

Configurazione di una doppia VPN da sito a sito basata su route attiva con PBR su FTD Gestito da FDM

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni su VPN](#)

[Configurazione VPN FTD sito1](#)

[Configurazione VPN FTD sito 2](#)

[Configurazioni su PBR](#)

[Configurazione PBR FTD sito1](#)

[Configurazione PBR FTD sito 2](#)

[Configurazioni su SLA Monitor](#)

[Configurazione monitoraggio SLA FTD del sito 1](#)

[Configurazione monitoraggio SLA FTD del sito 2](#)

[Configurazioni su route statica](#)

[Configurazione route statica FTD sito1](#)

[Configurazione route statica FTD sito 2](#)

[Verifica](#)

[Sia ISP1 che ISP2 funzionano correttamente](#)

[VPN](#)

[Percorso](#)

[Monitor SLA](#)

[Test Ping](#)

[L'ISP1 subisce un'interruzione mentre l'ISP2 funziona correttamente](#)

[VPN](#)

[Percorso](#)

[Monitor SLA](#)

[Test Ping](#)

[L'ISP2 subisce un'interruzione mentre l'ISP1 funziona correttamente](#)

[VPN](#)

[Percorso](#)

[Monitor SLA](#)

[Test Ping](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive come configurare la VPN da sito a sito basata su routing doppio attivo con PBR su FTD gestito da FDM.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di VPN
- Conoscenze base di Policy Based Routing (PBR)
- Conoscenze base del protocollo IP SLA (Service Level Agreement)
- Esperienza con FDM

Componenti usati

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

- Cisco FTDv versione 7.4.2
- Cisco FDM versione 7.4.2

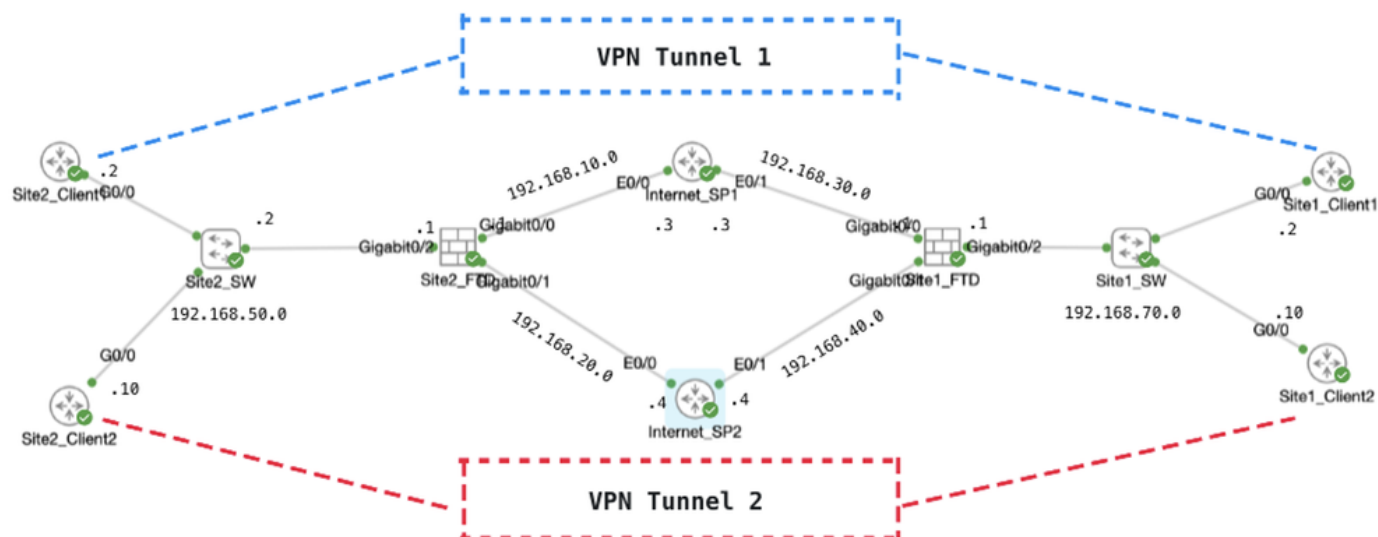
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Premesse

Questo documento spiega come configurare una VPN da sito a sito con doppia route attiva su FTD. In questo esempio, i FTD sia sul Sito1 che sul Sito2 hanno due connessioni ISP attive che stabiliscono la VPN da sito a sito con entrambi gli ISP contemporaneamente. Per impostazione predefinita, il traffico VPN attraversa il tunnel 1 su ISP1 (linea blu). Per host specifici, il traffico attraversa il tunnel 2 su ISP2 (linea rossa). In caso di interruzione, il traffico passa all'ISP2 come backup. Al contrario, se l'ISP2 subisce un'interruzione, il traffico passa all'ISP1 come backup. Per soddisfare questi requisiti, nell'esempio vengono utilizzati il Policy-Based Routing (PBR) e l'Internet Protocol Service Level Agreement (IP SLA).

Configurazione

Esempio di rete



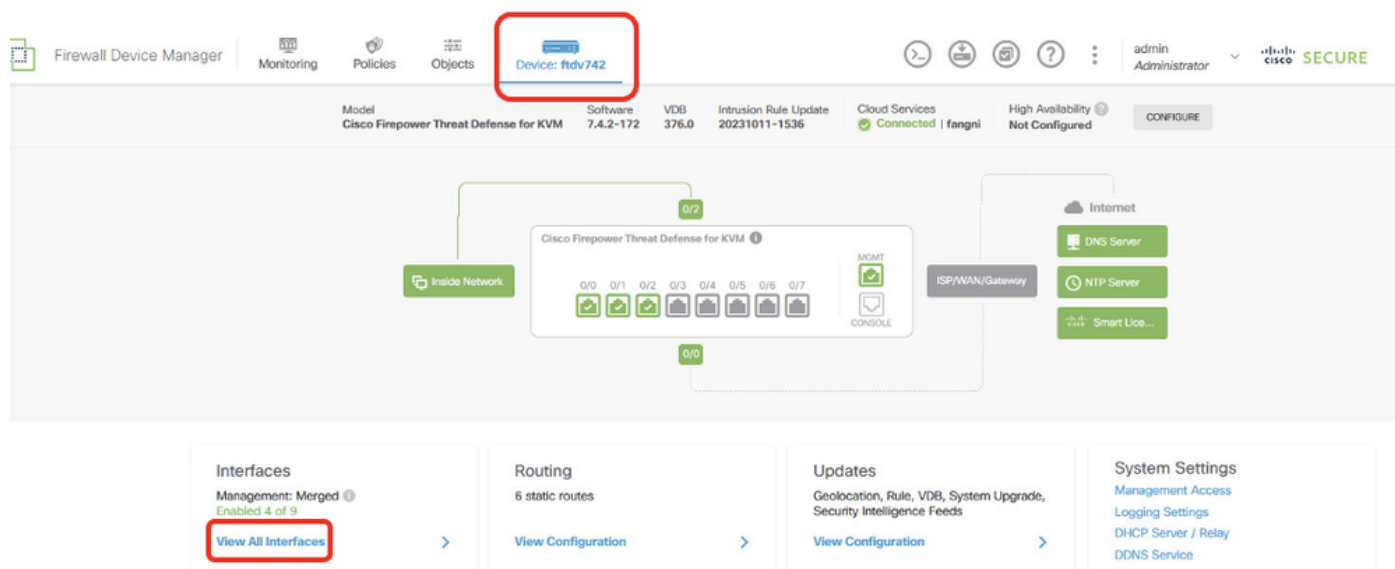
Topologia

Configurazioni su VPN

È essenziale garantire che la configurazione preliminare dell'interconnettività IP tra i nodi sia stata debitamente completata. I client sia in Site1 che in Site2 utilizzano FTD all'interno dell'indirizzo IP come gateway.

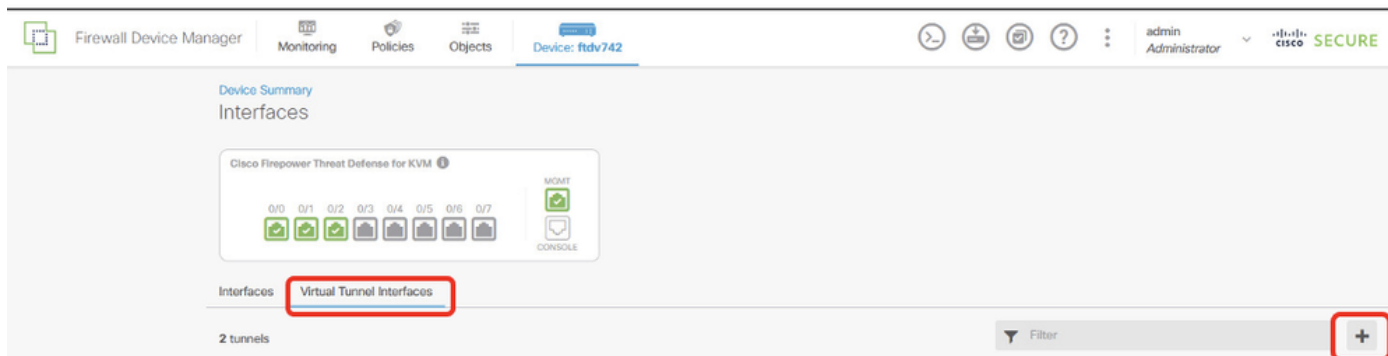
Configurazione VPN FTD sito1

Passaggio 1. Creare interfacce tunnel virtuali per ISP1 e ISP2. Accedere alla GUI FDM del FTD del sito 1. Passare a Dispositivo > Interfacce. Fare clic su Visualizza tutte le interfacce.



Sito1FTD_View_All_Interfaces

Passaggio 2. Fare clic sulla scheda Interfacce tunnel virtuale e quindi sul pulsante +.



Sito1FTD_Create_VTI

Passaggio 3. Fornire le informazioni necessarie sui dettagli VTI. Fare clic sul pulsante OK.

- Nome: demovti
- ID tunnel: 1
- Origine tunnel: esterno (Gigabit Ethernet0/0)
- Indirizzo IP E Subnet Mask: 169.254.10.1/24
- Stato: fare clic sul dispositivo di scorrimento nella posizione Attivato

Name

demovti

Status

☒

Most features work with named interfaces only, although some require unnamed interfaces.

Description

Tunnel ID *i*

1

Tunnel Source *i*

outside (GigabitEthernet0/0)

0 - 10413

IP Address and Subnet Mask

169.254.10.1 / 24

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

CANCEL

OK

Sito1FTD_VTI_Details_Tunnel1_ISP1

- Nome: demovti_sp2
- ID tunnel: 2

- Origine tunnel: esterno2 (Gigabit Ethernet0/1)
- Indirizzo IP E Subnet Mask: 169.254.20.11/24
- Stato: fare clic sul dispositivo di scorrimento nella posizione Attivato

Name: demovti_sp2

Status: ☒

Description:

Tunnel ID: 2 (Range: 0 - 10413)

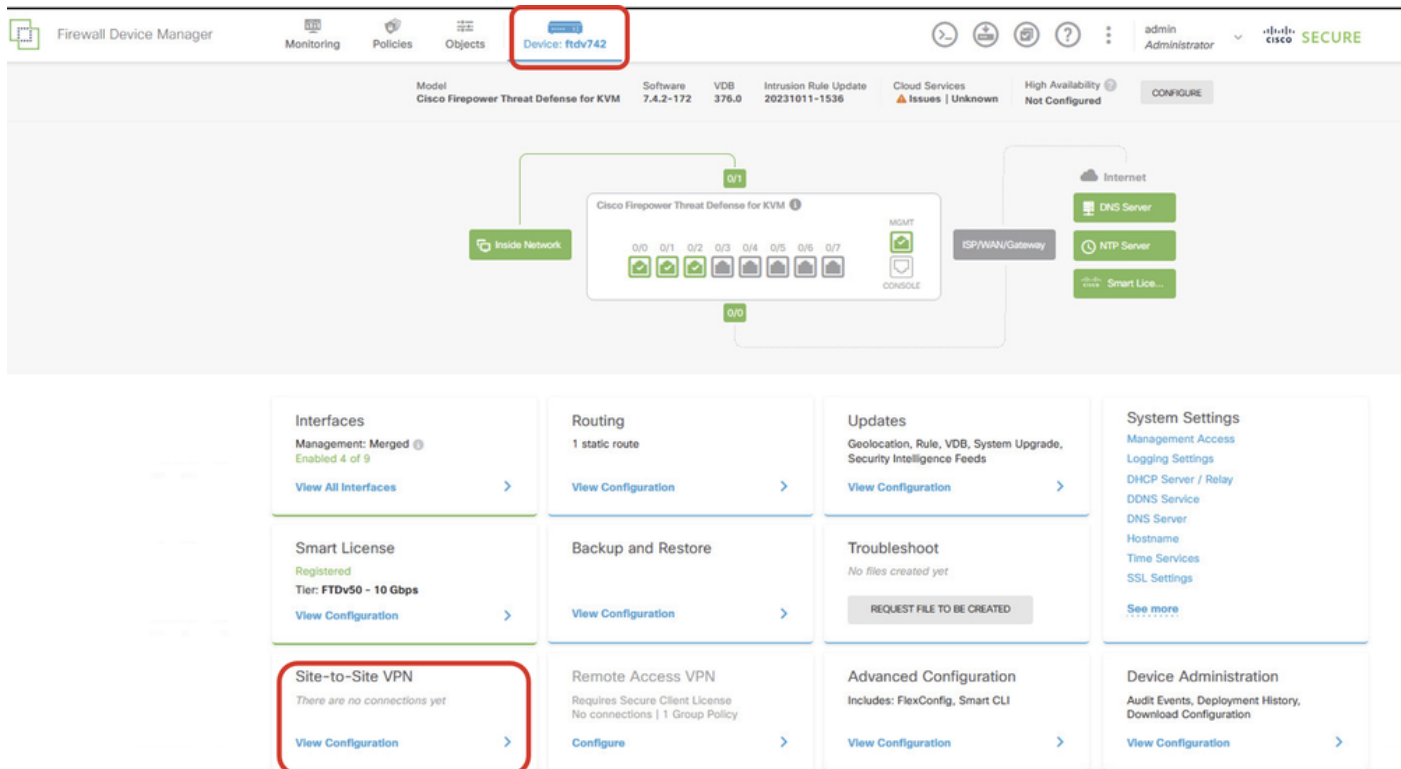
Tunnel Source: outside2 (GigabitEthernet0/1)

IP Address and Subnet Mask: 169.254.20.11 / 24 (Example: 192.168.5.15/17 or 192.168.5.15/255.255.128.0)

CANCEL OK

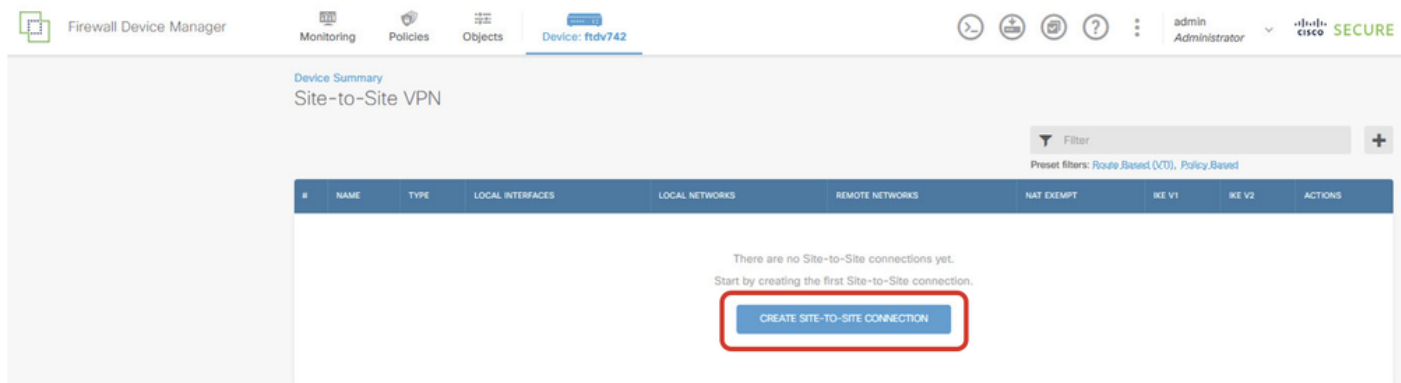
Sito1FTD_VTI_Details_Tunnel2_ISP2

Passaggio 4. Passare a Dispositivo > VPN da sito a sito. Fare clic sul pulsante Visualizza configurazione.



Sito1FTD_View_Site2Sito_VPN

Passaggio 5. Iniziare a creare una nuova VPN da sito a sito tramite ISP1. Fare clic sul pulsante CREA CONNESSIONE DA SITO A SITO o sul pulsante +.



Sito1FTD_Create_Site-to-Site_Connection

Passaggio 5.1. Fornire le informazioni necessarie sugli endpoint. Fare clic sul pulsante NEXT.

- Nome profilo connessione: Demo_S2S
- Tipo: VTI (Route Based)
- Interfaccia di accesso VPN locale: rimozione (creata nel passaggio 3)
- Indirizzo IP remoto: 192.168.10.1 (indirizzo IP Site2 FTD ISP1)

New Site-to-site VPN

1 Endpoints

2 Configuration

3 Summary



Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name: **Demo_S2S** Type: **Route Based (VTI)** Policy Based

Sites Configuration

LOCAL SITE	REMOTE SITE
Local VPN Access Interface: demovti (Tunnel1)	Remote IP Address: 192.168.10.1

CANCEL **NEXT**

Sito1FTD_ISP1_Site-to-Site_VPN_Define_Endpoints

Passaggio 5.2. Passare al criterio IKE. Fare clic sul pulsante MODIFICA.

Firewall Device Manager | Monitoring | Policies | Objects | **Device: ftdv742** | admin Administrator | CISCO SECURE

New Site-to-site VPN 1 Endpoints 2 **Configuration** 3 Summary

The diagram shows the VPN setup with the 'Configuration' step highlighted. It includes the 'Local Network', 'FTDV742' device, 'VPN TUNNEL', 'INTERNET', 'OUTSIDE 123.1.1.1' interface, 'PEER ENDPOINT', and 'Remote Network'.

Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

1 IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2 ☒

IKE VERSION 1 ☐

IKE Policy

Globally applied

EDIT...

IPSec Proposal

None selected

EDIT...

Sito1FTD_Edit_IKE_Policy

Passaggio 5.3. Per i criteri IKE, è possibile utilizzare criteri predefiniti oppure crearne uno nuovo facendo clic su Crea nuovo criterio IKE.

In questo esempio, attivare o disattivare un criterio IKE AES-SHA-SHA esistente e crearne uno nuovo a scopo dimostrativo. Per salvare, fare clic su OK.

- Nome: AES256_DH14_SHA256_SHA256
- Crittografia: AES, AES 256
- Gruppo DH: 14
- Hash di integrità: SHA256
- Hash PRF: SHA256
- Durata: 86400 (predefinito)

The image shows a two-pane configuration window for adding an IKE v2 Policy. The left pane lists available policies: AES-GCM-NULL-SHA, AES-SHA-SHA (selected), and DES-SHA-SHA. A red box highlights the 'Create New IKE Policy' button. The right pane, titled 'Add IKE v2 Policy', shows the configuration for the selected policy. Red boxes highlight the following fields: Priority (1), Name (AES256_DH14_SHA256_SHA256), State (toggle on), Encryption (AES, AES256), Diffie-Hellman Group (14), Integrity Hash (SHA, SHA256), Pseudo Random Function (PRF) Hash (SHA, SHA256), and Lifetime (86400 seconds). The 'OK' button is also highlighted.

Add IKE v2 Policy

Filter

☐ AES-GCM-NULL-SHA

☒ AES-SHA-SHA

☐ DES-SHA-SHA

Create New IKE Policy

OK

Priority: 1

Name: AES256_DH14_SHA256_SHA256

State: ☒

Encryption: AES x AES256

Diffie-Hellman Group: 14

Integrity Hash: SHA x SHA256

Pseudo Random Function (PRF) Hash: SHA x SHA256

Lifetime (seconds): 86400

Between 120 and 2147483647 seconds.

