

Configurazione di BGP over Route-Based VPN su FTD Gestito da FDM

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni su VPN](#)

[Configurazioni su BGP](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive la configurazione di BGP su VPN da sito a sito basata su route su FTDv gestito da FirePower Device Manager (FDM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di VPN
- Configurazioni BGP su FTDv
- Esperienza con FDM

Componenti usati

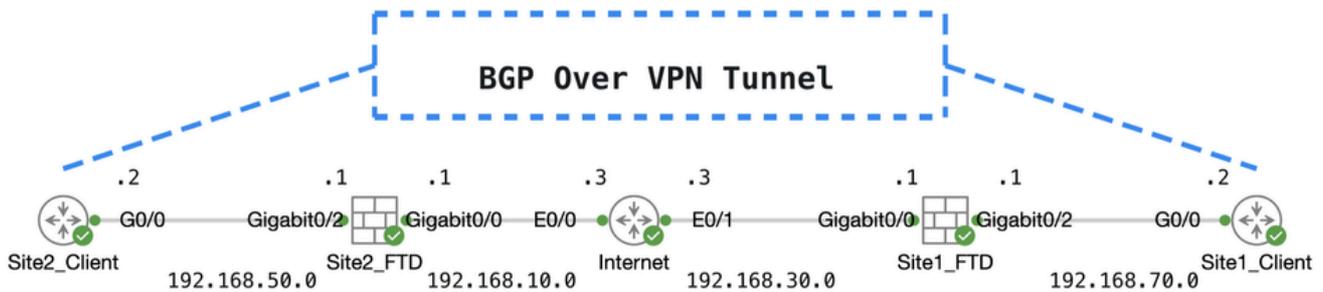
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 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.

Configurazione

Esempio di rete



Topografico

Configurazioni su VPN

Passaggio 1. Assicurarsi che l'interconnettività IP tra i nodi sia pronta e stabile. La licenza smart su FDM è stata registrata con lo smart account.

Passaggio 2. Il gateway del client Site1 è configurato con l'indirizzo IP interno di Site1 FTD (192.168.70.1). Il gateway del client Site2 è configurato con l'indirizzo IP interno di Site2 FTD (192.168.50.1). Inoltre, accertarsi che il percorso predefinito su entrambi gli FTD sia configurato correttamente dopo l'inizializzazione di FDM.

Accedere alla GUI di ciascun FDM. Passare a `Device > Routing`. Fare clic su `.View Configuration`. Fare clic sulla `Static Routing` scheda per verificare la route statica predefinita.

The screenshot shows the Firewall Device Manager GUI for device ftdv742. The 'Routing' section is active, and the 'Static Routing' tab is selected. A table displays the static routing configuration:

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	StaticRoute_IPv4	outside	IPv4	0.0.0.0/0	192.168.30.3		1	

Sito1_FTD_Gateway

Device Summary
Routing

Add Multiple Virtual Routers

Static Routing | BGP | OSPF | EIGRP | ECMP Traffic Zones

1 route

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	StaticRoute_IPv4	outside	IPv4	0.0.0.0/0	192.168.10.3		1	

Sito2_FTD_Gateway

Passaggio 3. Configurare la VPN da sito a sito basata sulla route. In questo esempio, configurare innanzitutto l'FTD Site1.

Passaggio 3.1. Accedere alla GUI FDM di Site1 FTD. Crea un nuovo oggetto di rete per la rete interna dell'FTD del sito 1. Passare a **Objects > Networks** e fare clic sul pulsante +.

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: ftdv742

Object Types

- Networks**
- Ports

Network Objects and Groups

9 objects

Filter

Preset filters: System defined, User defined

Crea_Oggetto_Rete

Passaggio 3.2. Fornire le informazioni necessarie. Fare clic sul OK pulsante.

