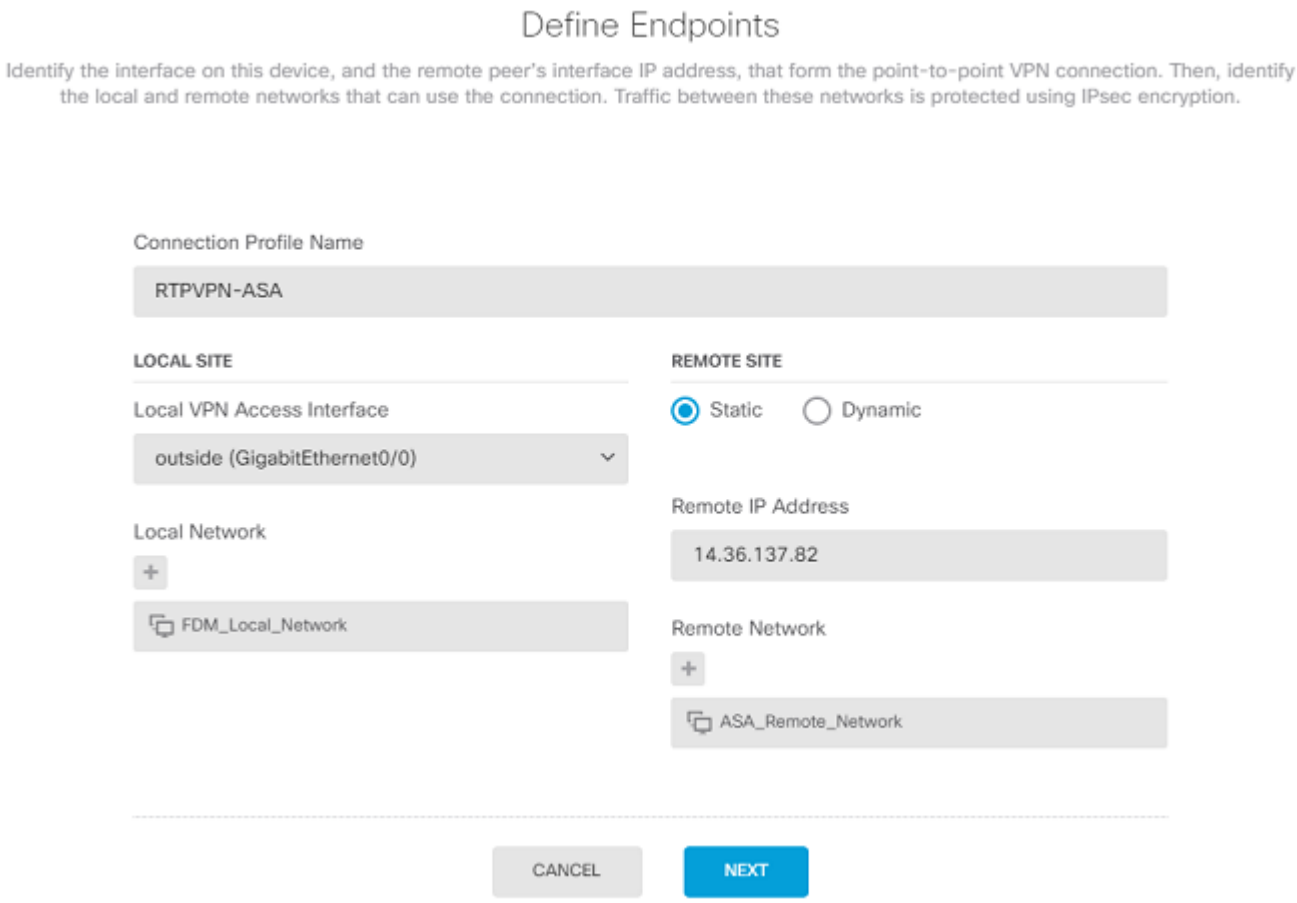
Eseguire la procedura guidata da sito a sito in FDM come illustrato nell'immagine.