CANCEL

OK

Sito1FTD_Add_New_IKE_Policy

Filter

AES-GCM-NULL-SHA

i

AES-SHA-SHA

i

DES-SHA-SHA

i

AES256_DH14_SHA256_SHA256

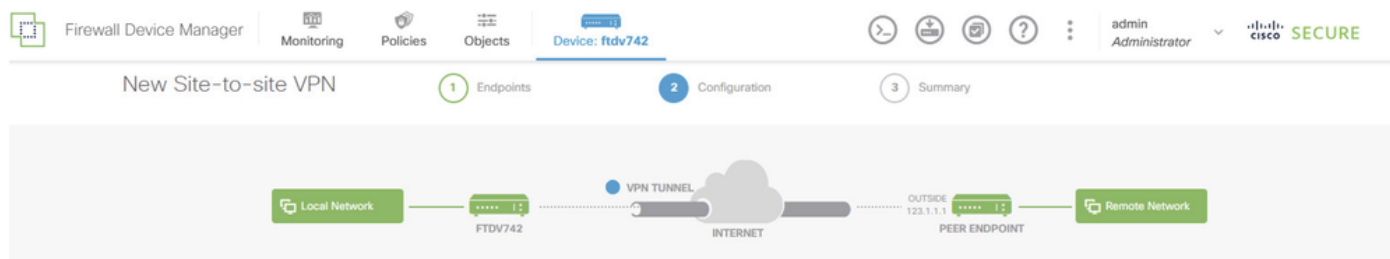
i

Create New IKE Policy

OK

Sito1FTD_Enable_New_IKE_Policy

Passaggio 5.4. Passare alla proposta IPSec. Fare clic sul pulsante MODIFICA.



Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

1 IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2 ☒

IKE VERSION 1 ☐

IKE Policy

Globally applied

EDIT...

IPSec Proposal

None selected

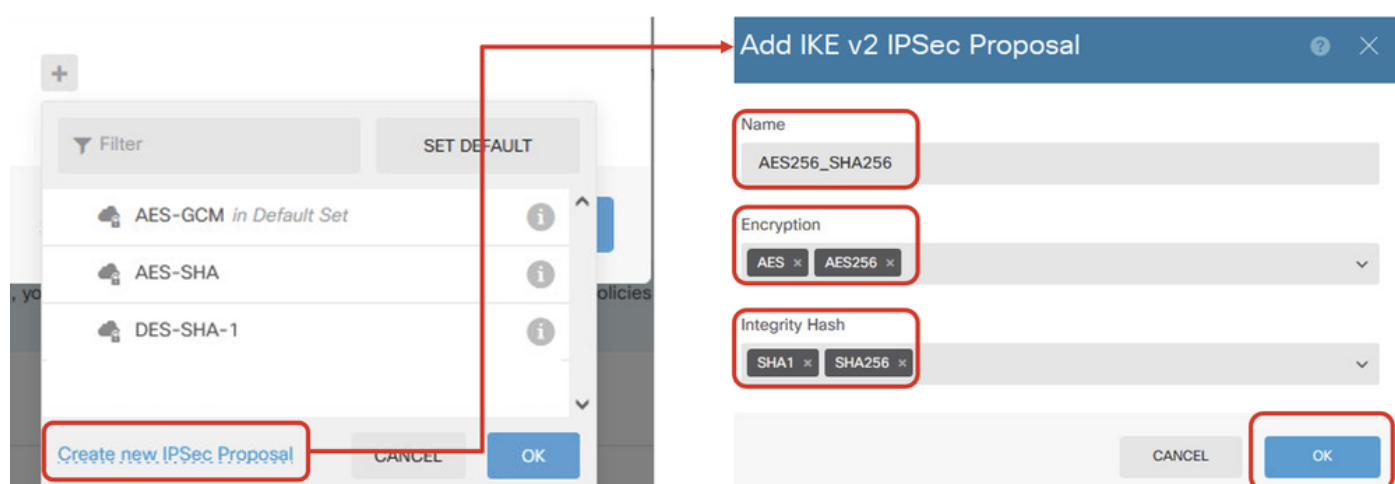
EDIT...



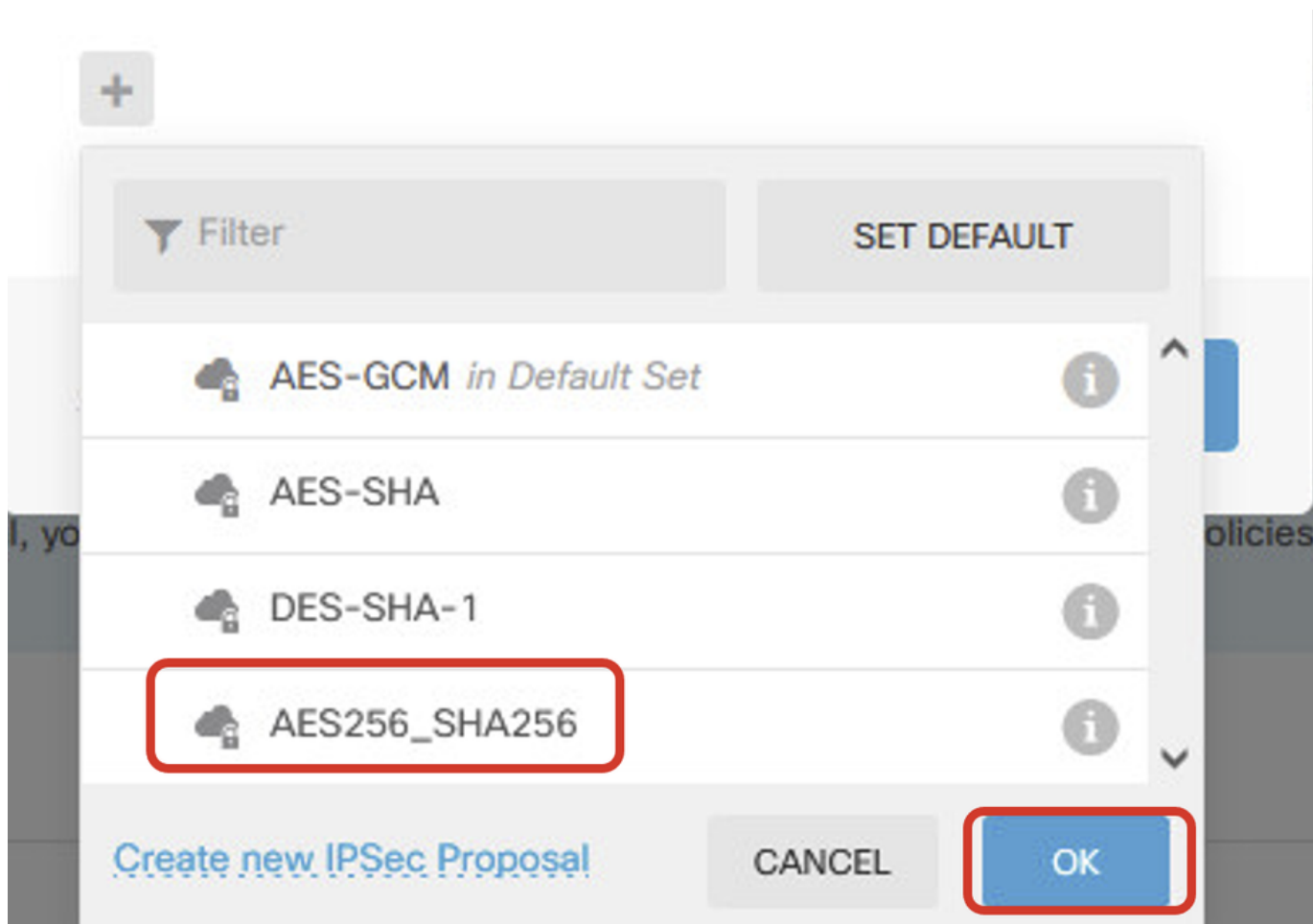
Sito1FTD_Edit_IKE_Proposta

Passaggio 5.5. Per una proposta IPsec, è possibile utilizzare una proposta predefinita oppure crearne una nuova facendo clic su Crea nuova proposta IPsec. In questo esempio, crearne uno nuovo a scopo dimostrativo. Per salvare, fare clic su OK.

- Nome: AES256_SHA256
- Crittografia: AES, AES 256
- Hash di integrità: SHA1, SHA256



Sito1FTD_Add_New_IKE_Proposta



Sito1FTD_Enable_New_IKE_Suggerimento

Passaggio 5.6. Scorrere la pagina e configurare la chiave già condivisa. Fare clic su Pulsante SUCCESSIVO.

Prendere nota di questa chiave già condivisa e configurarla in un FTD Site2 in un secondo momento.

Firewall Device Manager

MonitoringPoliciesObjectsDevice: ftdv742

FTDV742INTERNETPEER ENDPOINT

adminAdministrator

CISCOSECURITY

Privacy Configuration

Select the Internet Key Exchange (IKE) policy and enter the preshared keys needed to authenticate the VPN connection. Then, select the IPsec proposals to use for encrypting traffic.

IKE Policy

i IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2 ☒

IKE VERSION 1 ☐

IKE Policy

Globally applied [EDIT...](#)

IPSec Proposal

Custom set selected [EDIT...](#)

Authentication Type

☒ Pre-shared Manual Key ☐ Certificate

Local Pre-shared Key

Remote Peer Pre-shared Key

BACK

NEXT

Sito1FTD_Configure_Pre_Shared_Key

Passaggio 5.7. Esaminare la configurazione VPN. Se è necessario apportare modifiche, fare clic sul pulsante INDIETRO. Se tutto funziona, fare clic sul pulsante FINE.

Demo_S2S Connection Profile

i Peer endpoint needs to be configured according to specified below configuration.

VPN Access
Interface

 demovti (169.254.10.1)



Peer IP Address

192.168.10.1

IKE V2

IKE Policy aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14, aes,aes-256-sha,sha256-sha,sha256-14

IPSec Proposal aes,aes-256-sha-1,sha-256

Authentication Type Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration 28800 seconds

Lifetime Size 4608000 kilobytes

ADDITIONAL OPTIONS

Diffie-Hellman Null (not selected)

i Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

BACK

FINISH

Sito1FTD_ISP1_Review_VPN_Config_Summary

Passaggio 6. Ripetere il Passaggio 5. per creare una nuova VPN da sito a sito tramite ISP2.

Demo_S2S_SP2 Connection Profile

Peer endpoint needs to be configured according to specified below configuration.

VPN Access Interface

demovti_sp2 (169.254.20.11)

Peer IP Address

192.168.20.1

IKE V2

IKE Policy

aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14, aes,aes-256-sha,sha256-sha,sha256-14

IPSec Proposal

aes,aes-256-sha-1,sha-256

Authentication Type

Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration

28800 seconds

Lifetime Size

4608000 kilobytes

Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

Diffie-Hellman Group

Null (not selected)

BACK

FINISH

Sito1FTD_ISP2_Review_VPN_Config_Summary

Passaggio 7. Creare una regola di controllo dell'accesso per consentire il passaggio del traffico attraverso l'FTD. In questo esempio, consenti tutto per scopo dimostrativo. Modificare i criteri in base alle esigenze effettive.

Firewall Device Manager

Monitoring

Policies

Objects

Device: **ftdv742**

admin Administrator

Security Policies

→
 SSL Decryption →
 Identity →
 Security Intelligence →
 NAT →
 Access Control →
 Intrusion

1 rule

Filter

#	NAME	ACTION	SOURCE			DESTINATION			APPLICATIONS	URLS	USERS		ACTIONS
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS					
> 1	Demo_allow	Allow	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY		

Default Action

Access Control
 Block

Sito1FTD_Allow_Access_Control_Rule_Esempio

Passaggio 8. (Facoltativo) Configurare la regola di esenzione NAT per il traffico client su FTD se è

presente una NAT dinamica configurata per il client per accedere a Internet.

Per scopi dimostrativi, in questo esempio il NAT dinamico è configurato per i client al fine di accedere a Internet. È necessaria pertanto una regola di esenzione NAT.

Selezionare Policies > NAT. Fare clic sul pulsante +. Specificare i dettagli e fare clic su OK.

- Titolo: Esente da NAT
- Posizione: Prima delle regole NAT automatiche
- Tipo: Statico
- Interfaccia di origine: Interno
- Destinazione: Qualsiasi
- Indirizzo di origine originale: 192.168.70.0/24
- Indirizzo origine tradotto: 192.168.70.0/24
- Indirizzo di destinazione originale: 192.168.50.0/24
- Indirizzo di destinazione tradotto: 192.168.50.0/24
- Con Ricerca route abilitata

The screenshot shows the 'Add NAT Rule' dialog box in the Cisco Secure Firewall Device Manager. The dialog is for creating a 'NAT Exempt' rule. Key fields highlighted with red boxes include:

- Title: NAT Exempt
- Status: ON
- Placement: Before Auto NAT Rules
- Type: Static
- Source Interface: inside
- Destination Interface: Any
- Source Address: inside_192.168.70
- Source Port: Any
- Destination Address: peer_192.168.50.0
- Destination Port: Any
- OK button

Sito1FTD_Nat_Exempt_Rule

Add NAT Rule

Title

NAT Exempt

Create Rule for

Manual NAT

Status

☒

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement

Before Auto NAT Rules

Type

Static

Packet Translation

Advanced Options

☐ Translate DNS replies that match this rule

☐ Fallthrough to Interface PAT (Destination Interface)

☒ Perform route lookup for Destination interface

☐ Do not proxy ARP on Destination Interface

Show Diagram

☐

CANCEL

OK

Sito1FTD_Nat_Exempt_Rule_2

Firewall Device Manager

Monitoring

Policies

Objects

Device: ftdv742

admin Administrator

SECURE

Security Policies

SSL Decryption

Identity

Security Intelligence

NAT

Access Control

Intrusion

3 rules

Filter

#	NAME	TYPE	INTERFACES	ORIGINAL PACKET				TRANSLATED PACKET				ACTIONS
				SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	
Manual NAT Rules												
> 1	NAT Exempt	STATIC	Inside Any	inside_192.1...	peer_192.16...	ANY	ANY	inside_192.1...	peer_192.16...	ANY	ANY	
Manual NAT Rules (After)												
> 1	ISP1NatRule	DYNAMIC	Inside outside	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY	
> 3	ISP2NatRule	DYNAMIC	Inside outside2	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY	

Sito1FTD_Nat_Rule_Overview

Passaggio 9. Distribuire le modifiche alla configurazione.

Firewall Device Manager

Monitoring

Policies

Objects

Device: ftdv742

admin Administrator

SECURE

Sito1FTD_Deployment_Changes

Configurazione VPN FTD sito 2

Passaggio 10. Ripetere i passaggi da 1 a 9 con i parametri corrispondenti per l'FTD del sito 2.

DemoS2S Connection Profile

VPN Access Interface

demovti25 (169.254.10.2)

Peer IP Address

192.168.30.1

IKE V2

IKE Policy

aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14, aes,aes-256-sha,sha256-sha,sha256-14

IPSec Proposal

aes,aes-256-sha-1,sha-256

Authentication Type

Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration

28800 seconds

Lifetime Size

4608000 kilobytes

Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

Diffie-Hellman Group

Null (not selected)

BACK

FINISH

Site2FTD_ISP1_Review_VPN_Config_Summary

Demo_S2S_SP2 Connection Profile

Peer endpoint needs to be configured according to specified below configuration.

VPN Access Interface demovti_sp2 (169.254.20.12)



Peer IP Address 192.168.40.1

IKE V2

IKE Policy aes,aes-192,aes-256-sha512,sha384,sha,sha256-sha512,sha384,sha,sha256-21,20,16,15,14, aes,aes-256-sha,sha256-sha,sha256-14
IPSec Proposal aes,aes-256-sha-1,sha-256
Authentication Type Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

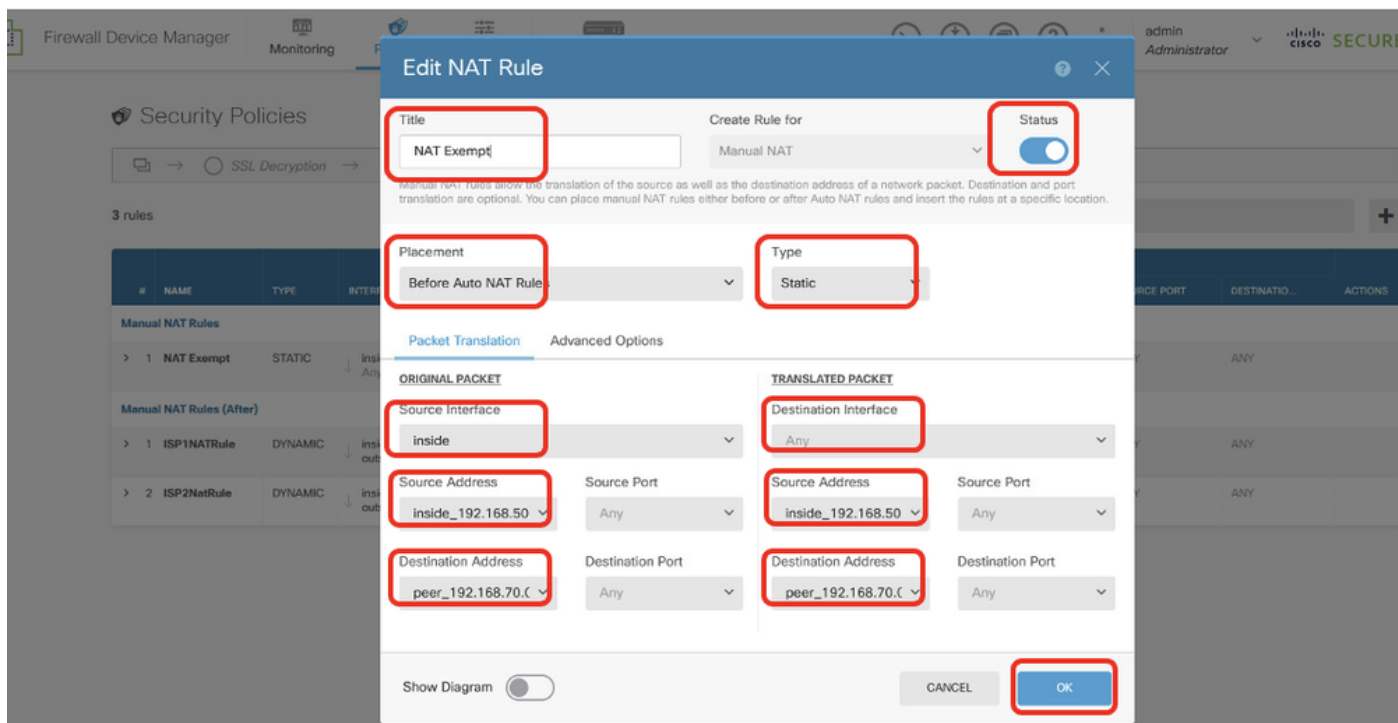
Lifetime Duration 28800 seconds
Lifetime Size 4608000 kilobytes

Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

Diffie-Hellman Group Null (not selected)

BACK

FINISH

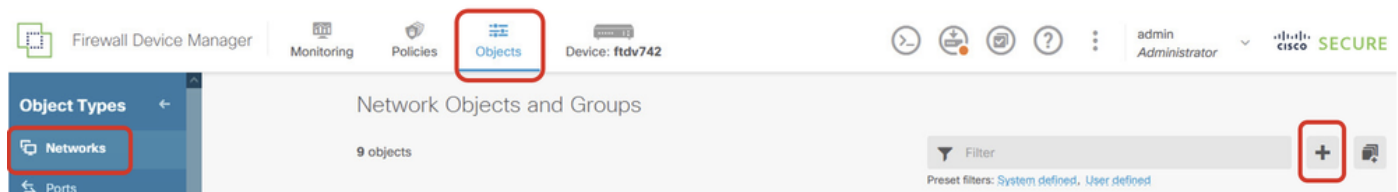


Site2FTD_Nat_Exempt_Rule

Configurazioni su PBR

Configurazione PBR FTD sito1

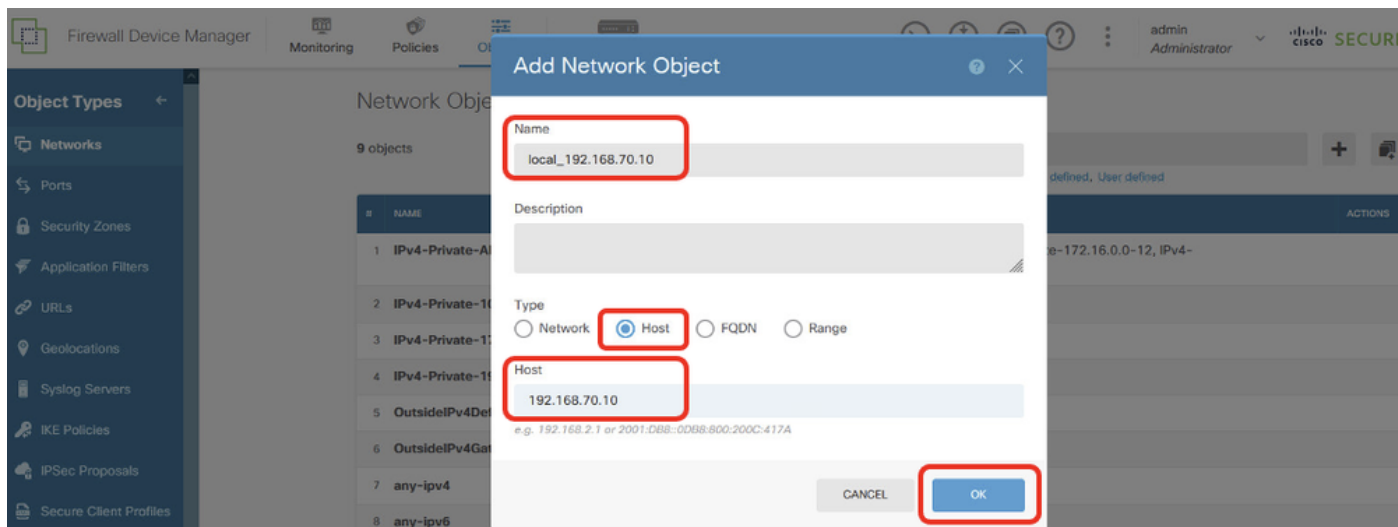
Passaggio 11. Creare nuovi oggetti di rete da utilizzare con l'elenco degli accessi PBR per il FTD del sito 1. Passare a Oggetti > Reti e fare clic sul pulsante +.