- Nome: inside_192.168.70.0
- Tipo: rete
- Rete: 192.168.70.0/24

Add Network Object



Name

inside_192.168.70.0

Description

Type



Network



Host



FQDN



Range

Network

192.168.70.0/24

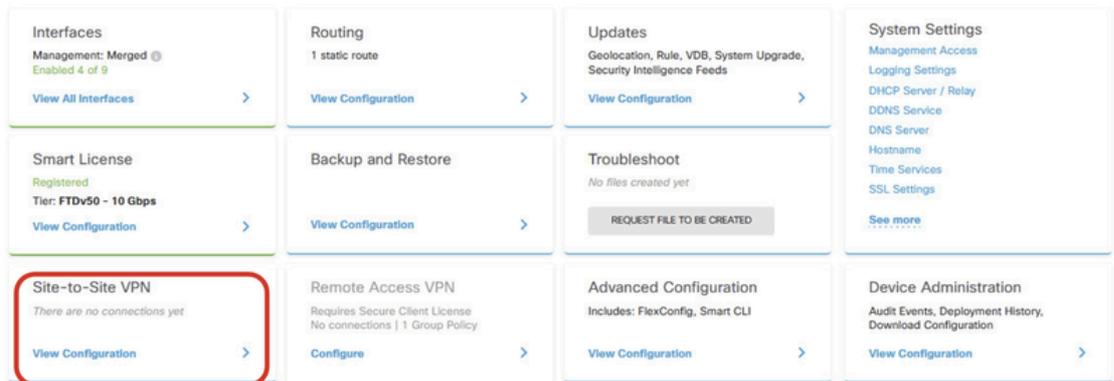
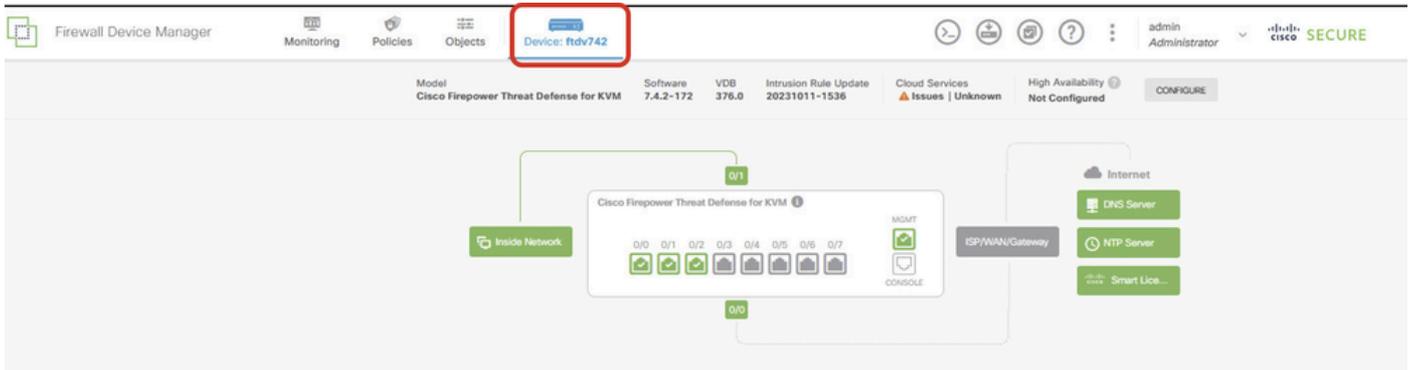
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