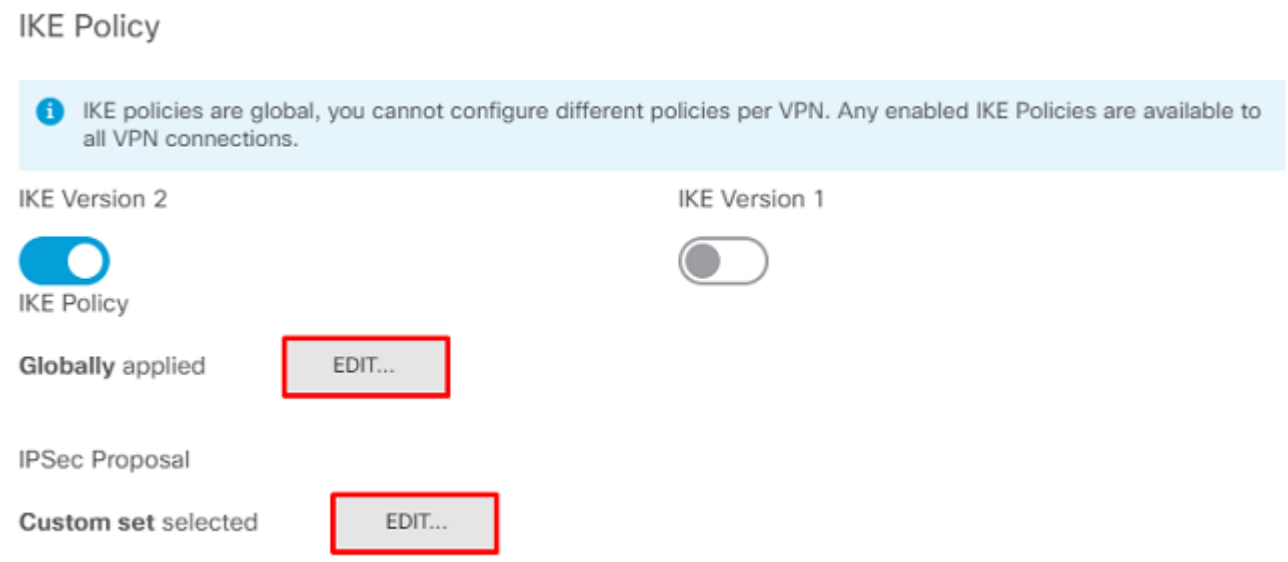
Assegnare alla connessione da sito a sito un nome di profilo di connessione facilmente identificabile.

Scegliere l'interfaccia esterna corretta per l'FTD, quindi scegliere la rete locale da crittografare sulla VPN da sito a sito.