Sito1FTD_Create_Network_Object

Passaggio 11.1. Creare l'oggetto dell'indirizzo IP del client2 del sito 1. Fornire le informazioni necessarie. Fare clic sul pulsante OK.

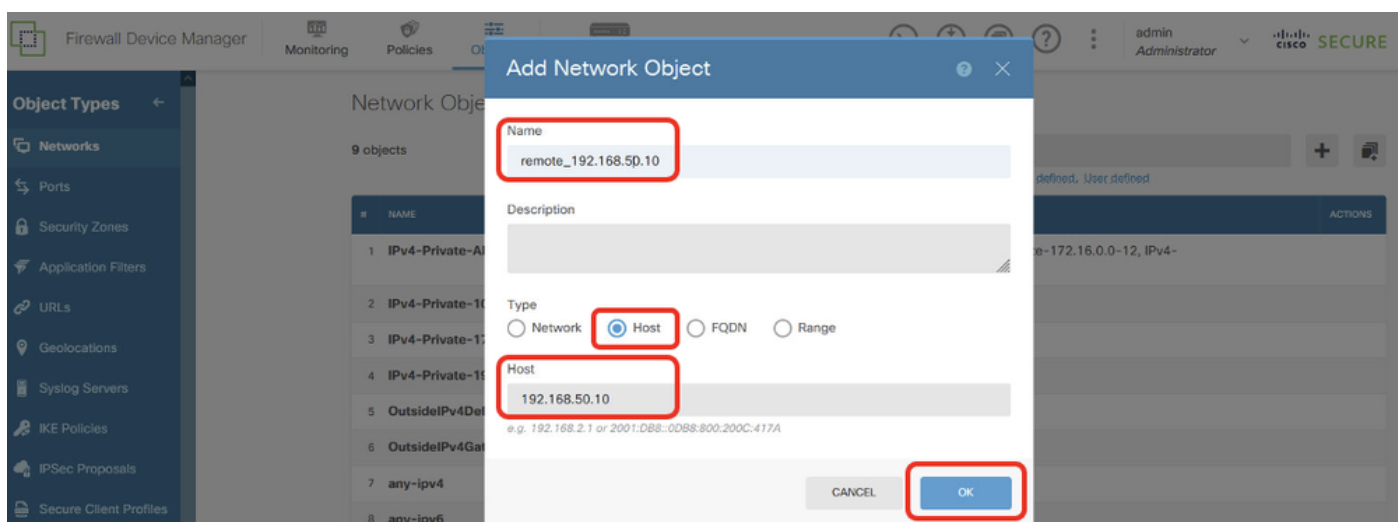
- Nome: local_192.168.70.10
- Tipo: Host
- Host: 192.168.70.10



Sito1FTD_Sito1FTD_PBR_LocalObject

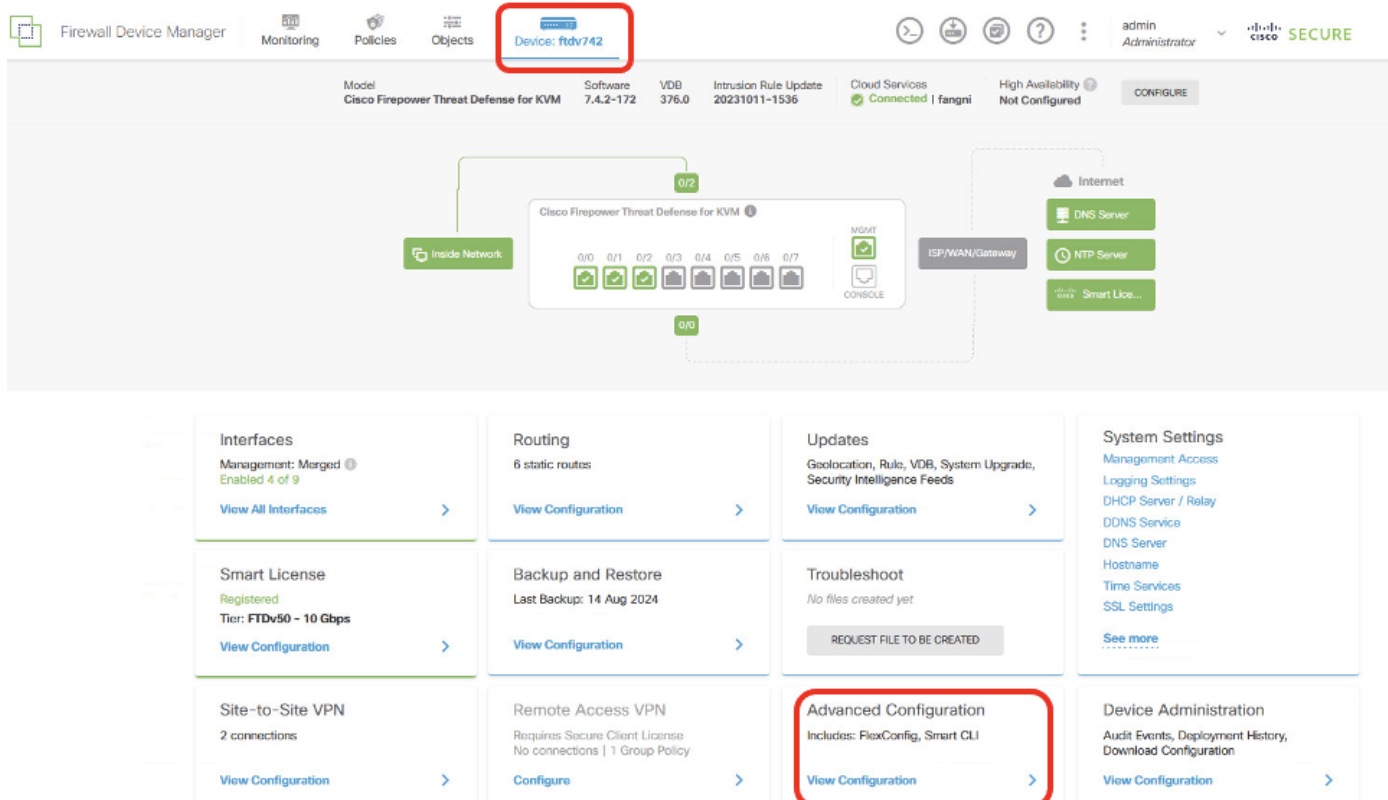
Passaggio 11.2. Creare l'oggetto dell'indirizzo IP del client2 del sito. Fornire le informazioni necessarie. Fare clic sul pulsante OK.

- Nome: remote_192.168.50.10
- Tipo: Host
- Host: 192.168.50.10



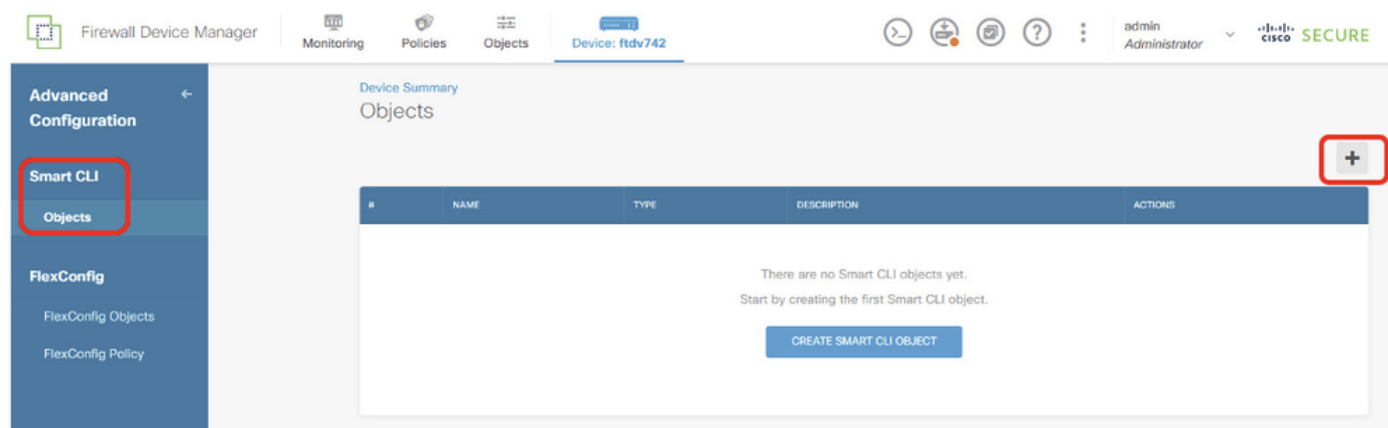
Sito1FTD_PBR_RemoteObject

Passaggio 12. Creare un elenco degli accessi estesi per PBR. Selezionare Periferica > Configurazione avanzata. Fare clic su Visualizza configurazione.



Sito1FTD_View_Advanced_Configuration

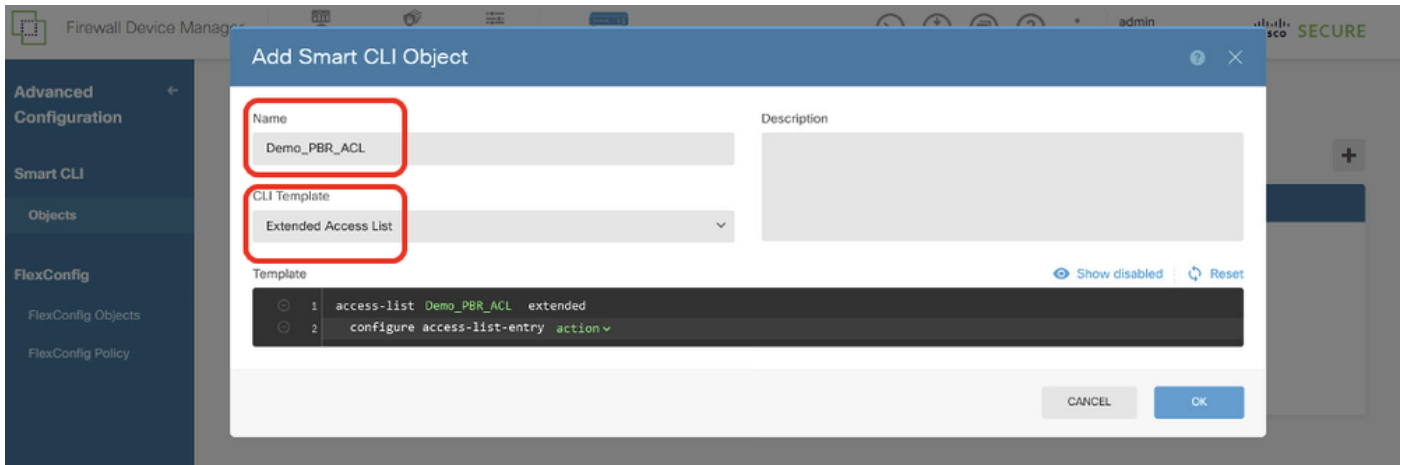
Passaggio 12.1. Passare a Smart CLI > Oggetti. Fare clic sul pulsante +.



Sito1FTD_Add_SmartCLI_Object

Passaggio 12.2. Immettere un nome per l'oggetto e scegliere il modello CLI.

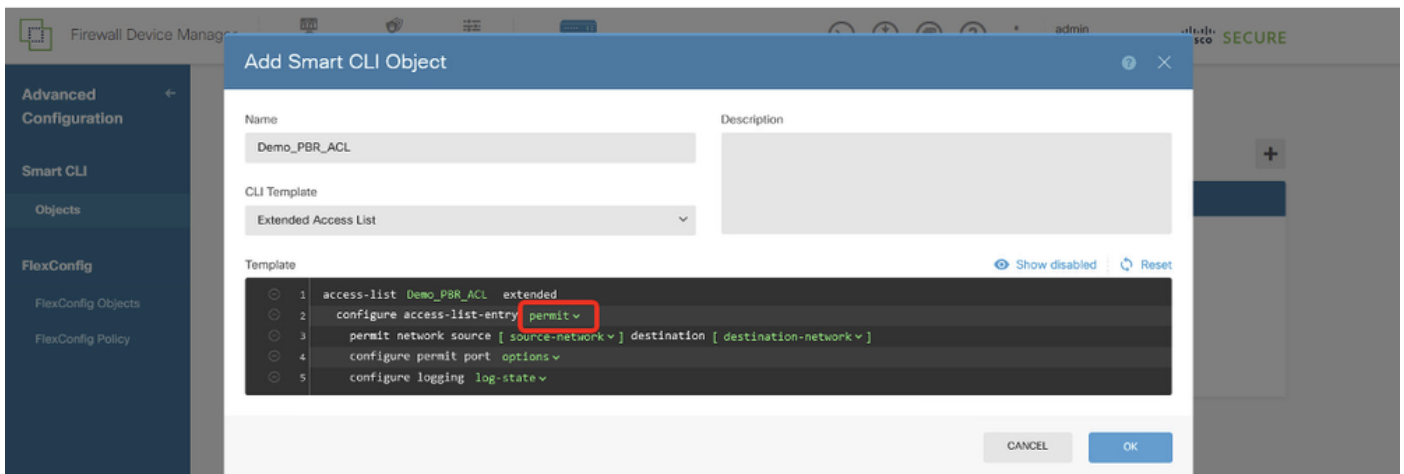
- Nome: Demo_PBR_ACL
- Modello CLI: Elenco accessi estesi



Sito1FTD_Create_PBR_ACL_1

Passaggio 12.3. Passare a Modello e configurare. Per salvare, fare clic sul pulsante OK.

Riga 2, fare clic su azione. Scegliere permesso.

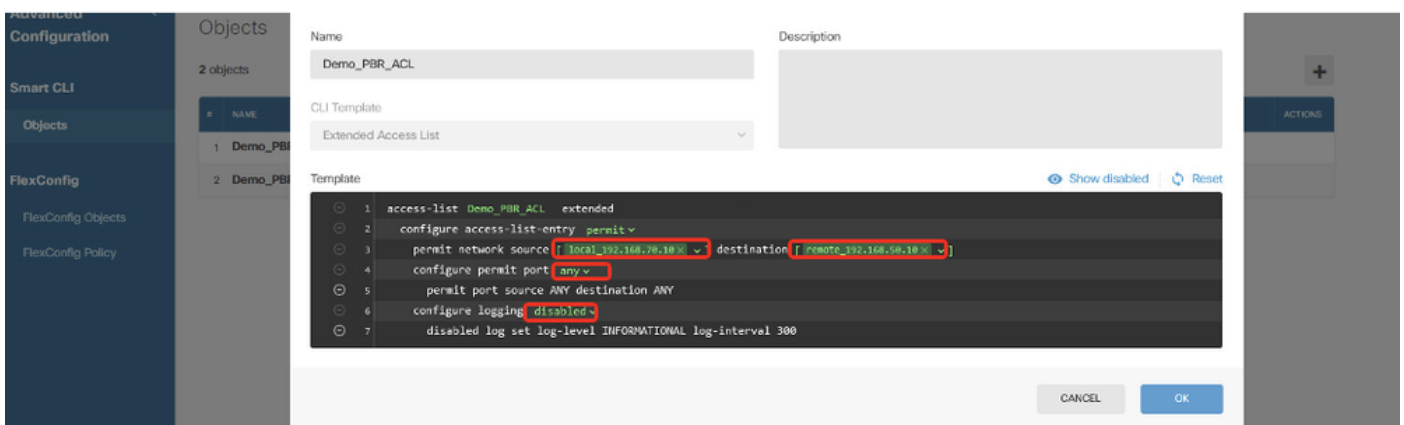


Sito1FTD_Create_PBR_ACL_2

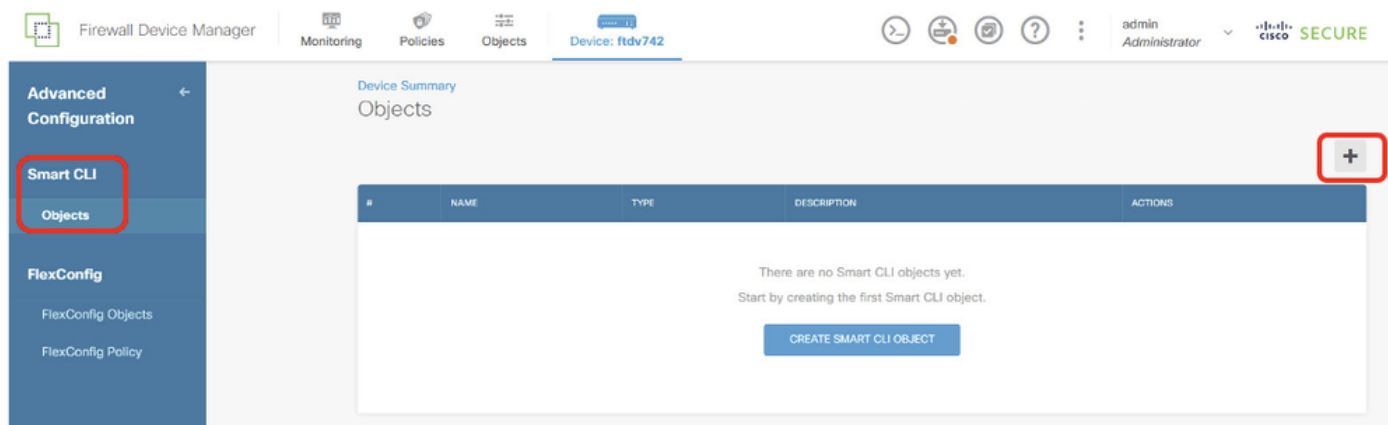
Linea 3, fare clic su source-network. Scegliere local_192.168.70.10. Fare clic su rete di destinazione. Selezionare remote_192.168.50.10.

Linea 4, fare clic su opzioni e scegliere qualsiasi.

Alla riga 6, fare clic su log-state e selezionare disabled.

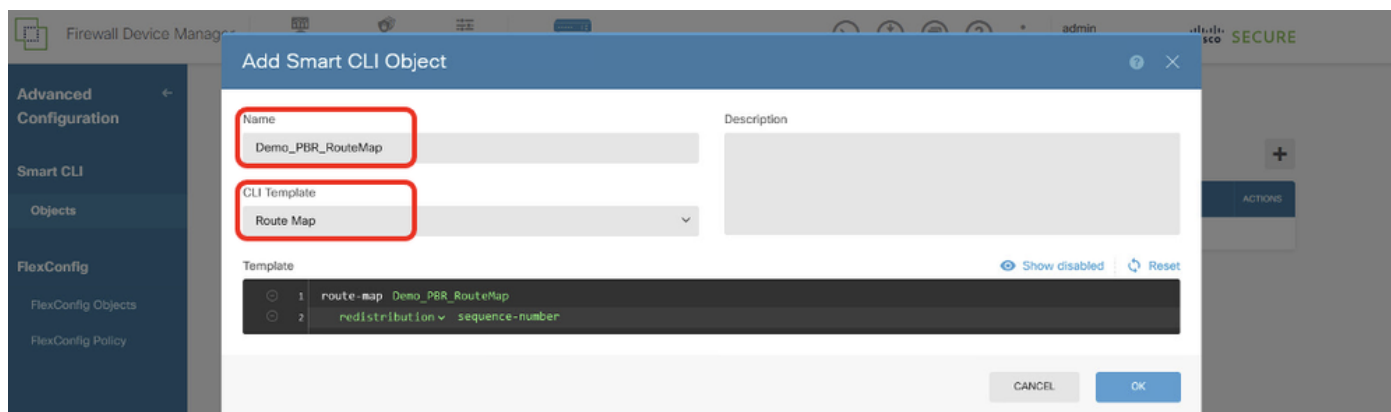


Passaggio 13. Creare la mappa del percorso per PBR. Passare a Dispositivo > Configurazione avanzata > Smart CLI > Oggetti. Fare clic sul pulsante +.