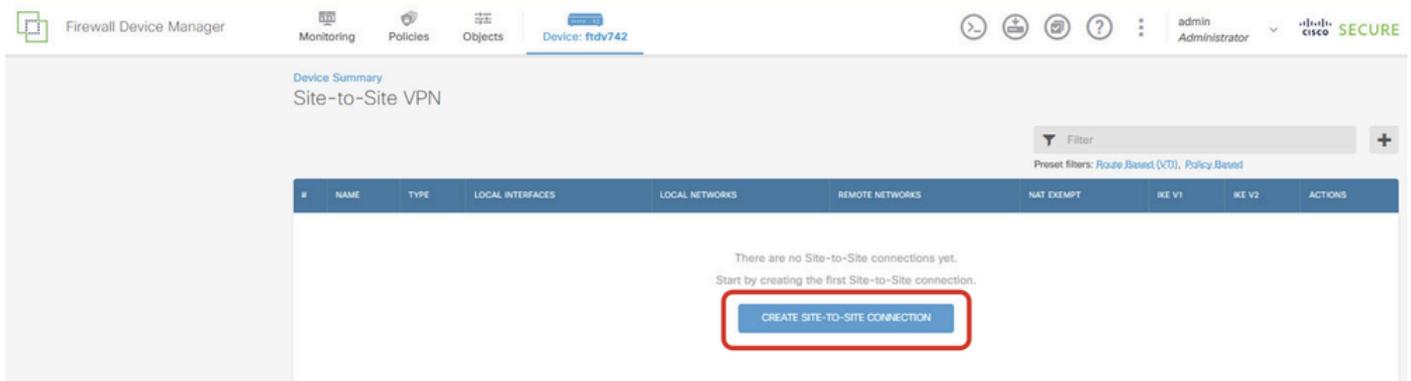
Sito1_Interno_Rete

Passaggio 3.3. Passare a **Device > Site-to-Site VPN** . Fare clic su **.View Configuration**



Visualizza VPN da sito a sito

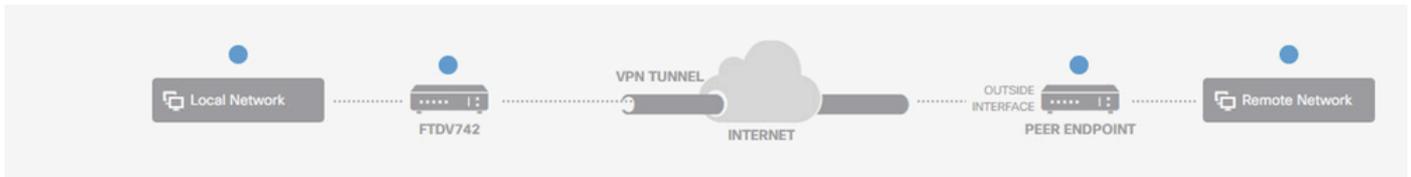
Passaggio 3.4. Iniziare a creare una nuova VPN da sito a sito. Fare clic su **CREATE SITE-TO-SITE CONNECTION**



Create_Site-to-Site_Connection

Passaggio 3.5. Fornire le informazioni necessarie.

- Nome profilo connessione: Demo_S2S
- Tipo: basato su route (VTI)
- Interfaccia di accesso VPN locale: fare clic sull'elenco a discesa, quindi fare clic su **Create new Virtual Tunnel Interface**.



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 Please select Filter Nothing found Create new Virtual Tunnel Interface	Remote IP Address

NEXT

Creazione guidata VPN_in_VPN

Passaggio 3.6. Fornire le informazioni necessarie per creare una nuova VTI. Fare clic sul pulsante OK.

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

Name Status

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

Description

Tunnel ID 0 - 10413 Tunnel Source

IP Address and Subnet Mask /

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

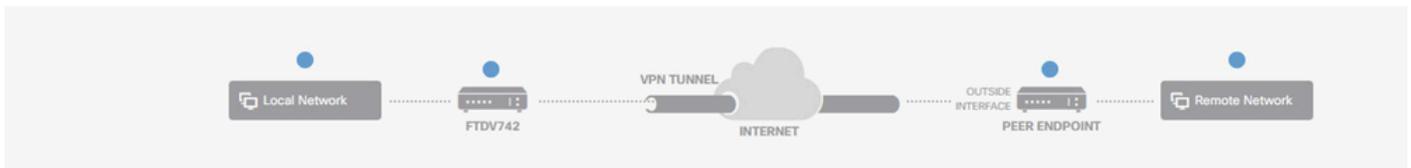
Crea_dettagli_VTI

Passaggio 3.7. Continuare a fornire le informazioni necessarie. Fare clic sul pulsante NEXT.