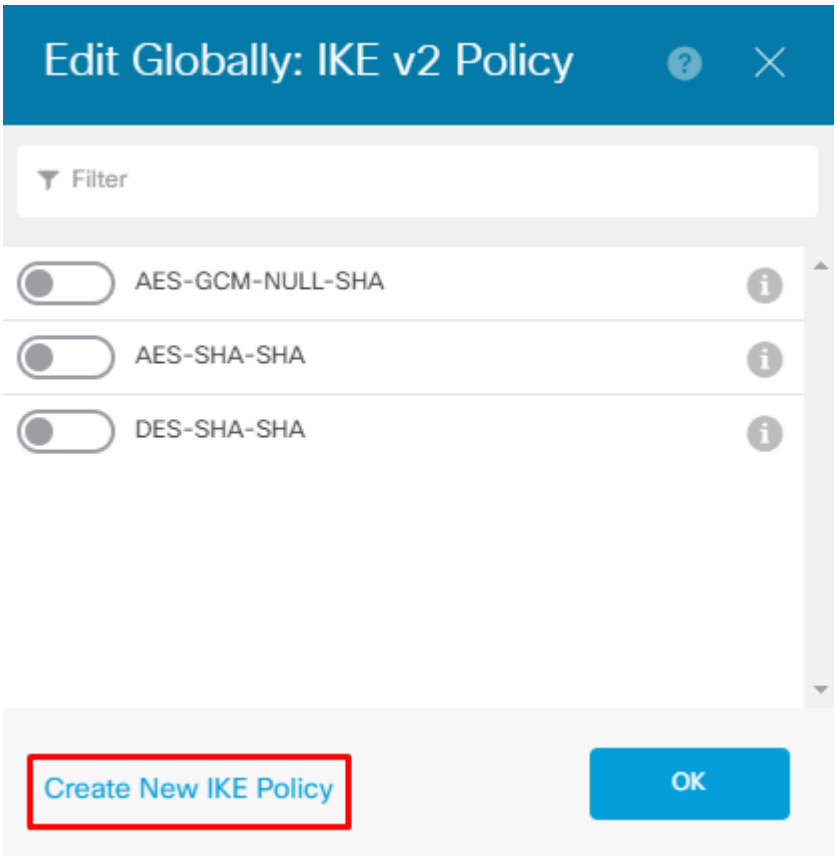
Impostare l'interfaccia pubblica del peer remoto. Quindi, scegliere la rete peer remota crittografata tramite la VPN da sito a sito, come mostrato nell'immagine.



Nella pagina successiva scegliere il pulsante **Modifica** per impostare i parametri IKE (Internet Key Exchange) come mostrato nell'immagine.