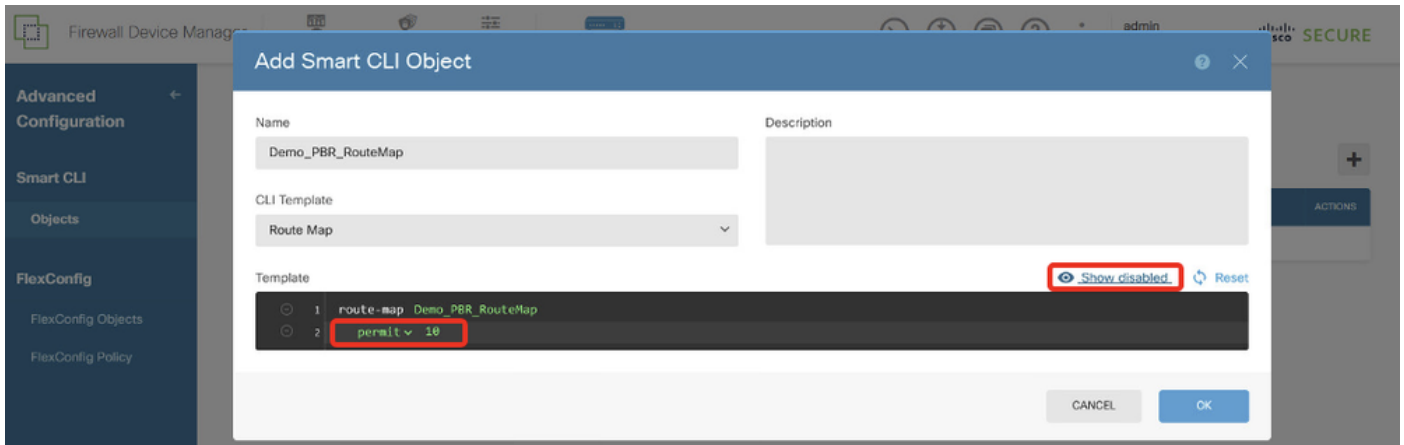
Passaggio 13.1. Immettere un nome per l'oggetto e scegliere il modello CLI.

- Nome: Demo_PBR_RouteMap
- Modello CLI: Mappa ciclo di lavorazione



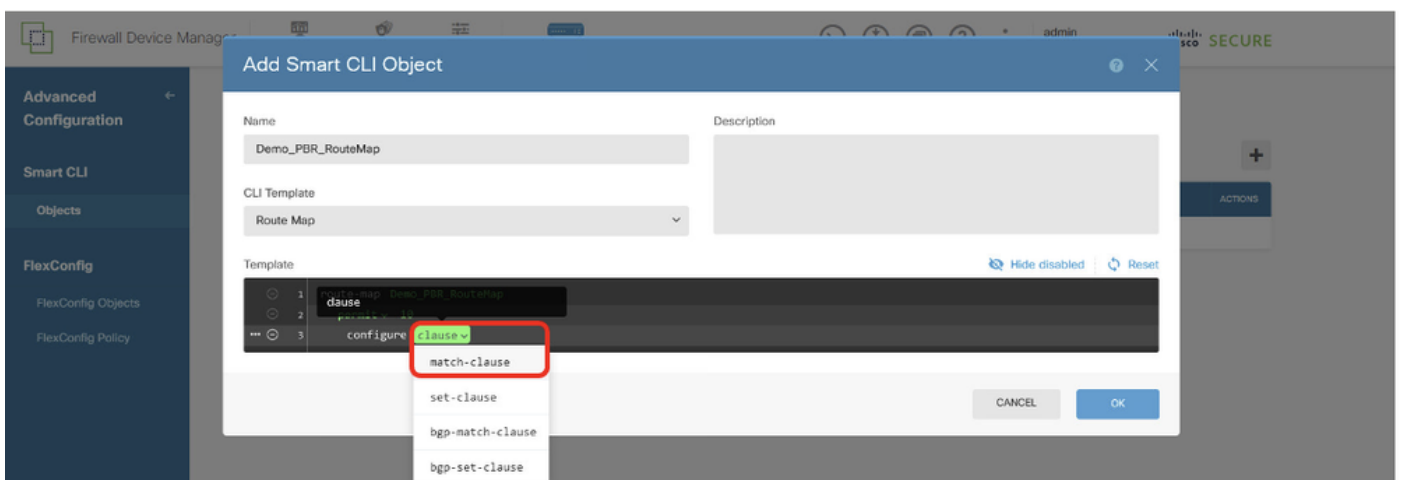
Passaggio 13.2. Passare a Modello e configurare. Fare clic sul pulsante OK per salvare.

Linea 2, fare clic su redistribuzione. Scegliere permesso. Fare clic su numero-sequenza, input manuale 10. Fare clic su Mostra disattivato.



Sito1FTD_Create_PBR_RouteMap_2

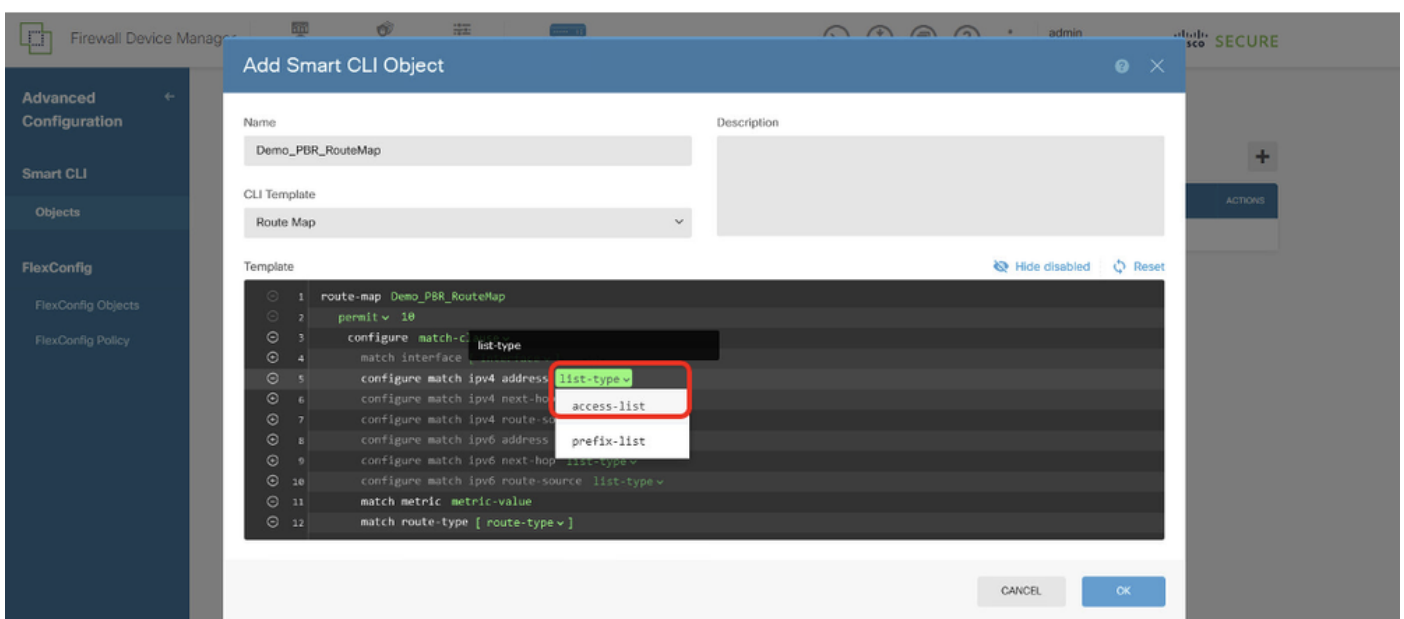
Linea 3: fare clic su + per attivare la linea. Fare clic su clausola. Scegliere match-clause.



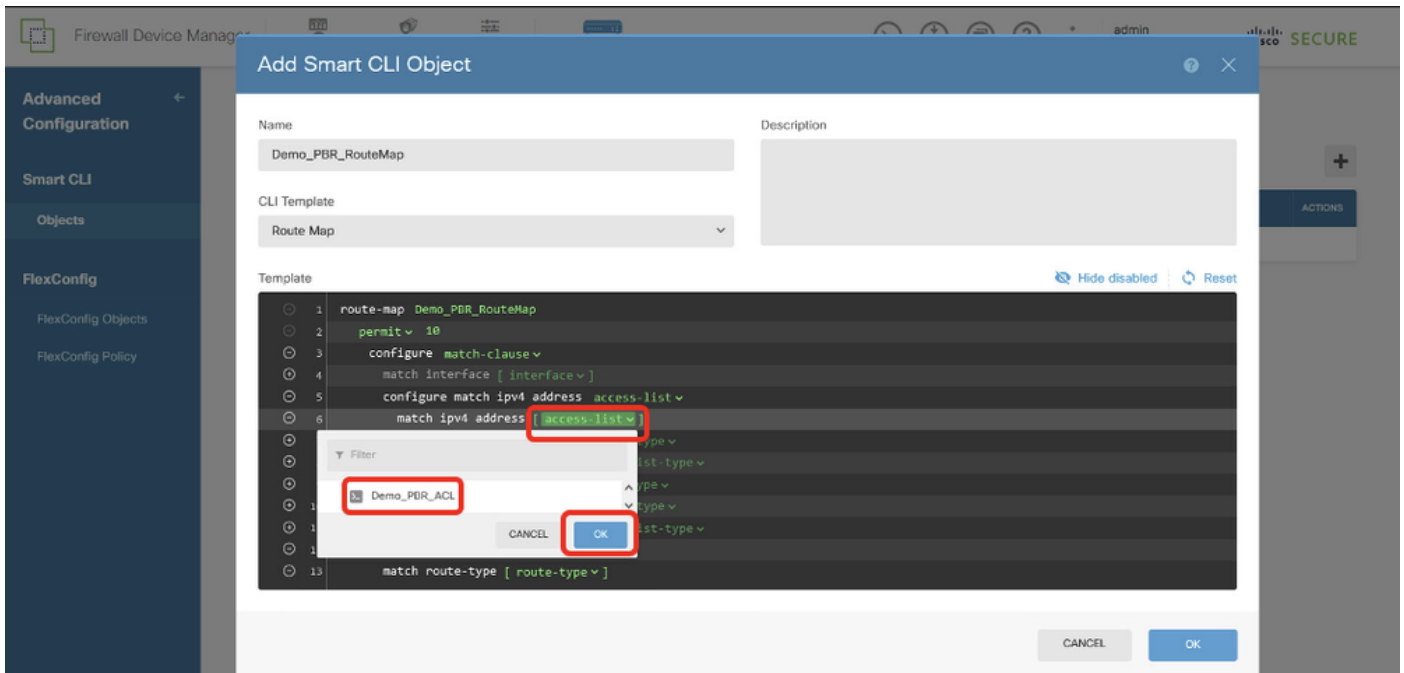
Sito1FTD_Create_PBR_RouteMap_3

Linea 4, fare clic - per disattivare la linea.

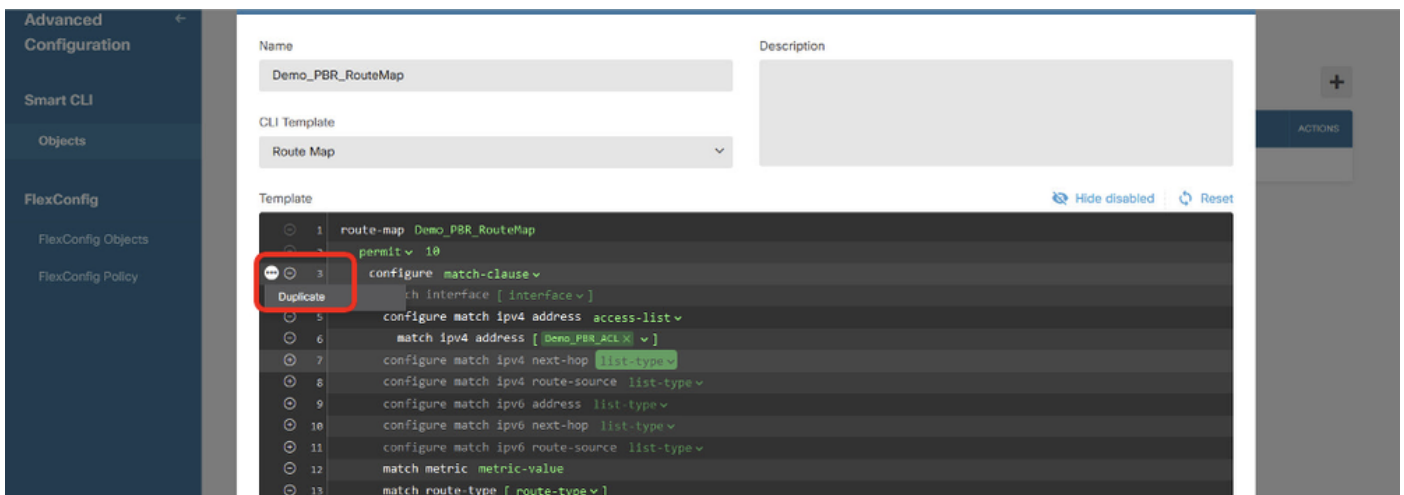
Linea 5, fare clic su + per attivare la linea. Fare clic su list-type. Selezionare access-list.



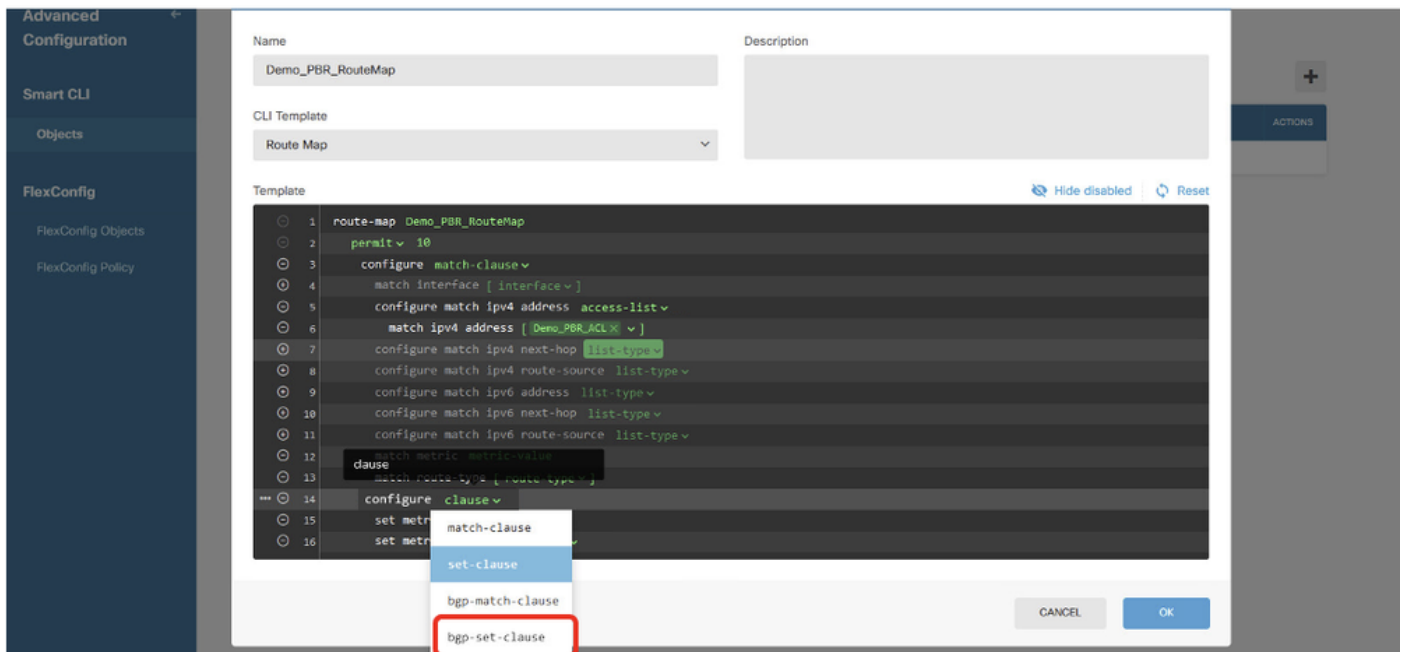
Alla riga 6, fare clic su access-list. Selezionare il nome dell'ACL creato nel passaggio 12. Nell'esempio, questo nome è Demo_PBR_ACL.



Tornare alla riga 3. Fare clic sulle opzioni ... e scegliere Duplica.



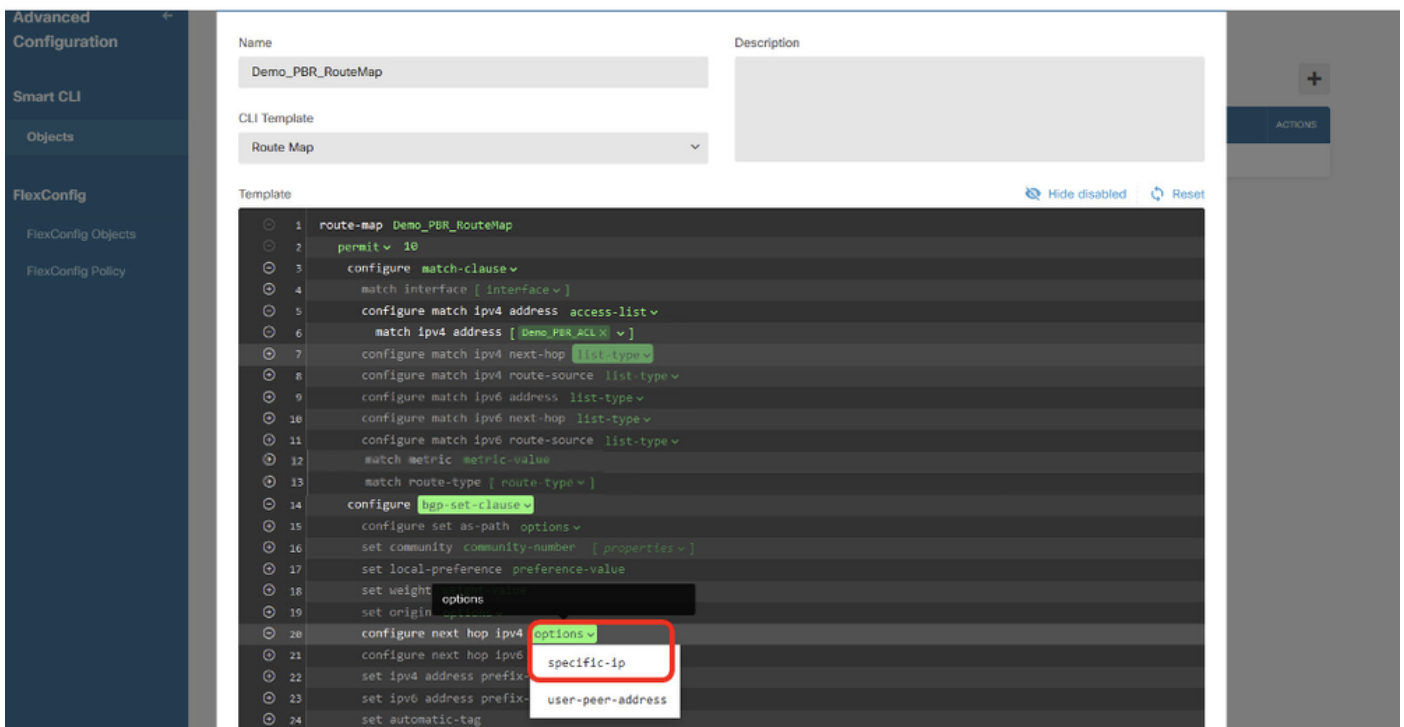
Alla riga 14, fare clic su clause, quindi selezionare bgp-set-clause.



Sito1FTD_Create_PBR_RouteMap_7

Nelle righe 12, 13, 15, 16, 17, 18, 19, 21, 22, 23, 24, fare clic - pulsante per disabilitare.