- Interfaccia di accesso VPN locale: rimozione (creata nel passaggio 3.6.1)
- Indirizzo IP remoto: 192.168.10.1

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

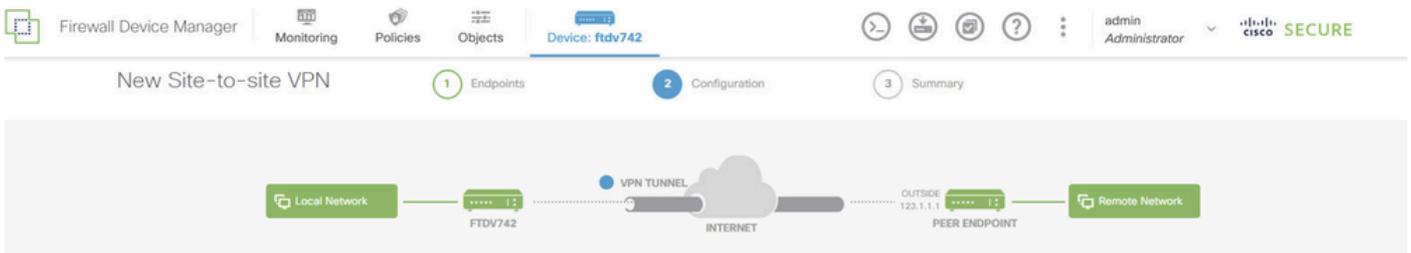
Type: Route Based (VTI) Policy Based

Sites Configuration

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

Passaggio 1 di VPN_Wizard_Endpoints

Passaggio 3.8. Passare al criterio IKE. 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

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

IPSec Proposal

None selected

Modifica_Criterio_IKE

Passaggio 3.9. Per il criterio IKE, è possibile utilizzare un criterio predefinito o 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 sul pulsante OK.

- Nome: AES256_DH14_SHA256_SHA256
- Crittografia: AES, AES256
- Gruppo DH: 14
- Hash integrità: SHA, SHA256
- Hash PRF: SHA, SHA256
- Durata: 86400 (predefinita)

The image shows two screenshots of a network configuration interface. The left screenshot displays a list of IKE policies with a filter bar. The 'AES-SHA-SHA' policy is selected and highlighted with a red box. Below the list is a 'Create New IKE Policy' button, also highlighted with a red box. The right screenshot shows the 'Add IKE v2 Policy' configuration dialog. The 'Name' field is set to 'AES256_DH14_SHA256_SHA256'. The 'Encryption' field is set to 'AES' and 'AES256'. The 'Diffie-Hellman Group' is set to '14'. The 'Integrity Hash' field is set to 'SHA' and 'SHA256'. The 'Pseudo Random Function (PRF) Hash' field is set to 'SHA' and 'SHA256'. The 'Lifetime (seconds)' is set to '86400'. The 'State' toggle is turned on. The 'OK' button at the bottom right is highlighted with a red box. A red arrow points from the 'Create New IKE Policy' button in the left screenshot to the 'Add IKE v2 Policy' dialog in the right screenshot.

Aggiungi_Nuovo_Criterio_IKE

Filter

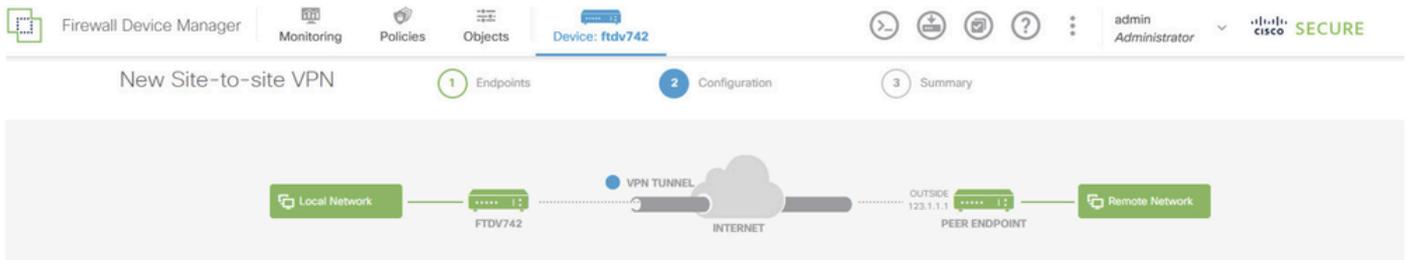
<input type="checkbox"/>	AES-GCM-NULL-SHA	i
<input checked="" type="checkbox"/>	AES-SHA-SHA	i
<input type="checkbox"/>	DES-SHA-SHA	i
<input checked="" type="checkbox"/>	AES256_DH14_SHA256_SHA256	i