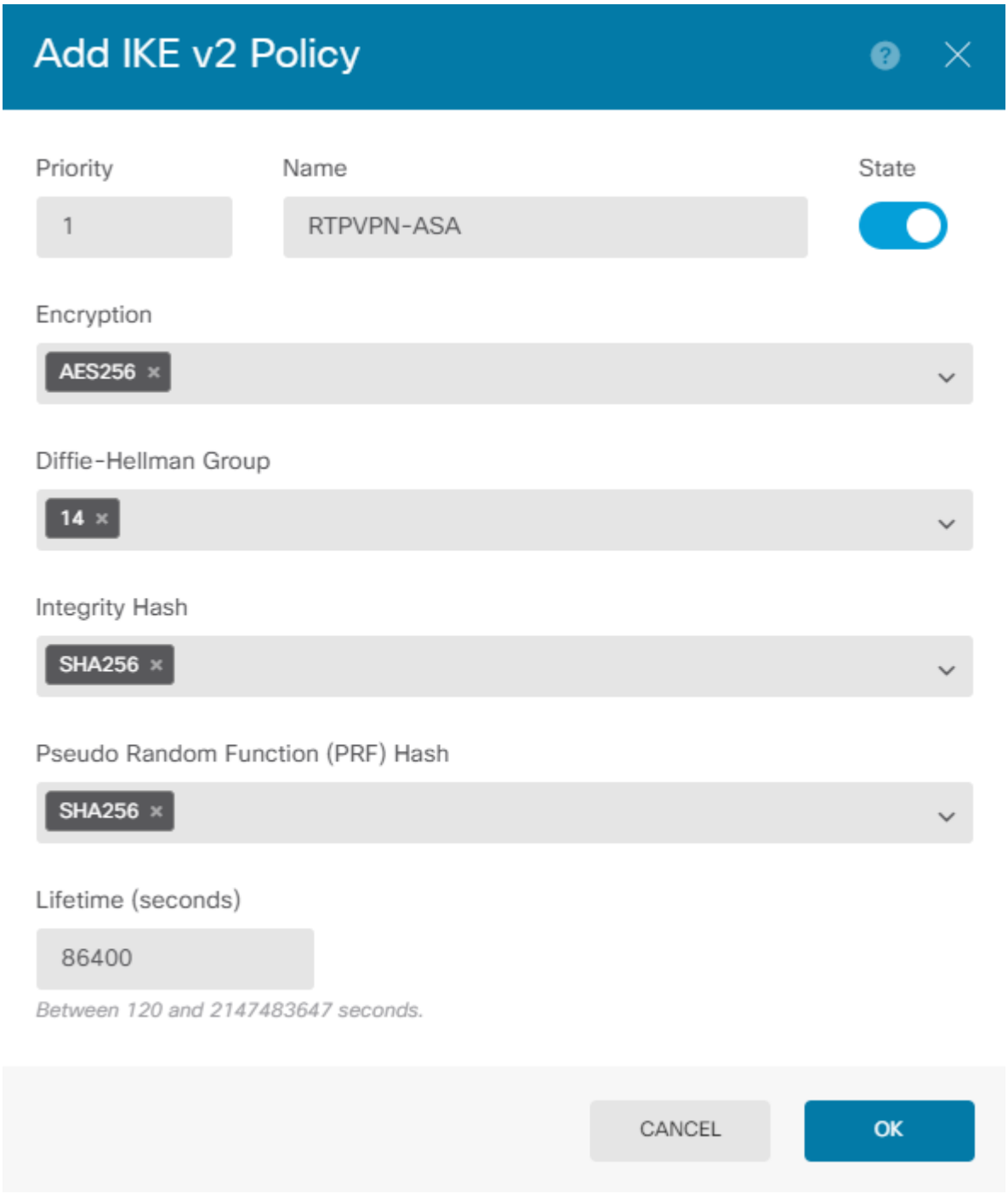


Scegliere il pulsante **Crea nuovo criterio IKE** come illustrato nell'immagine.

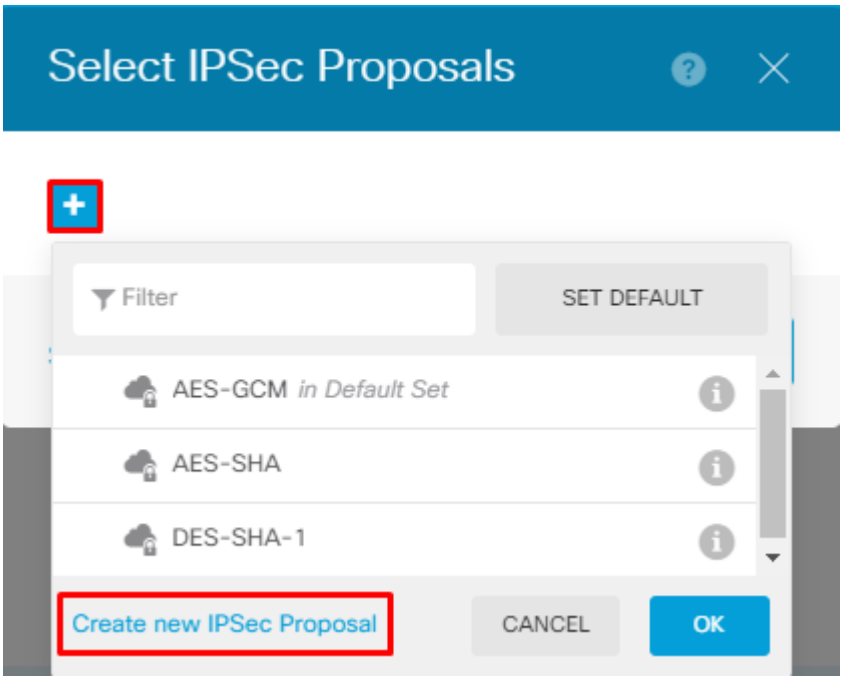


In questa guida vengono utilizzati i seguenti parametri per lo scambio iniziale di IKEv2:

Crittografia AES-256
Integrità SHA256
Gruppo DH 14
PRF SHA256



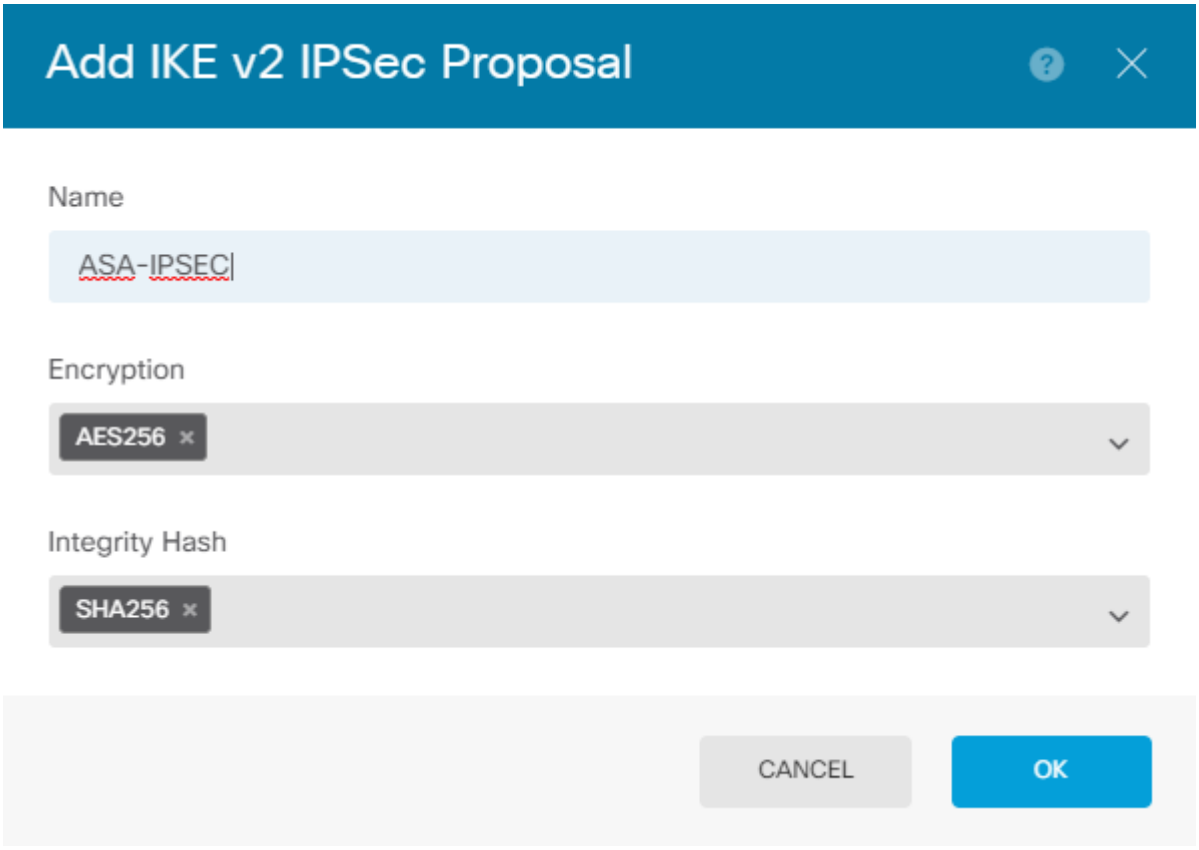
Nella pagina principale scegliere il pulsante **Modifica** per la proposta IPSec. Creare una nuova proposta IPSec come illustrato nell'immagine.



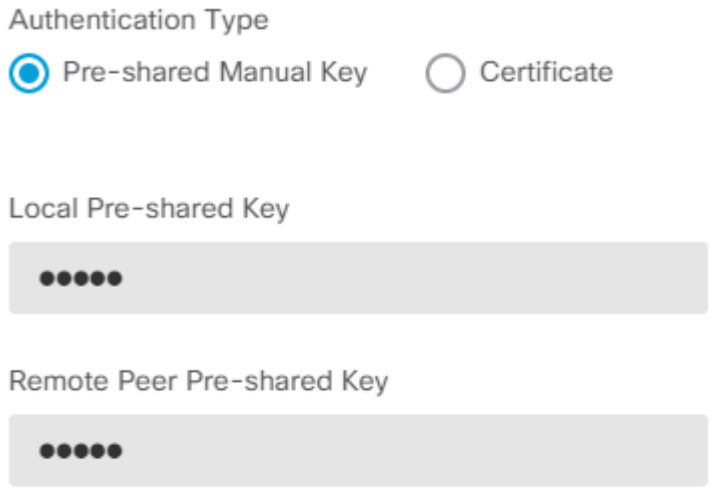
In questa guida vengono utilizzati i seguenti parametri per IPSec:

Crittografia AES-256

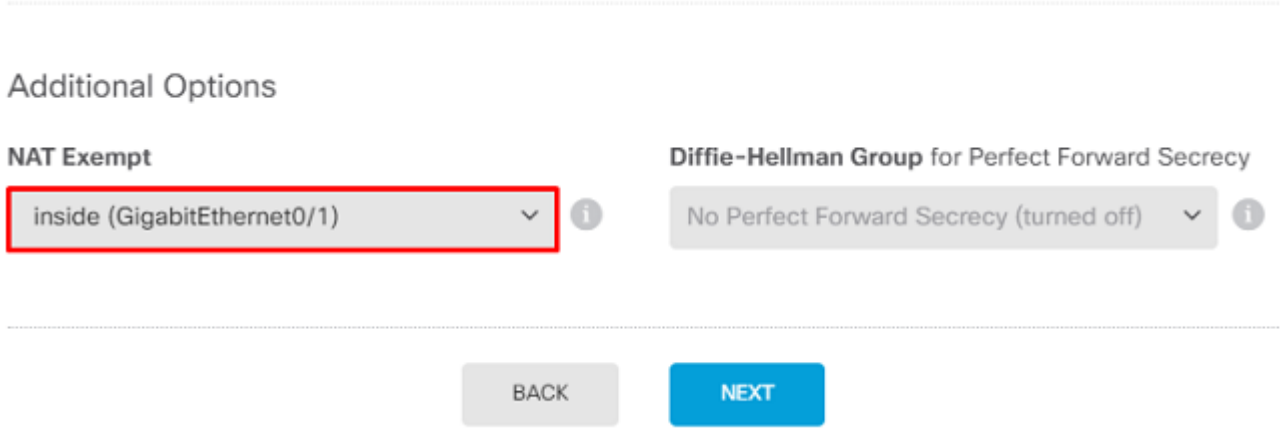
Integrità SHA256



Impostare l'autenticazione su una chiave già condivisa e immettere la chiave già condivisa (PSK) utilizzata su entrambe le estremità. In questa guida viene utilizzata la chiave PSK di Cisco come mostrato nell'immagine.



Impostare l'interfaccia NAT Exempt interna. Se vengono utilizzate più interfacce interne, è necessario creare una regola di esenzione NAT manuale in **Policy > NAT**.



Nella pagina finale viene visualizzato un riepilogo della connessione da sito a sito. Accertarsi di aver selezionato gli indirizzi IP corretti e di aver utilizzato i parametri di crittografia corretti, quindi fare clic sul pulsante Fine. Distribuire la nuova VPN da sito a sito.

La configurazione ASA viene completata con l'uso della CLI.

Configurazione 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 FDM_GP internal
Group-policy FDM_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 172.16.100.10 type ipsec-l2l
Tunnel-group 172.16.100.10 general-attributes
 Default-group-policy FDM_GP
Tunnel-group 172.16.100.10 ipsec-attributes
 ikev2 local-authentication pre-shared-key cisco
 ikev2 remote-authentication pre-shared-key cisco
```

5. Creare un elenco degli accessi che definisca il traffico da crittografare: (FTDSubnet 10.10.116.0/24) (ASASubnet 10.10.110.0/24):

```
Object network FDMSubnet
 Subnet 10.10.116.0 255.255.255.0
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 FDM
 Protocol esp encryption aes-256
```

```
Protocol esp integrity sha-256
```

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