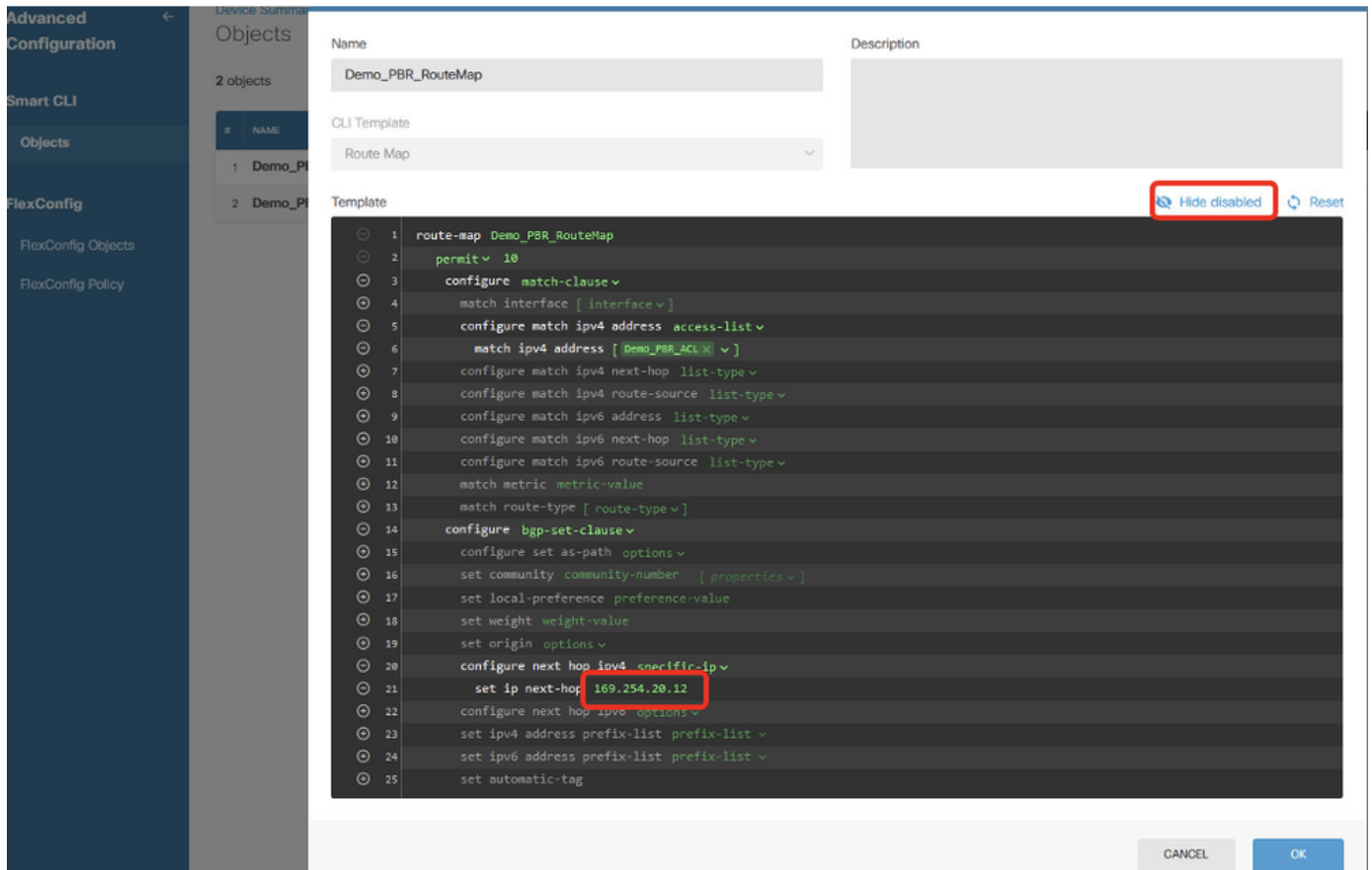
Nella riga 20, fare clic su options (opzioni), quindi selezionare specific-ip (ip specifico).



Sito1FTD_Create_PBR_RouteMap_8

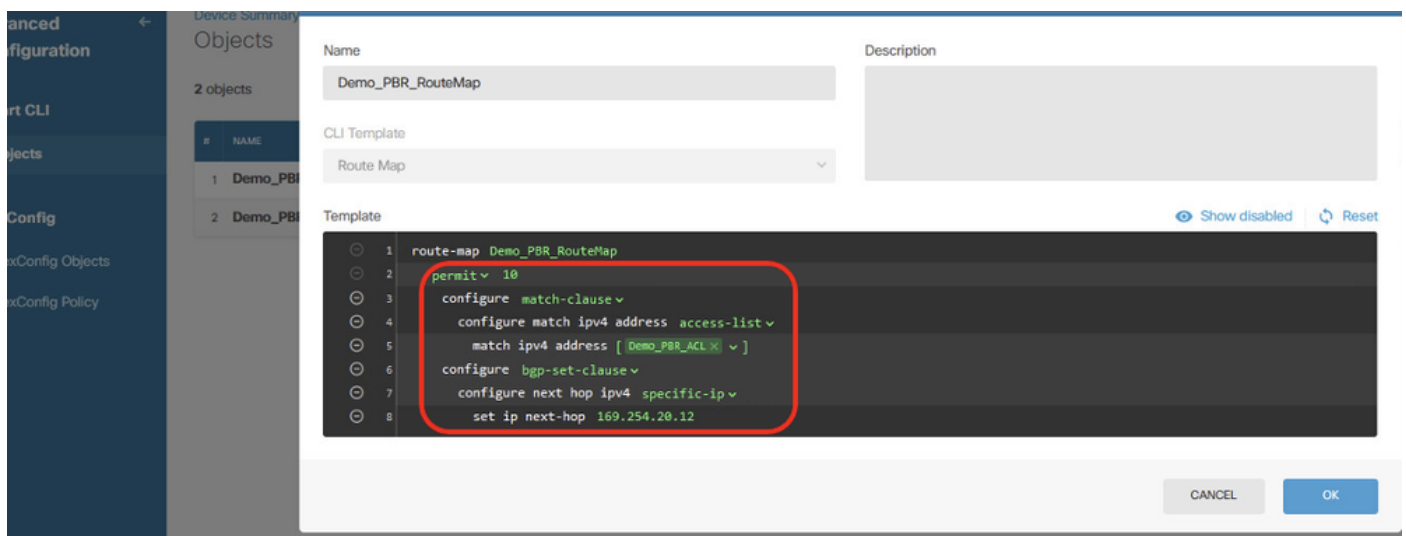
Alla riga 21, fare clic su ip-address. Inserire manualmente l'indirizzo IP dell'hop successivo.

Nell'esempio, questo valore è l'indirizzo IP del peer Site2 FTD VTI tunnel2 (169.254.20.12). Fare clic su Nascondi disattivato.



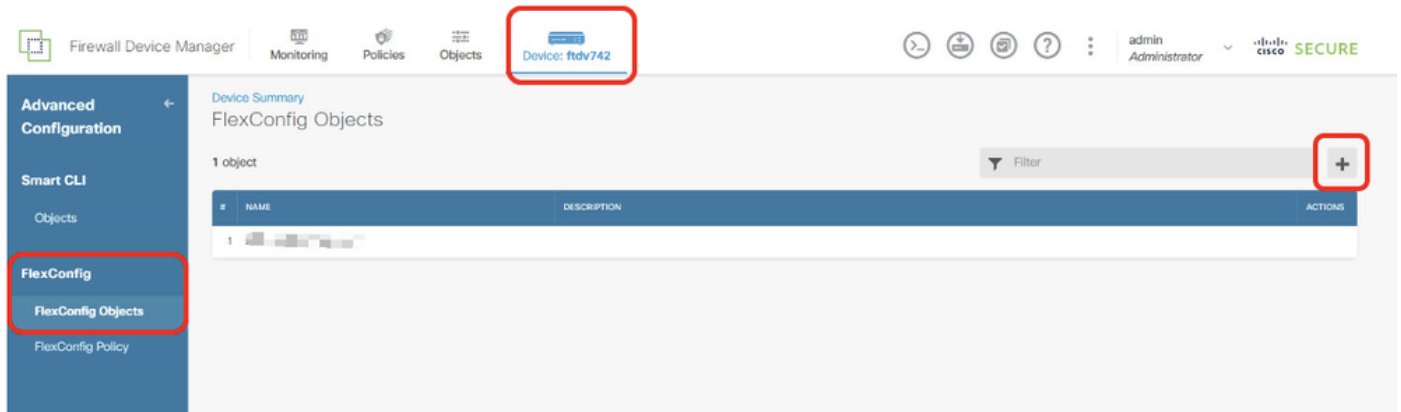
Sito1FTD_Create_PBR_RouteMap_9

Esaminare la configurazione della mappa dei percorsi.



Sito1FTD_Create_PBR_RouteMap_10

Passaggio 14. Creare un oggetto FlexConfig per PBR. Selezionare Dispositivo > Configurazione avanzata > Oggetti FlexConfig e fare clic sul pulsante +.



Sito1FTD_Create_PBR_FlexObj_1

Passaggio 14.1. Immettere un nome per l'oggetto. In questo esempio, Demo_PBR_FlexObj. Nell'editor Template e Nega template, immettere le righe di comando.

- Modello:

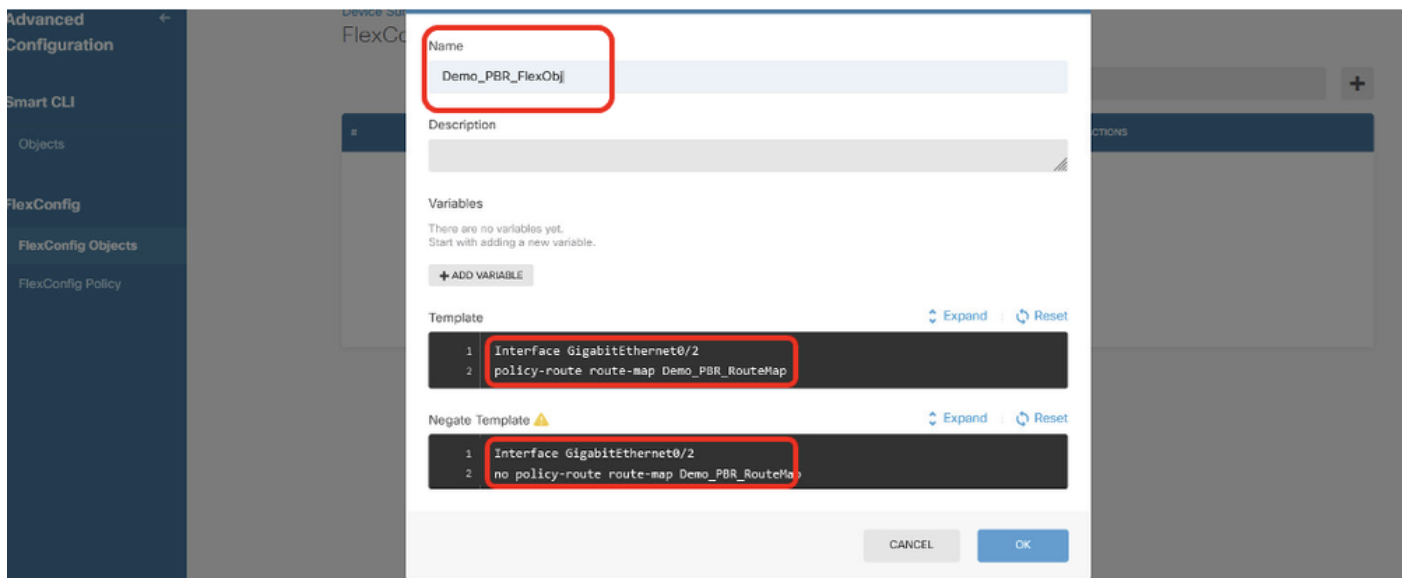
interfaccia Gigabit Ethernet0/2

policy-route route-map_Demo_PBR_RouteMap_Site2

- Nega modello:

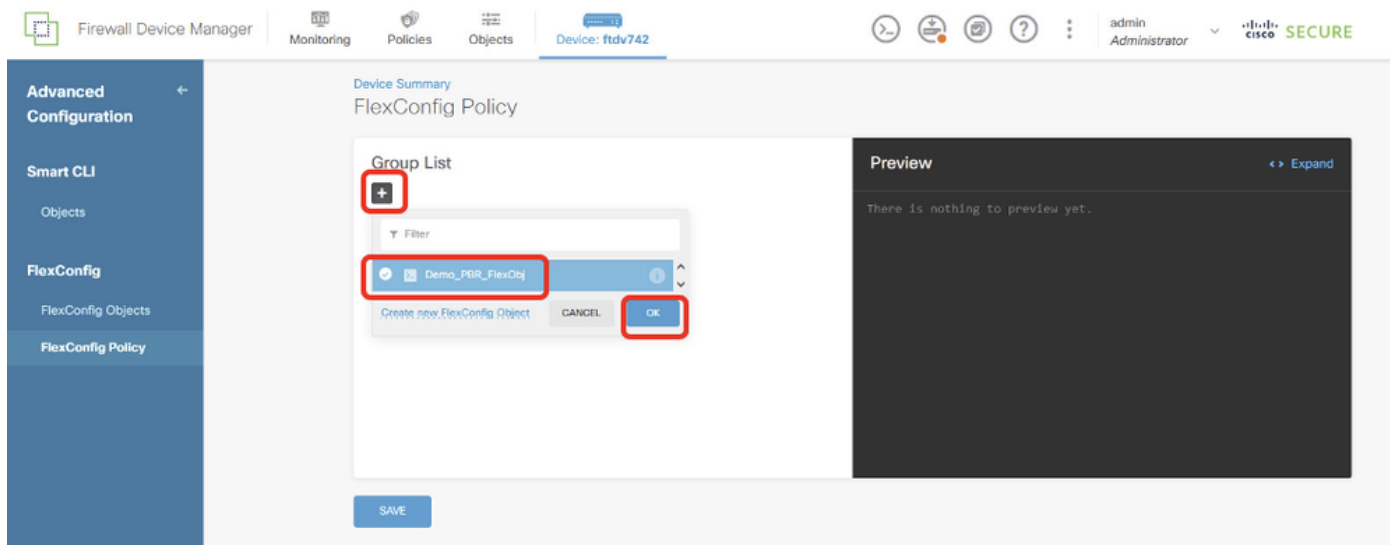
interfaccia Gigabit Ethernet0/2

nessuna route-route-map Demo_PBR_RouteMap_Site2



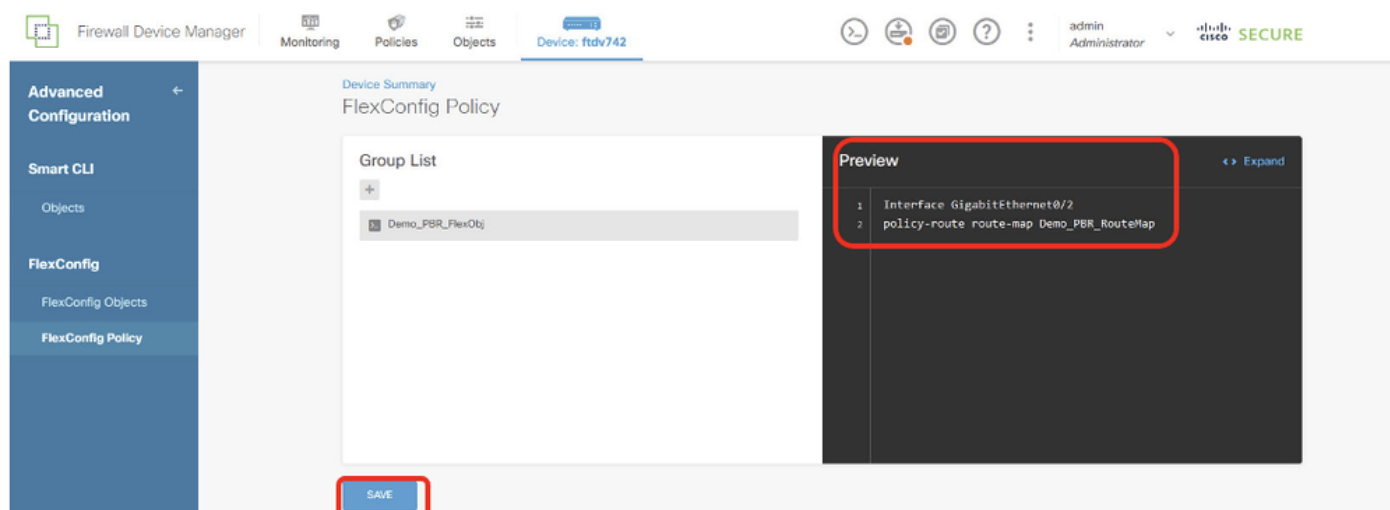
Sito1FTD_Create_PBR_FlexObj_2

Passaggio 15. Creare il criterio FlexConfig per PBR. Passare a Dispositivo > Configurazione avanzata > Criterio FlexConfig. Fare clic sul pulsante +. Scegliere il nome dell'oggetto FlexConfig creato nel passaggio 14. Fare clic sul pulsante OK.



Sito1FTD_Create_PBR_FlexPolicy_1

Passaggio 15.1. Verificare il comando nella finestra Anteprima. Se è corretto, fare clic su Salva.



Sito1FTD_Create_PBR_FlexPolicy_2

Passaggio 16. Distribuire le modifiche alla configurazione.



Sito1FTD_Deployment_Changes

Configurazione PBR FTD sito 2

Passaggio 17. Ripetere il passaggio 11. fino al passaggio 16. per creare PBR con i parametri corrispondenti per l'FTD del sito 2.

Firewall Device Manager

Advanced Configuration

Smart CLI

Objects

FlexConfig

FlexConfig Objects

FlexConfig Policy

Add Smart CLI Object

Name: Demo_PBR_ACL_Site2

Description:

CLI Template: Extended Access List

Template

```
1 access-list Demo_PBR_ACL_Site2 extended
2 configure access-list-entry permit
3 permit network source [ local_192.168.50.10 % ] destination [ remote_192.168.70.10 % ]
4 configure permit port any
5 permit port source ANY destination ANY
6 configure logging disabled
7 disabled log set log-level INFORMATIONAL log-interval 300
```

Show disabled Reset

CANCEL OK

Site2FTD_Create_PBR_ACL

Firewall Device Manager

Advanced Configuration

Smart CLI

Objects

FlexConfig

FlexConfig Objects

FlexConfig Policy

Add Smart CLI Object

Name: Demo_PBR_RouteMap_Site2

Description:

CLI Template: Route Map

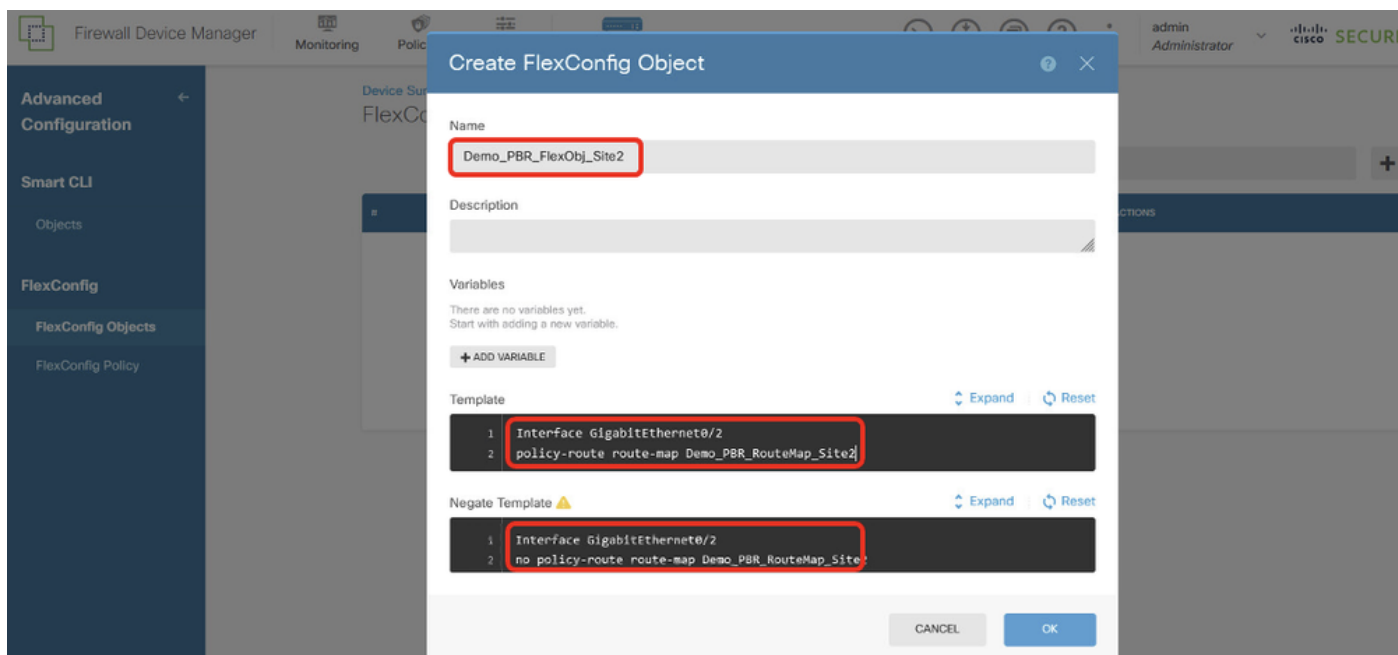
Template

```
1 route-map Demo_PBR_RouteMap_Site2
2 permit 10
3 configure match-clause
4 configure match ipv4 address access-list
5 match ipv4 address [ Demo_PBR_ACL_Site2 % ]
6 configure bgp-set-clause
7 configure next hop ipv4 specific-ip
8 set ip next-hop 169.254.20.11
```