Create New IKE Policy

OK

Abilita_Nuovo_Criterio_IKE

Passaggio 3.10. 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

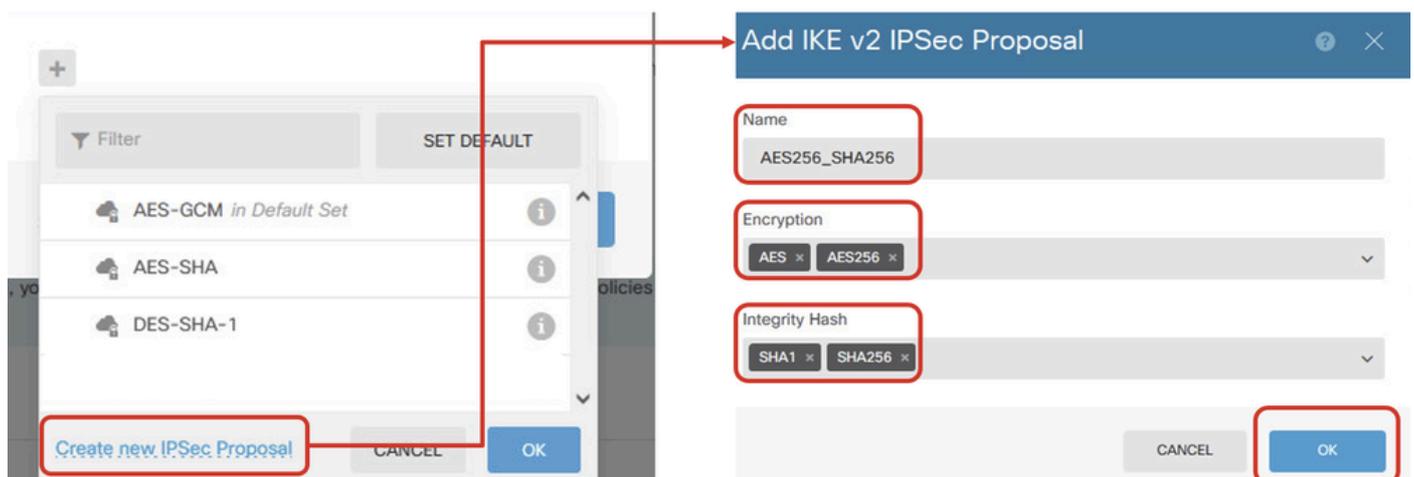
IPSec Proposal

None selected !