```
Crypto map outside_map 20 set peer 172.16.100.10
Crypto map outside_map 20 match address ASAtoFTD
Crypto map outside_map 20 set ikev2 ipsec-proposal FTD
Crypto map outside_map 20 interface outside
```

8. Creare un'istruzione di esenzione NAT che impedisca al traffico VPN di essere NATTED dal firewall:

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

Verifica

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

Tentativo di avviare il traffico attraverso il tunnel VPN. Per accedere alla riga di comando dell'ASA o dell'FTD, è possibile usare il comando packet tracer. Quando si usa il comando packet-tracer per richiamare il tunnel VPN, occorre eseguirlo due volte per verificare se il tunnel viene attivato. La prima volta che il comando viene emesso, il tunnel VPN è inattivo, quindi il comando packet-tracer ha esito negativo con VPN encrypt DROP. Non utilizzare l'indirizzo IP interno del firewall come indirizzo IP di origine nel packet-tracer, in quanto questa operazione ha sempre esito negativo.

```
firepower# packet-tracer input inside icmp 10.10.116.10 8 0 10.10.110.10

Phase: 9
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:


firepower# packet-tracer input inside icmp 10.10.116.10 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 |s2sAclSrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 |s2sAclSrcNwgV4|
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 NGFW_ONBOX_ACL global
access-list NGFW_ONBOX_ACL advanced trust object-group |acSvcg-268435457 ifc inside any ifc outside any
access-list NGFW_ONBOX_ACL remark rule-id 268435457: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule
object-group service |acSvcg-268435457
service-object ip
Additional Information:

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static |s2sAclSrcNwgV4|c9911223-779d-11ea-9c1b-5ddd47126971 |s2sAclSrcNwgV4|
Additional Information:
Static translate 10.10.116.10/0 to 10.10.116.10/0

Phase: 9
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, passare alla CLI dell'FTD o dell'ASA.

Dalla CLI dell'FTD, verificare le fasi 1 e 2 con il comando **show crypto ikev2 sa**.

```
> show crypto ikev2 sa

IKEv2 SAs:

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

Tunnel-id Local                                         Remote
```

```
  3821043 172.16.100.10/500                                   192.168.200.10/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/1150 sec
Child sa: local selector  10.10.116.0/0 - 10.10.116.255/65535
          remote selector 10.10.110.0/0 - 10.10.110.255/65535
          ESP spi in/out: 0x7398dcbd/0x2303b0c0
```

Risoluzione dei problemi

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

Problemi iniziali di connettività

Quando si costruisce una VPN, ci sono due lati che negoziano il tunnel. Pertanto, è consigliabile ottenere entrambi i lati della conversazione quando si risolvono i problemi relativi a qualsiasi tipo di errore del tunnel. Per una guida dettagliata su come eseguire il debug dei tunnel IKEv2, fare riferimento a:

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

Utilizzare questo comando per acquisire pacchetti sul dispositivo:

```
Capture capout interface outside match ip host 172.16.100.10 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 del pacchetto con il comando **show cap capout**.

```
firepower# show cap capout

4 packets captured

   1: 01:21:06.763983       172.16.100.10.500 > 192.168.200.10.500:  udp 574
   2: 01:21:06.769415       192.168.200.10.500 > 172.16.100.10.500:  udp 619
   3: 01:21:06.770666       172.16.100.10.500 > 192.168.200.10.500:  udp 288
   4: 01:21:06.773748       192.168.200.10.500 > 172.16.100.10.500:  udp 256
```

Problemi specifici del traffico

Di seguito sono riportati i problemi più comuni che gli utenti riscontrano nel traffico:

- 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.
- Access Control List che blocca il traffico.
- NAT (Network Address Translation) non ignorato per il traffico VPN.

Informazioni correlate

Per ulteriori informazioni sulle VPN da sito a sito sull'FTD gestito da FDM, è possibile trovare la guida alla configurazione completa qui.

- Guida alla configurazione di FTD gestito da FDM.

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).