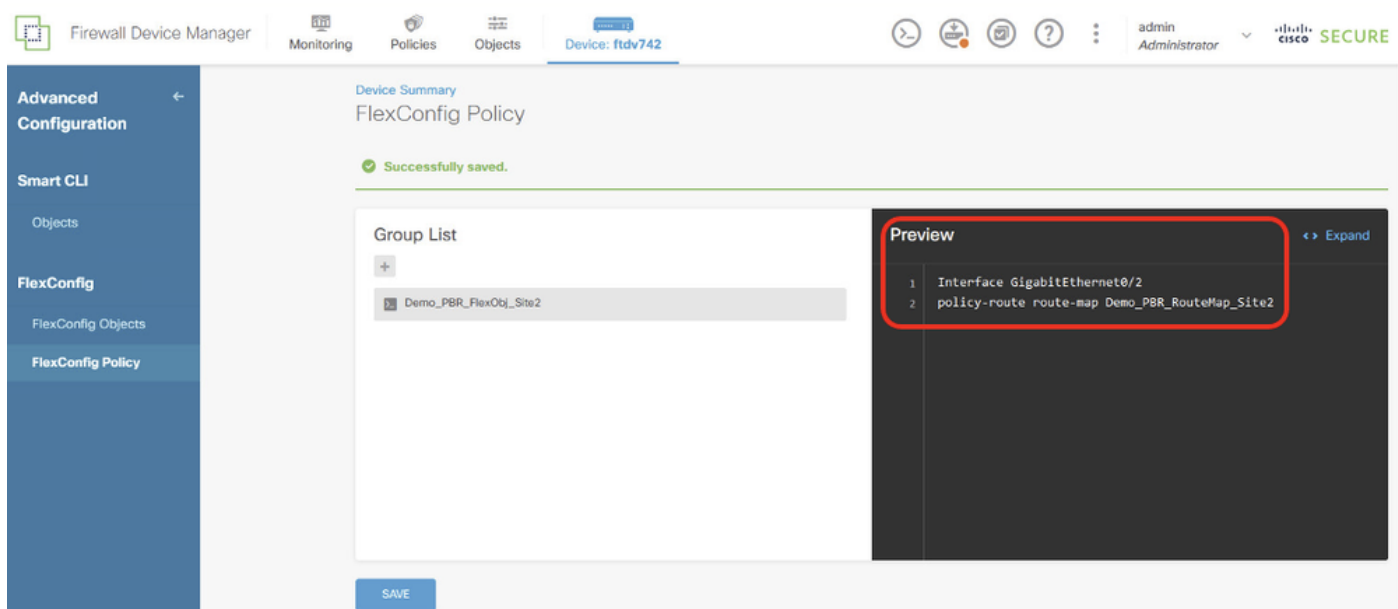
Show disabled Reset

CANCEL OK

Site2FTD_Create_PBR_RouteMap



Site2FTD_Create_PBR_FlexObj

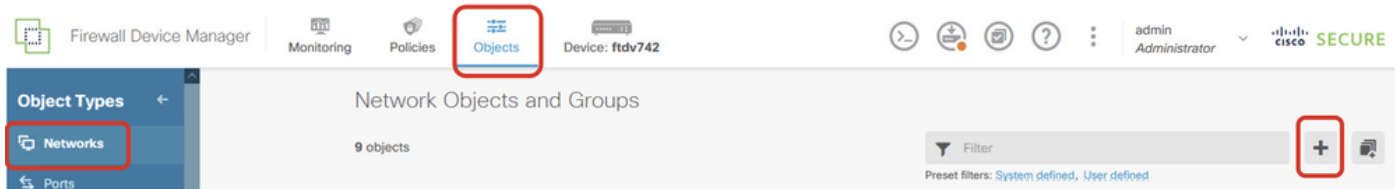


Site2FTD_Create_PBR_FlexPolicy

Configurazioni su SLA Monitor

Configurazione monitoraggio SLA FTD del sito 1

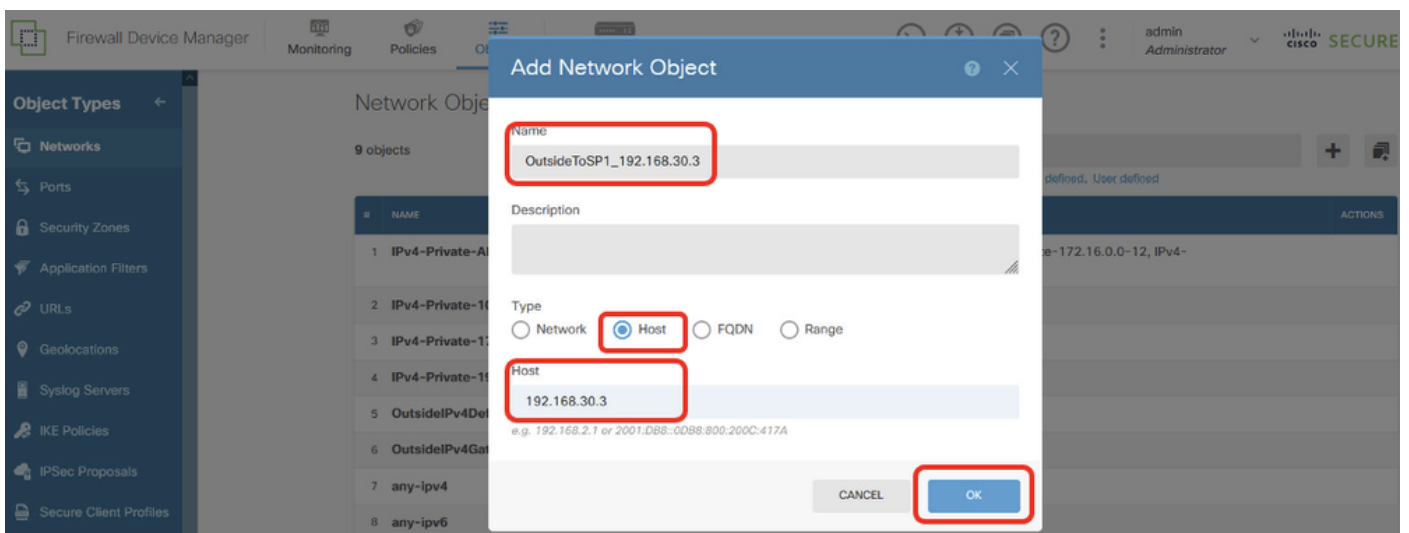
Passaggio 18. Creare nuovi oggetti di rete da utilizzare per i monitor SLA per il FTD del sito 1. Passare a Oggetti > Reti, fare clic sul pulsante +.



Sito1FTD_Create_Network_Object

Passaggio 18.1. Creare l'oggetto per l'indirizzo IP del gateway ISP1. Fornire le informazioni necessarie. Fare clic sul pulsante OK.

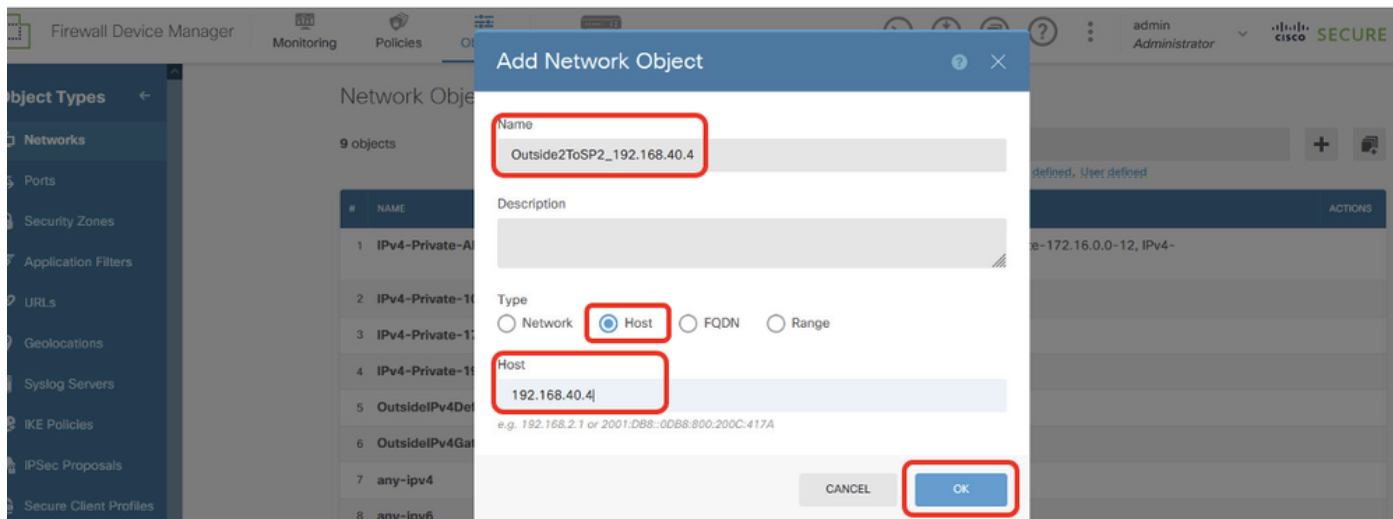
- Nome: OutsideToSP1_192.168.30.3
- Tipo: Host
- Host: 192.168.30.3



Sito1FTD_Create_SLAMonitor_NetObj_ISP1

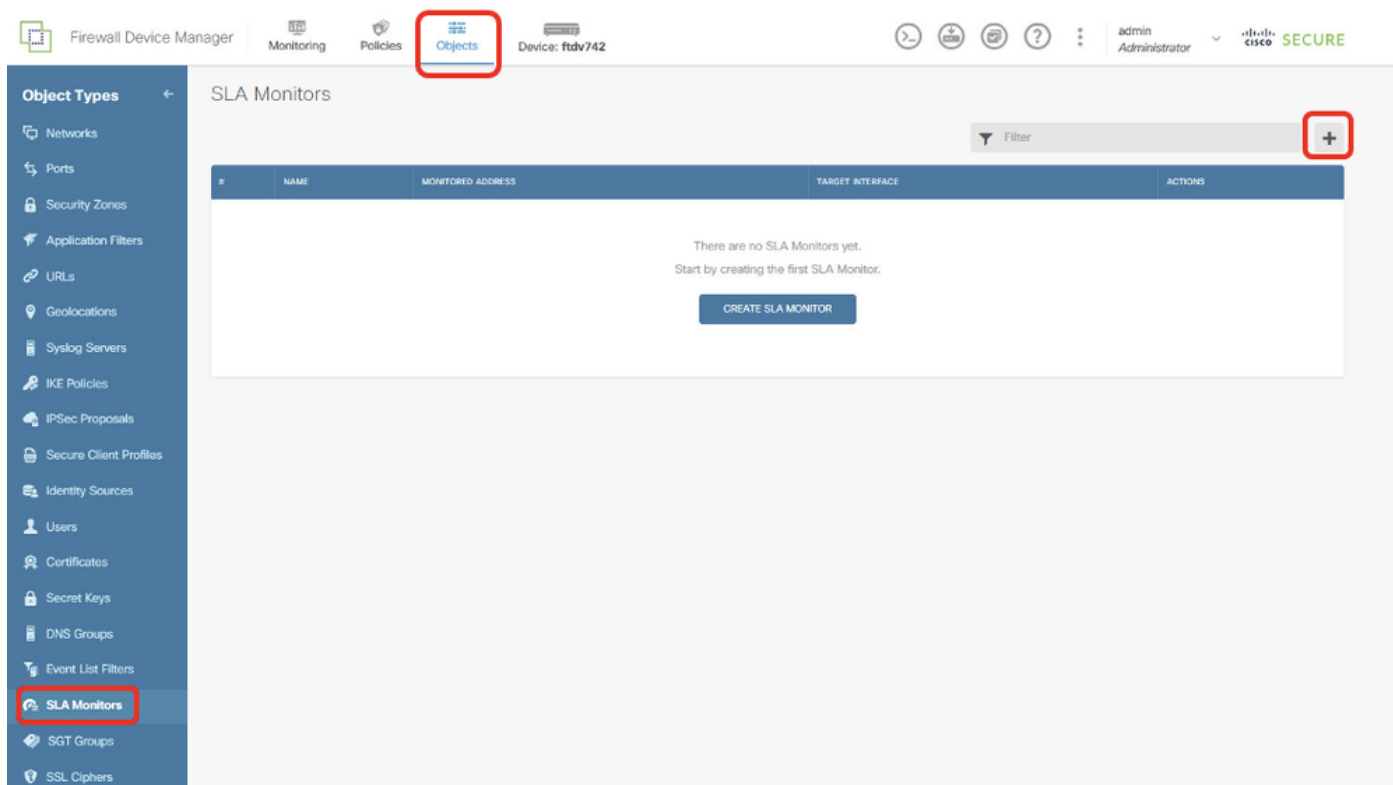
Passaggio 18.2. Creare l'oggetto per l'indirizzo IP del gateway ISP2. Fornire le informazioni necessarie. Fare clic sul pulsante OK.

- Nome: Outside2ToSP2_192.168.40.4
- Tipo: Host
- Host: 192.168.40.4



Sito1FTD_Create_SLAMonitor_NetObj_ISP2

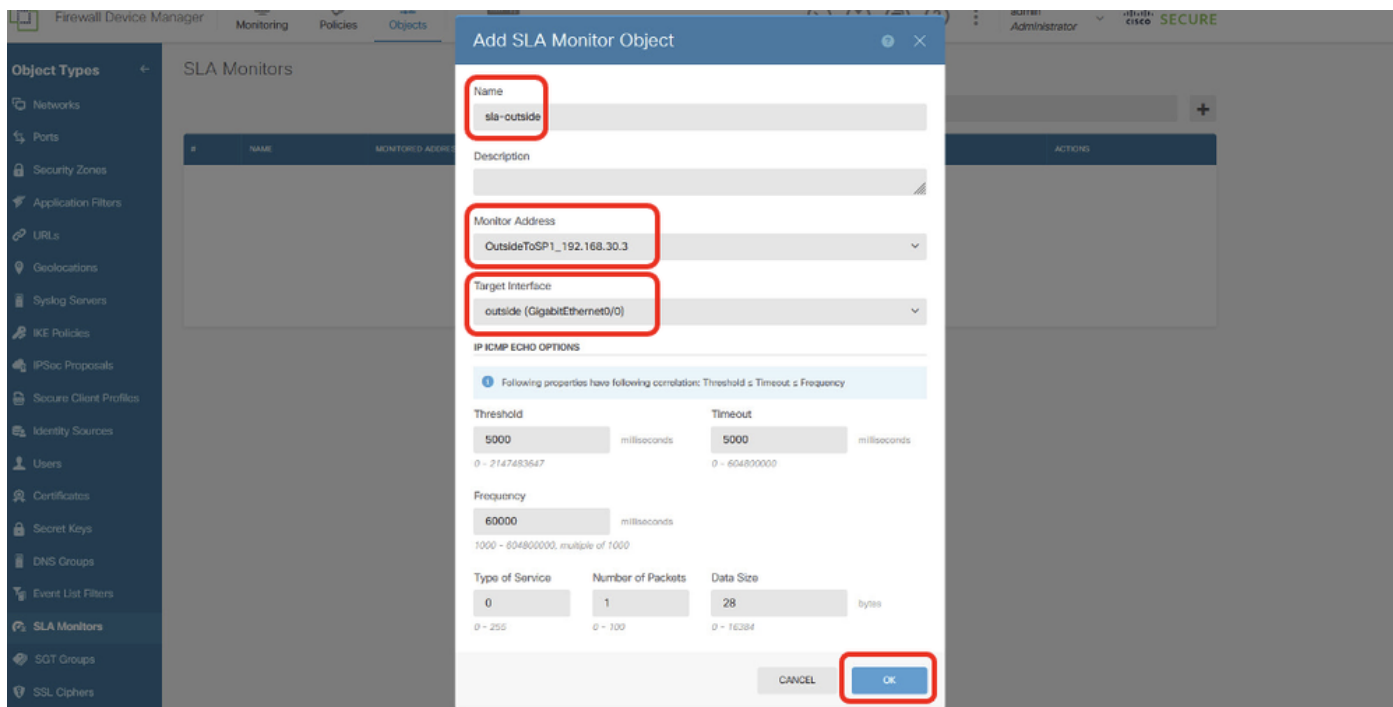
Passaggio 19. Creazione del monitoraggio del contratto di servizio. Passare a Oggetti > Tipi di oggetto > Monitor SLA. Fare clic sul pulsante + per creare un nuovo monitoraggio del contratto di servizio.



Sito1FTD_Create_SLAMonitor

Passaggio 19.1. Nella finestra Aggiungi oggetto di monitoraggio SLA, fornire le informazioni necessarie per il gateway ISP1. Fare clic sul pulsante OK per salvare.

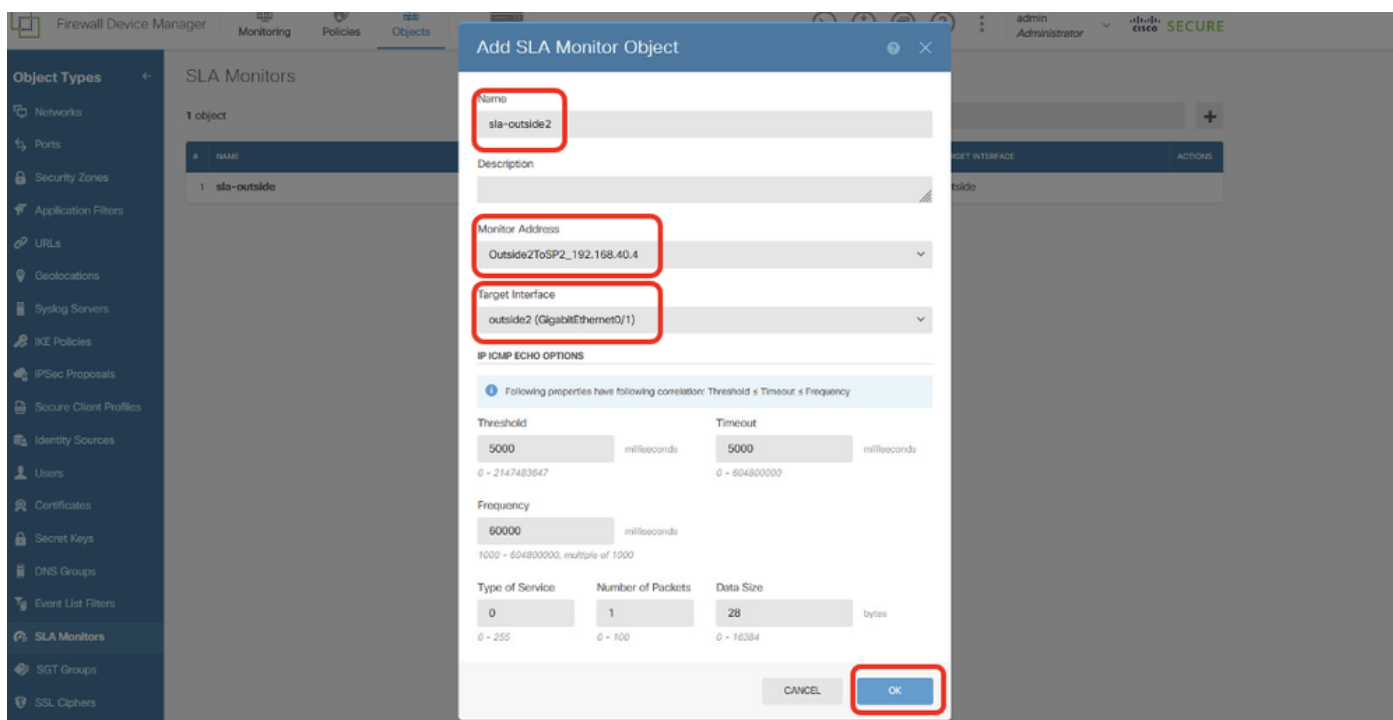
- Nome: sla-esterno
- Indirizzo monitor: OutsideToSP1_192.168.30.3
- Interfaccia di destinazione: esterno (Gigabit Ethernet0/0)
- OPZIONI ECHO IP ICMP: predefinito



Site1FTD_Create_SLAMonitor_NetObj_ISP1_Details

Passaggio 19.2. Continuare a fare clic sul pulsante + per creare un nuovo monitoraggio SLA per il gateway ISP2. Nella finestra Aggiungi oggetto di monitoraggio SLA, fornire le informazioni necessarie per il gateway ISP2. Fare clic sul pulsante OK per salvare.

- Nome: sla-esterno2
- Indirizzo monitor: Outside2ToSP2_192.168.40.4
- Interfaccia di destinazione: esterno2(Gigabit Ethernet0/1)
- OPZIONI ECHO IP ICMP: predefinito



Sito1FTD_Create_SLAMonitor_NetObj_ISP2_Details

Passaggio 20. Distribuire le modifiche alla configurazione.



Sito1FTD_Deployment_Changes

Configurazione monitoraggio SLA FTD del sito 2

Passaggio 21. Ripetere il passaggio 18. fino al passaggio 20. creare il controllo del contratto di servizio con i parametri corrispondenti nell'FTD del sito 2.

SLA Monitor

2 objects

#	NAME
1	sla-outside
2	sla-outside

Name: sla-outside

Description:

Monitor Address: OutsideToSP1_192.168.10.3

Target Interface: outside (GigabitEthernet0/0)

IP ICMP ECHO OPTIONS

Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold: 5000 milliseconds (0 - 2147483647)

Timeout: 5000 milliseconds (0 - 604800000)

Frequency: 60000 milliseconds (1000 - 604800000, multiple of 1000)

Type of Service: 0 (0 - 255)

Number of Packets: 1 (0 - 100)

Data Size: 28 bytes (0 - 16384)

CANCEL OK

Site2FTD_Create_SLAMonitor_NetObj_ISP1_Details

Object Types

- Networks
- Ports
- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Secure Client Profiles
- Identity Sources
- Users
- Certificates
- Secret Keys
- DNS Groups
- Event List Filters
- SLA Monitors**
- SGT Groups

SLA Monitor

2 objects

#	NAME
1	sla-outside2
2	sla-outside2

Name
sla-outside2

Description

Monitor Address
Outside2ToSP2_192.168.20.4

Target Interface
outside2 (GigabitEthernet0/1)

IP ICMP ECHO OPTIONS

Following properties have following correlation: Threshold ≤ Timeout ≤ Frequency

Threshold
5000 milliseconds
0 - 2147483647

Timeout
5000 milliseconds
0 - 604800000

Frequency
60000 milliseconds
1000 - 604800000, multiple of 1000

Type of Service
0
0 - 255

Number of Packets
1
0 - 100

Data Size
28 bytes
0 - 16384

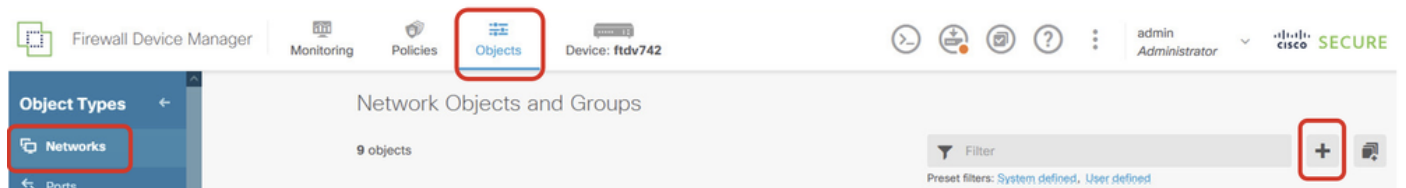
CANCEL **OK**

Site2FTD_Create_SLAMonitor_NetObj_ISP2_Details

Configurazioni su route statica

Configurazione route statica FTD sito1

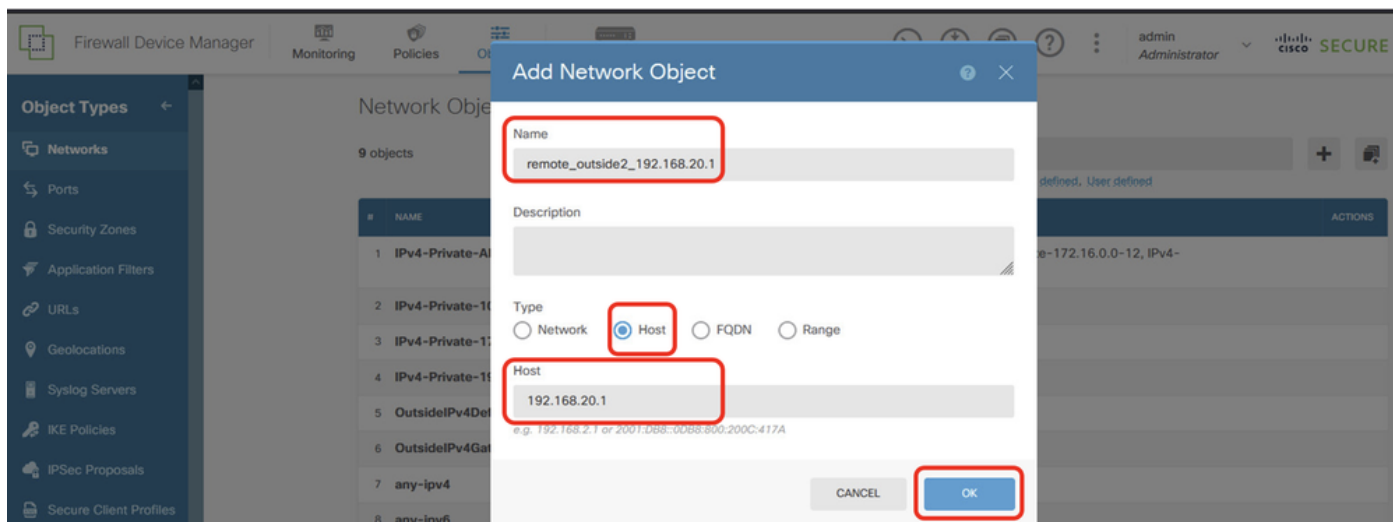
Passaggio 22. Creare nuovi oggetti di rete da utilizzare per l'instradamento statico per il FTD del sito 1. Passare a Oggetti > Reti, fare clic sul pulsante +.



Sito1FTD_Create_Obj

Passaggio 2.1. Creare l'oggetto per l'indirizzo IP esterno2 del FTD Sito2 peer. Fornire le informazioni necessarie. Fare clic sul pulsante OK.

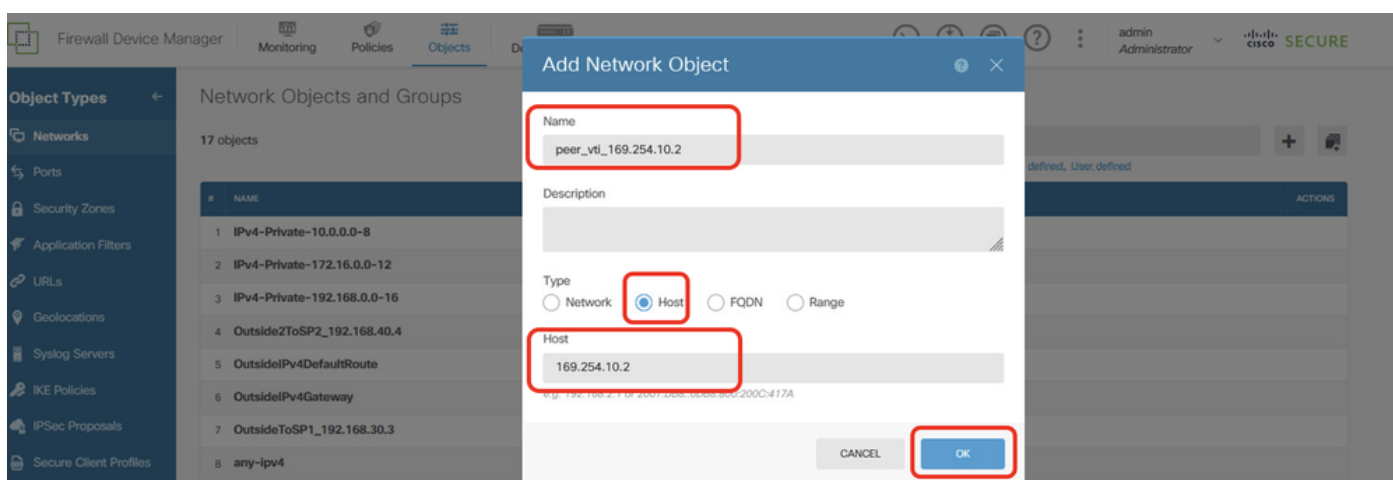
- Nome: remote_outside2_192.168.20.1
- Tipo: HOST
- Rete: 192.168.20.1



Sito1FTD_Create_NetObj_StaticRoute_1

Passaggio 2.2. Creare l'oggetto per l'indirizzo IP del tunnel VTI 1 del FTD Sito 2 peer. Fornire le informazioni necessarie. Fare clic sul pulsante OK.

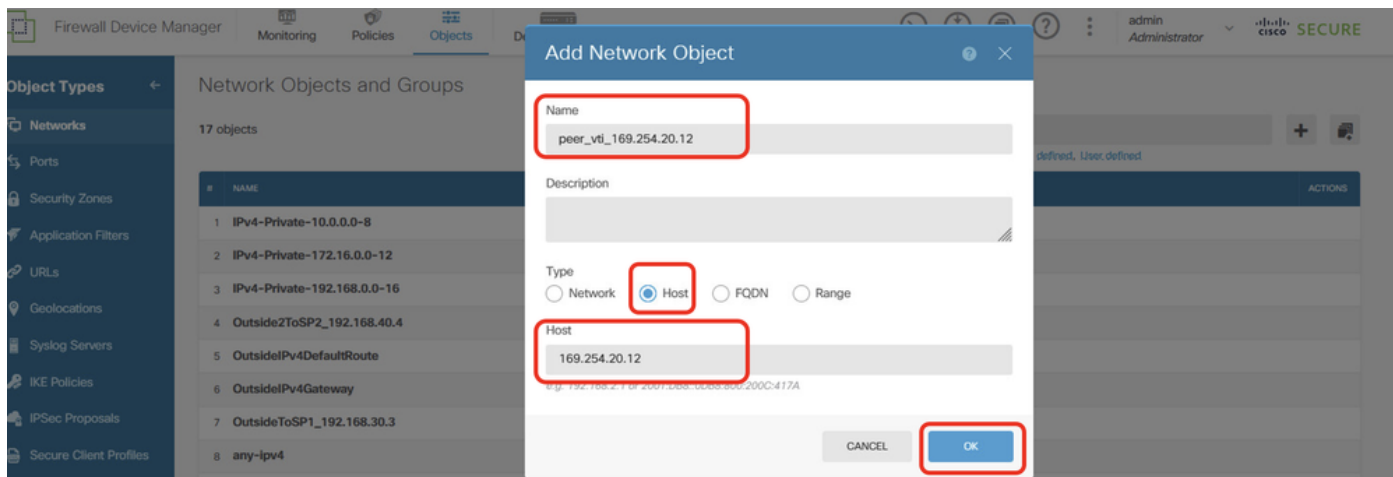
- Nome: peer_vti_169.254.10.2
- Tipo: HOST
- Rete: 169.254.10.2



Sito1FTD_Create_NetObj_StaticRoute_2

Passaggio 2.3. Creare l'oggetto per l'indirizzo IP del tunnel VTI2 del FTD Sito2 peer. Fornire le informazioni necessarie. Fare clic sul pulsante OK.

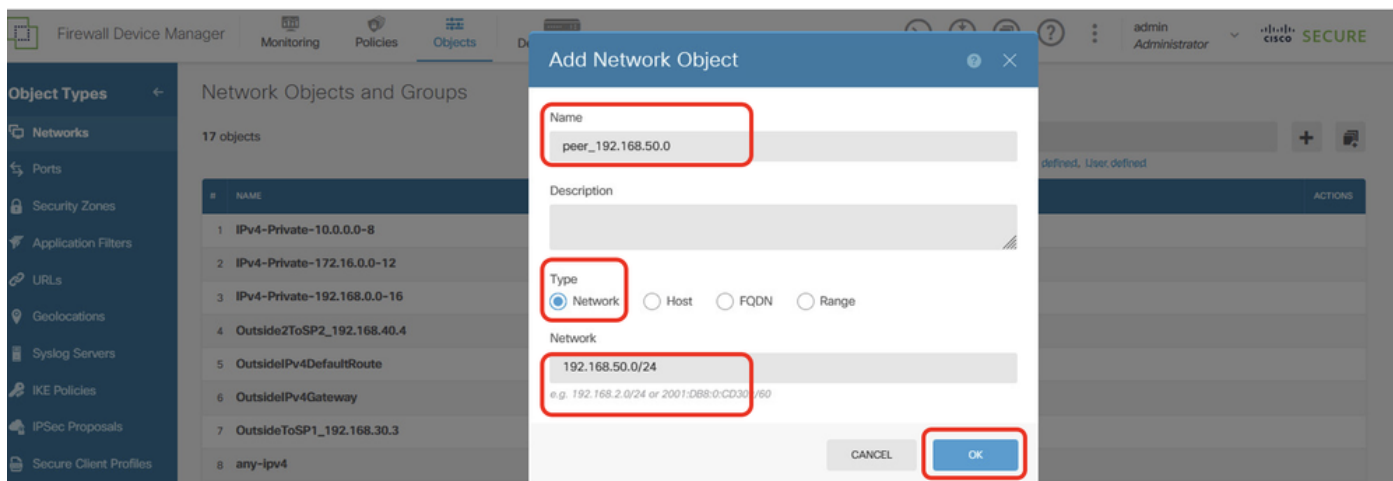
- Nome: peer_vti_169.254.20.12
- Tipo: HOST
- Rete: 169.254.20.12



Sito1FTD_Create_NetObj_StaticRoute_3

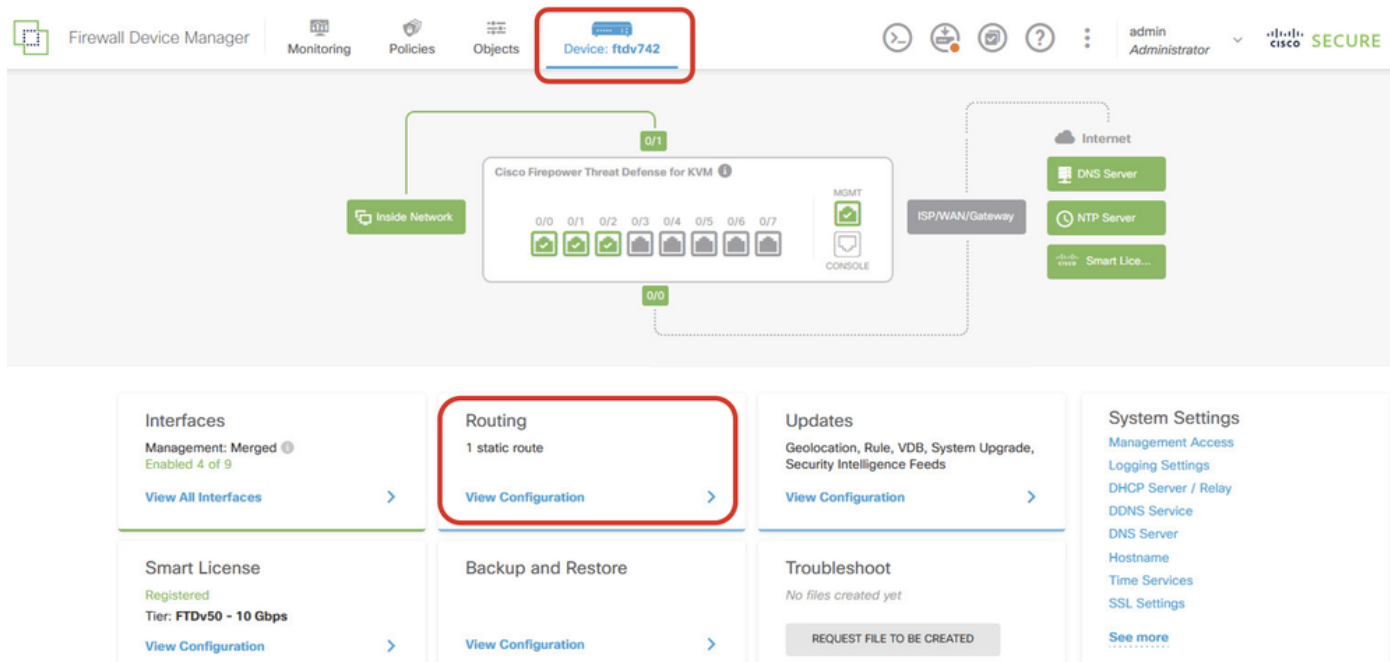
Passaggio 2.4. Creare l'oggetto per la rete interna del FTD Sito2 peer. Fornire le informazioni necessarie. Fare clic sul pulsante OK.

- Nome: peer_192.168.50.0
- Tipo: RETE
- Rete: 192.168.50.0/24



Sito1FTD_Create_NetObj_StaticRoute_4

Passaggio 23. Passare a Periferica > Ciclo. Fare clic su Visualizza configurazione. Fare clic sulla scheda Instradamento statico. Fare clic sul pulsante + per aggiungere una nuova route statica.



Sito1FTD_View_Route_Configuration



Sito1FTD_Add_Static_Route

Passaggio 23.1. Creare una route predefinita utilizzando il gateway ISP1 con monitoraggio SLA. Se il gateway ISP1 subisce un'interruzione, il traffico passa al percorso predefinito di backup tramite ISP2. Una volta ripristinato ISP1, il traffico torna a utilizzare ISP1. Fornire le informazioni necessarie. Fare clic sul pulsante OK per salvare.

- Nome: ToSP1GW
- Interfaccia: esterno (Gigabit Ethernet0/0)
- Protocollo: IPv4
- Reti: any-ipv4
- Gateway: OutsideToSP1_192.168.30.3
- Metrica: 1
- Monitor SLA: sla-esterno

Add Static Route



Name

ToSP1GW

Description

Interface

outside (GigabitEthernet0/0)

Protocol



IPv4



IPv6

Networks



any-ipv4

Gateway

OutsideToSP1_192.168.30.3

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside

CANCEL

OK

Passaggio 23.2. Creare il percorso predefinito di backup tramite il gateway ISP2 del gateway. La metrica deve essere maggiore di 1. In questo esempio, la metrica è 2. Fornire le informazioni necessarie. Fare clic sul pulsante OK per salvare.

- Nome: PredefinitoInSP2GW
- Interfaccia: esterno2(Gigabit Ethernet0/1)
- Protocollo: IPv4
- Reti: any-ipv4
- Gateway: Outside2ToSP2_192.168.40.4
- Metrica: 2

Add Static Route



Name

DefaultToSP2GW

Description

Interface

outside2 (GigabitEthernet0/1)

Protocol



IPv4



IPv6

Networks



any-ipv4

Gateway

Outside2ToSP2_192.168.40.4

Metric

2

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

Passaggio 23.3. Creare una route statica per il traffico di destinazione verso l'indirizzo IP esterno2 di un FTD Sito2 peer tramite gateway ISP2, con monitoraggio SLA, utilizzata per stabilire una VPN con FTD Sito2 esterno. Fornire le informazioni necessarie. Fare clic sul pulsante OK per salvare.

- Nome: SpecificoASP2GW
- Interfaccia: esterno2(Gigabit Ethernet0/1)
- Protocollo: IPv4
- Reti: remote_outside2_192.168.20.1
- Gateway: Outside2ToSP2_192.168.40.4
- Metrica: 1
- Monitor SLA: sla-esterno2

Add Static Route



Name

SpecificToSP2GW

Description

Interface

outside2 (GigabitEthernet0/1)

Protocol



IPv4



IPv6

Networks



remote_outside2_192.168.20.1

Gateway

Outside2ToSP2_192.168.40.4

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside2

CANCEL

OK

Passaggio 23.4. Creare un percorso statico per il traffico di destinazione verso la rete interna dell'FTD Sito2 peer tramite il tunnel VTI peer 1 dell'FTD Sito2 come gateway, con monitoraggio SLA per la crittografia del traffico client tramite il tunnel 1. Se il gateway ISP1 subisce un'interruzione, il traffico VPN passa al tunnel VTI 2 dell'ISP2. Una volta ripristinato l'ISP1, il traffico torna al tunnel VTI 1 dell'ISP1. Fornire le informazioni necessarie. Fare clic sul pulsante OK per salvare.

- Nome: ToVTISP1
- Interfaccia: demovti(Tunnel1)
- Protocollo: IPv4
- Reti: peer_192.168.50.0
- Gateway: peer_vti_169.254.10.2
- Metrica: 1
- Monitor SLA: sla-esterno

Add Static Route



Name

ToVTISP1|

Description

Interface

demovti (Tunnel1)

Protocol

☒ IPv4

☐ IPv6

Networks



peer_192.168.50.0

Gateway

peer_vti_169.254.10.2

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside

CANCEL

OK

Passaggio 23.5. Creare una route statica di backup per il traffico di destinazione alla rete interna dell'FTD Sito2 peer tramite il tunnel VTI peer 2 dell'FTD Sito2 come gateway, utilizzata per crittografare il traffico client tramite il tunnel 2. Impostare la metrica su un valore superiore a 1. In questo esempio, la metrica è 22. Fornire le informazioni necessarie. Fare clic sul pulsante OK per salvare.

- Nome: ToVTISP2_Backup
- Interfaccia: demovti_sp2(Tunnel2)
- Protocollo: IPv4
- Reti: peer_192.168.50.0
- Gateway: peer_vti_169.254.20.12
- Metrica: 22

Add Static Route



Name

ToVTISP2_Backup

Description

Interface

demovti_sp2 (Tunnel2)

Protocol



IPv4



IPv6

Networks



peer_192.168.50.0

Gateway

peer_vti_169.254.20.12

Metric

22

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

Passaggio 23.6. Creare una route statica per il traffico PBR. Traffico di destinazione verso il client Site2 tramite il tunnel VTI peer 2 dell'FTD del sito2 come gateway, con monitoraggio SLA. Fornire le informazioni necessarie. Fare clic sul pulsante OK per salvare.

- Nome: ToVTISP2
- Interfaccia: demovti_sp2(Tunnel2)
- Protocollo: IPv4
- Reti: remote_192.168.50.10
- Gateway: peer_vti_169.254.20.12
- Metrica: 1
- Monitor SLA: sla-esterno2

Add Static Route



Name

ToVTISP2

Description

Interface

demovti_sp2 (Tunnel2)

Protocol

☒ IPv4

☐ IPv6

Networks



remote_192.168.50.10

Gateway

peer_vti_169.254.20.12

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

sla-outside2

CANCEL

OK

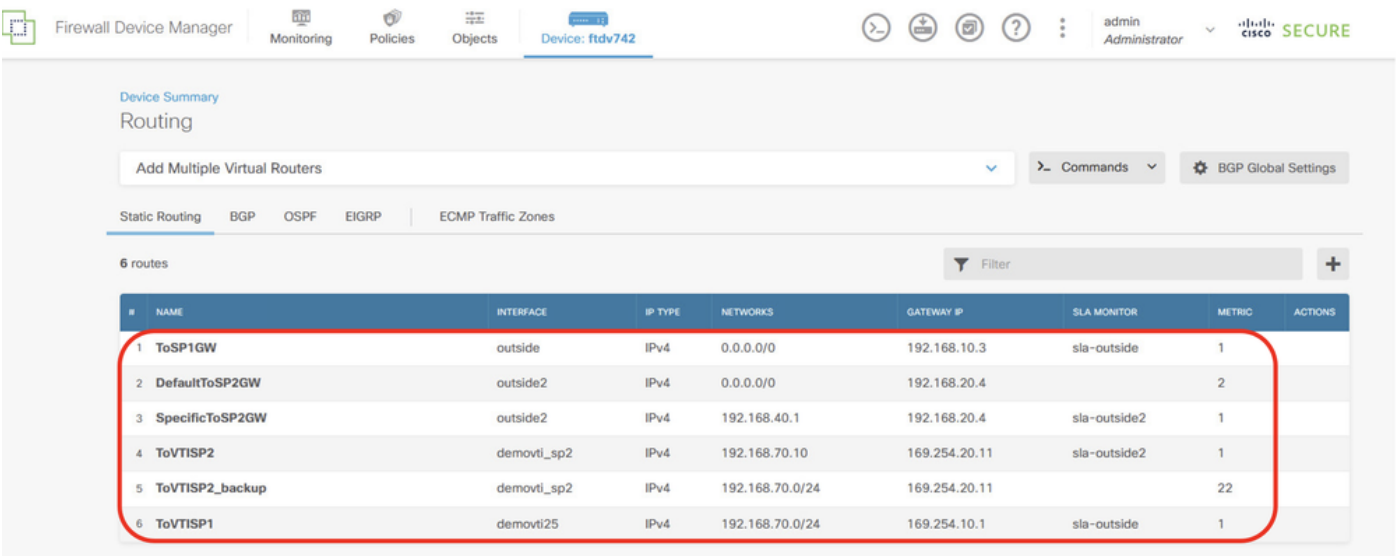
Passaggio 24. Distribuire le modifiche alla configurazione.



Sito1FTD_Deployment_Changes

Configurazione route statica FTD sito 2

Passaggio 25. Ripetere i passaggi da 22 a 24 per creare una route statica con i parametri corrispondenti per l'FTD del sito 2.



Site2FTD_Create_StaticRoute

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente. Passare alla CLI di Site1 FTD e Site2 FTD tramite console o SSH.

Sia ISP1 che ISP2 funzionano correttamente

VPN

//Site1 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:156, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local	Remote
1072332533 192.168.30.1/500	192.168.10.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK	
Life/Active Time: 86400/44895 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: 0xec031247/0xc2f3f549

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local	Remote
1045734377 192.168.40.1/500	192.168.20.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK	
Life/Active Time: 86400/77860 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: 0x47bfa607/0x82e8781d	

// Site2 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:44, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local	Remote
499259237 192.168.10.1/500	192.168.30.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK	
Life/Active Time: 86400/44985 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: 0xc2f3f549/0xec031247	

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local	Remote
477599833 192.168.20.1/500	192.168.40.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK	
Life/Active Time: 86400/77950 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: 0x82e8781d/0x47bfa607	

Percorso

// Site1 FTD:

ftdv742# show route

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 192.168.30.3 to network 0.0.0.0

```
S*      0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C       169.254.10.0 255.255.255.0 is directly connected, demovti
L       169.254.10.1 255.255.255.255 is directly connected, demovti
C       169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L       169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S       192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
C       192.168.30.0 255.255.255.0 is directly connected, outside
L       192.168.30.1 255.255.255.255 is directly connected, outside
C       192.168.40.0 255.255.255.0 is directly connected, outside2
L       192.168.40.1 255.255.255.255 is directly connected, outside2
S       192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
S       192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C       192.168.70.0 255.255.255.0 is directly connected, inside
L       192.168.70.1 255.255.255.255 is directly connected, inside
```

// Site2 FTD:

ftdv742# show route

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 192.168.10.3 to network 0.0.0.0

```
S*      0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C       169.254.10.0 255.255.255.0 is directly connected, demovti25
L       169.254.10.2 255.255.255.255 is directly connected, demovti25
C       169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L       169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C       192.168.10.0 255.255.255.0 is directly connected, outside
L       192.168.10.1 255.255.255.255 is directly connected, outside
C       192.168.20.0 255.255.255.0 is directly connected, outside2
L       192.168.20.1 255.255.255.255 is directly connected, outside2
S       192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C       192.168.50.0 255.255.255.0 is directly connected, inside
L       192.168.50.1 255.255.255.255 is directly connected, inside
S       192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
S       192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

Monitor SLA

// Site1 FTD:

ftdv742# show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 188426425
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.40.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 855903900
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.30.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.173 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30 RTTMin: 30 RTTMax: 30
NumOfRTT: 1 RTTSum: 30 RTTSum2: 900

Entry number: 855903900
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.178 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30 RTTMin: 30 RTTMax: 30
NumOfRTT: 1 RTTSum: 30 RTTSum2: 900

// Site2 FTD:

ftdv742# show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 550063734
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.20.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 609724264
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.10.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never

Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

```
ftdv742# show sla monitor operational-state
Entry number: 550063734
Modification time: 09:05:52.864 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.916 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100
```

```
Entry number: 609724264
Modification time: 09:05:52.856 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.921 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100
```

Test Ping

Scenario 1. Sito1 Client1 ping Sito2 Client1.

Prima di eseguire il ping, controllare i contatori di show crypto ipsec sa | inc interface:|encap|decap su FTD Site1.

Nell'esempio, il tunnel 1 mostra 1497 pacchetti per l'incapsulamento e 1498 pacchetti per il decapsulamento.

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
```

```
#pkts encaps: 1497, #pkts encrypt: 1497, #pkts digest: 1497
#pkts decaps: 1498, #pkts decrypt: 1498, #pkts verify: 1498
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
#pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
#pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 ping Site2 Client1 riuscito.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/97/227 ms
```

Controllare i contatori di show crypto ipsec sa | inc interface:|encap|decap nel file FTD del sito 1 dopo il completamento del ping.

Nell'esempio, il tunnel 1 mostra 1502 pacchetti per l'incapsulamento e 1503 pacchetti per la decapsulamento, con entrambi i contatori che aumentano di 5 pacchetti, in modo da soddisfare le 5 richieste echo ping. Vale a dire che i ping da Site1 Client1 a Site2 Client1 vengono instradati tramite il tunnel ISP1 1. Nel tunnel 2 non viene mostrato alcun aumento dei contatori di incapsulamento o decapsulamento, a conferma che non è usato per questo traffico.

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
#pkts encaps: 1502, #pkts encrypt: 1502, #pkts digest: 1502
#pkts decaps: 1503, #pkts decrypt: 1503, #pkts verify: 1503
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
#pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
#pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Scenario 2. Sito1 Client2 ping Sito2 Client2.

Prima di eseguire il ping, controllare i contatori di show crypto ipsec sa | inc interface:|encap|decap su FTD Site1.

Nell'esempio, il tunnel Tunnel2 mostra 21 pacchetti per l'incapsulamento e 20 pacchetti per il decapsulamento.

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
    #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
    #pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
    #pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client2: ping di Site2 Client2 completato.

```
Site1_Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/39/87 ms
```

Controllare i contatori di show crypto ipsec sa | inc interface:|encap|decap nel file FTD del sito 1 dopo il completamento del ping.

Nell'esempio, il tunnel 2 mostra 26 pacchetti per l'incapsulamento e 25 pacchetti per la decapsulamento, entrambi i contatori aumentano di 5 pacchetti, in modo da soddisfare le 5 richieste echo ping. Vale a dire che i ping da Site1 Client2 a Site2 Client2 sono instradati tramite il tunnel ISP2 2. Il tunnel 1 non mostra alcun aumento dei contatori di incapsulamento o decapsulamento, a conferma che non è usato per questo traffico.

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
    #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
    #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
    #pkts decaps: 25, #pkts decrypt: 25, #pkts verify: 25
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

L'ISP1 subisce un'interruzione mentre l'ISP2 funziona correttamente

In questo esempio, spegnere manualmente l'interfaccia E0/1 sull'ISP1 per simulare un'interruzione nell'ISP1.

```
Internet_SP1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP1(config)#
Internet_SP1(config)#interface E0/1
Internet_SP1(config-if)#shutdown
Internet_SP1(config-if)#exit
Internet_SP1(config)#
```

VPN

Il Tunnel1 è andato in tilt. Solo il tunnel 2 è attivo con SA IKEV2.

// Site1 FTD:

```
ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
  IP address 169.254.10.1, subnet mask 255.255.255.0
Tunnel Interface Information:
  Source interface: outside    IP address: 192.168.30.1
  Destination IP address: 192.168.10.1
  IPsec MTU Overhead : 0
  Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
```

```
ftdv742# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local                                Remote
1045734377 192.168.40.1/500                    192.168.20.1/500
  Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
  Life/Active Time: 86400/80266 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: 0x47bfa607/0x82e8781d
```

// Site2 FTD:

```
ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti25", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
  IP address 169.254.10.2, subnet mask 255.255.255.0
Tunnel Interface Information:
  Source interface: outside    IP address: 192.168.10.1
  Destination IP address: 192.168.30.1
  IPsec MTU Overhead : 0
  Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
```

```
ftdv742#
```

```
ftdv742# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
477599833 192.168.20.1/500 192.168.40.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/80382 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: 0x82e8781d/0x47bfa607
```

Percorso

Nella tabella di route vengono applicate le route di backup.

// Site1 FTD:

ftdv742# show route

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 192.168.40.4 to network 0.0.0.0

```
S* 0.0.0.0 0.0.0.0 [2/0] via 192.168.40.4, outside2
C 169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L 169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S 192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
C 192.168.30.0 255.255.255.0 is directly connected, outside
L 192.168.30.1 255.255.255.255 is directly connected, outside
C 192.168.40.0 255.255.255.0 is directly connected, outside2
L 192.168.40.1 255.255.255.255 is directly connected, outside2
S 192.168.50.0 255.255.255.0 [22/0] via 169.254.20.12, demovti_sp2
S 192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C 192.168.70.0 255.255.255.0 is directly connected, inside
L 192.168.70.1 255.255.255.255 is directly connected, inside
```

// Site2 FTD:

ftdv742# show route

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 192.168.10.3 to network 0.0.0.0

```
S*    0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C     169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L     169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C     192.168.10.0 255.255.255.0 is directly connected, outside
L     192.168.10.1 255.255.255.255 is directly connected, outside
C     192.168.20.0 255.255.255.0 is directly connected, outside2
L     192.168.20.1 255.255.255.255 is directly connected, outside2
S     192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C     192.168.50.0 255.255.255.0 is directly connected, inside
L     192.168.50.1 255.255.255.255 is directly connected, inside
S     192.168.70.0 255.255.255.0 [22/0] via 169.254.20.11, demovti_sp2
S     192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

Monitor SLA

Sul FTD del sito 1, il monitor SLA visualizza il timeout numero voce 855903900 (l'indirizzo di destinazione è 192.168.30.3) per ISP1.

// Site1 FTD:

```
ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.131 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 100
Latest operation start time: 14:22:05.132 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 100    RTTMin: 100    RTTMax: 100
NumOfRTT: 1    RTTSum: 100    RTTSum2: 10000
```

```
Entry number: 855903900
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:22:05.134 UTC Thu Aug 15 2024
Latest operation return code: Timeout
```

RTT Values:
RTTAvg: 0 RTTMin: 0 RTTMax: 0
NumOfRTT: 0 RTTSum: 0 RTTSum2: 0

ftdv742# show track

Track 1

Response Time Reporter 855903900 reachability
Reachability is Down
7 changes, last change 00:11:03
Latest operation return code: Timeout
Tracked by:
STATIC-IP-ROUTING 0

Track 2

Response Time Reporter 188426425 reachability
Reachability is Up
4 changes, last change 13:15:11
Latest operation return code: OK
Latest RTT (milliseconds) 140
Tracked by:
STATIC-IP-ROUTING 0

Test Ping

Prima di eseguire il ping, controllare i contatori di show crypto ipsec sa | inc interface:|encap|decap su FTD Site1.

Nell'esempio, il tunnel 2 mostra 36 pacchetti per l'incapsulamento e 35 pacchetti per la decapsulamento.

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
    #pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
    #pkts decaps: 35, #pkts decrypt: 35, #pkts verify: 35
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 ping Site2 Client1 riuscito.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 22/133/253 ms
```

Site1 Client2: ping di Site2 Client2 completato.

```
Site1_Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 34/56/87 ms
```

Controllare i contatori di show crypto ipsec sa | inc interface:|encap|decap in Site1 FTD dopo il completamento del ping.

Nell'esempio, il tunnel 2 mostra 46 pacchetti per l'incapsulamento e 45 pacchetti per la decapsulamento, con entrambi i contatori che aumentano di 10 pacchetti, in base alle 10 richieste echo ping. Vale a dire che i pacchetti ping sono indirizzati tramite ISP2 Tunnel 2.

```
// Site1 FTD:
```

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
    #pkts encaps: 46, #pkts encrypt: 46, #pkts digest: 46
    #pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

L'ISP2 subisce un'interruzione mentre l'ISP1 funziona correttamente

In questo esempio, spegnere manualmente l'interfaccia E0/1 sull'ISP2 per simulare che l'ISP2 abbia subito un'interruzione.

```
Internet_SP2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Internet_SP2(config)#
Internet_SP2(config)#int e0/1
Internet_SP2(config-if)#shutdown
Internet_SP2(config-if)#^Z
Internet_SP2#
```

VPN

Il Tunnel2 si è interrotto. Solo il tunnel 1 è attivo con la SA IKEV2.

```
// Site1 FTD:
```

```
ftdv742# show interface tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
  IP address 169.254.20.11, subnet mask 255.255.255.0
  Tunnel Interface Information:
```

```
Source interface: outside2    IP address: 192.168.40.1
Destination IP address: 192.168.20.1
IPsec MTU Overhead : 0
Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
```

```
ftdv742# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:159, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
1375077093 192.168.30.1/500 192.168.10.1/500
  Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
  Life/Active Time: 86400/349 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: 0x40f407b4/0x26598bcc
```

// Site2 FTD:

```
ftdv742# show int tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
  IP address 169.254.20.12, subnet mask 255.255.255.0
Tunnel Interface Information:
  Source interface: outside2    IP address: 192.168.20.1
  Destination IP address: 192.168.40.1
  IPsec MTU Overhead : 0
  Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
```

```
ftdv742# show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:165, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
1025640731 192.168.10.1/500 192.168.30.1/500
  Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
  Life/Active Time: 86400/379 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: 0x26598bcc/0x40f407b4
```

Percorso

Nella tabella di route, la route correlata all'ISP2 è scomparsa per il traffico PBR.

// Site1 FTD:

```
ftdv742# show route
```

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 192.168.30.3 to network 0.0.0.0

```
S*      0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C       169.254.10.0 255.255.255.0 is directly connected, demovti
L       169.254.10.1 255.255.255.255 is directly connected, demovti
C       192.168.30.0 255.255.255.0 is directly connected, outside
L       192.168.30.1 255.255.255.255 is directly connected, outside
C       192.168.40.0 255.255.255.0 is directly connected, outside2
L       192.168.40.1 255.255.255.255 is directly connected, outside2
S       192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
C       192.168.70.0 255.255.255.0 is directly connected, inside
L       192.168.70.1 255.255.255.255 is directly connected, inside
```

// Site2 FTD:

ftdv742# show route

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 192.168.10.3 to network 0.0.0.0

```
S*      0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C       169.254.10.0 255.255.255.0 is directly connected, demovti25
L       169.254.10.2 255.255.255.255 is directly connected, demovti25
C       192.168.10.0 255.255.255.0 is directly connected, outside
L       192.168.10.1 255.255.255.255 is directly connected, outside
C       192.168.20.0 255.255.255.0 is directly connected, outside2
L       192.168.20.1 255.255.255.255 is directly connected, outside2
S       192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C       192.168.50.0 255.255.255.0 is directly connected, inside
L       192.168.50.1 255.255.255.255 is directly connected, inside
S       192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
```

Monitor SLA

Nel FTD del sito 1, il monitor SLA visualizza il numero di voce 188426425 timeout (l'indirizzo di destinazione è 192.168.40.4) per ISP2.

// Site1 FTD:

```
ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:52:05.174 UTC Thu Aug 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0
```

```
Entry number: 855903900
Modification time: 08:37:05.135 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 10
Latest operation start time: 14:52:05.177 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 10    RTTMin: 10    RTTMax: 10
NumOfRTT: 1    RTTSum: 10    RTTSum2: 100
```

```
ftdv742# show track
```

```
Track 1
```

```
Response Time Reporter 855903900 reachability
Reachability is Up
8 changes, last change 00:14:37
Latest operation return code: OK
Latest RTT (millisecs) 60
Tracked by:
  STATIC-IP-ROUTING 0
```

```
Track 2
```

```
Response Time Reporter 188426425 reachability
Reachability is Down
5 changes, last change 00:09:30
Latest operation return code: Timeout
Tracked by:
  STATIC-IP-ROUTING 0
```

Test Ping

Prima di eseguire il ping, controllare i contatori di show crypto ipsec sa | inc interface:|encap|decap

su FTD Site1.

Nell'esempio, il tunnel 1 mostra 74 pacchetti per l'incapsulamento e 73 pacchetti per il decapsulamento.

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 74, #pkts encrypt: 74, #pkts digest: 74
    #pkts decaps: 73, #pkts decrypt: 73, #pkts verify: 73
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 ping Site2 Client1 riuscito.

```
Site1_Client1#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/158/255 ms
```

Site1 Client2: ping di Site2 Client2 completato.

```
Site1_Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/58/143 ms
```

Controllare i contatori di show crypto ipsec sa | inc interface:|encap|decap in Site1 FTD dopo il completamento del ping.

Nell'esempio, il tunnel 1 mostra 84 pacchetti per l'incapsulamento e 83 pacchetti per la decapsulamento, con entrambi i contatori che aumentano di 10 pacchetti, in base alle 10 richieste echo ping. Vale a dire che i pacchetti ping sono indirizzati tramite ISP1 Tunnel 1.

// Site1 FTD:

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 84, #pkts encrypt: 84, #pkts digest: 84
    #pkts decaps: 83, #pkts decrypt: 83, #pkts verify: 83
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Risoluzione dei problemi

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

È possibile usare questi comandi di debug per risolvere i problemi della sezione VPN.

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug vti 255
```

È possibile utilizzare questi comandi di debug per risolvere i problemi relativi alla sezione PBR.

```
debug policy-route
```

È possibile utilizzare questi comandi di debug per risolvere i problemi relativi alla sezione Monitor SLA.

```
ftdv742# debug sla monitor ?
  error  Output IP SLA Monitor Error Messages
  trace  Output IP SLA Monitor Trace Messages
```

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).