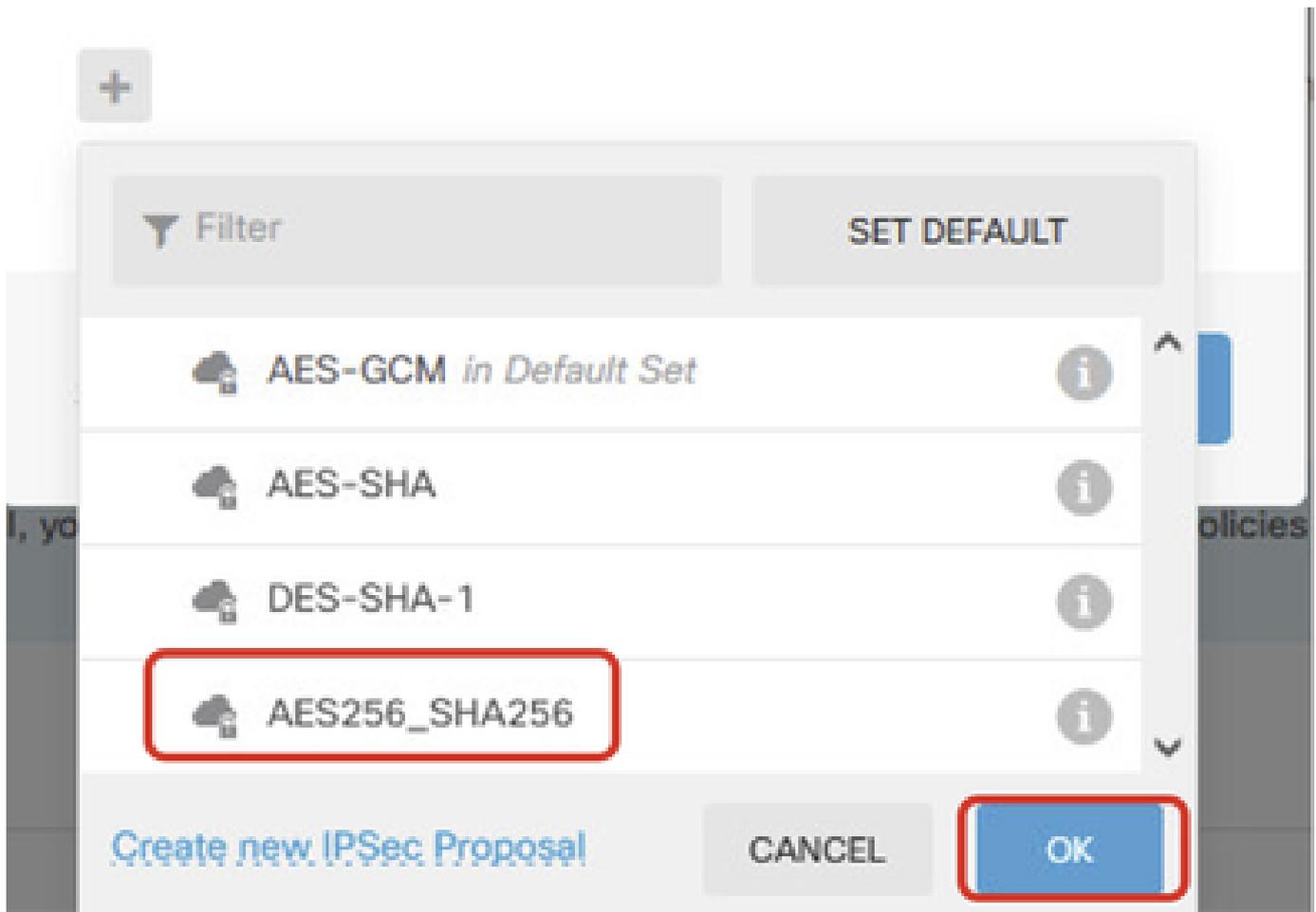
Modifica_Proposta_IKE

Passaggio 3.11. Per la 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. Fornire le informazioni necessarie. Per salvare, fare clic sul pulsante OK.

- Nome: AES256_SHA256
- Crittografia: AES, AES256
- Hash di integrità: SHA1, SHA256



Aggiungi_nuova_proposta_IPsec



Abilita_Nuova_proposta_IPSec

Passaggio 3.12. Configurare la chiave già condivisa. Fare clic sul pulsante NEXT.

Prendere nota di questa chiave già condivisa e configurarla in un secondo momento nell'FTD del sito 2.

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

FTDV742 | INTERNET | PEER ENDPOINT

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

IPSec Proposal
Custom set selected

Authentication Type
 Pre-shared Manual Key Certificate

Local Pre-shared Key

Remote Peer Pre-shared Key

Configura_Chiave_già_condivisa

Passaggio 3.13. 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

VPN_Wizard_Complete

Passaggio 3.14. Creare una regola di controllo dell'accesso per consentire il passaggio del traffico attraverso l'FTD. In questo esempio, consentire tutti per scopi dimostrativi. Modificare i criteri in base alle esigenze effettive.

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes "Firewall Device Manager", "Monitoring", "Policies", "Objects", and "Device: ftdv742". The breadcrumb trail is: "Security Policies" > "Access Control". A notification icon with the number "1" is visible. Below the breadcrumb, there is a "Filter" input field and a "1 rule" indicator. The main table displays the configuration for the "Demo_allow" rule:

#	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		

At the bottom, the "Default Action" is set to "Access Control" with a "Block" button and a dropdown menu.

Passaggio 3.15. (Facoltativo) Configurare la regola di esenzione NAT per il traffico client su FTD se per il client è configurato NAT dinamico per l'accesso a Internet. Nell'esempio, non è necessario configurare una regola di esenzione NAT in quanto su ciascun FTD non è configurato alcun NAT dinamico.

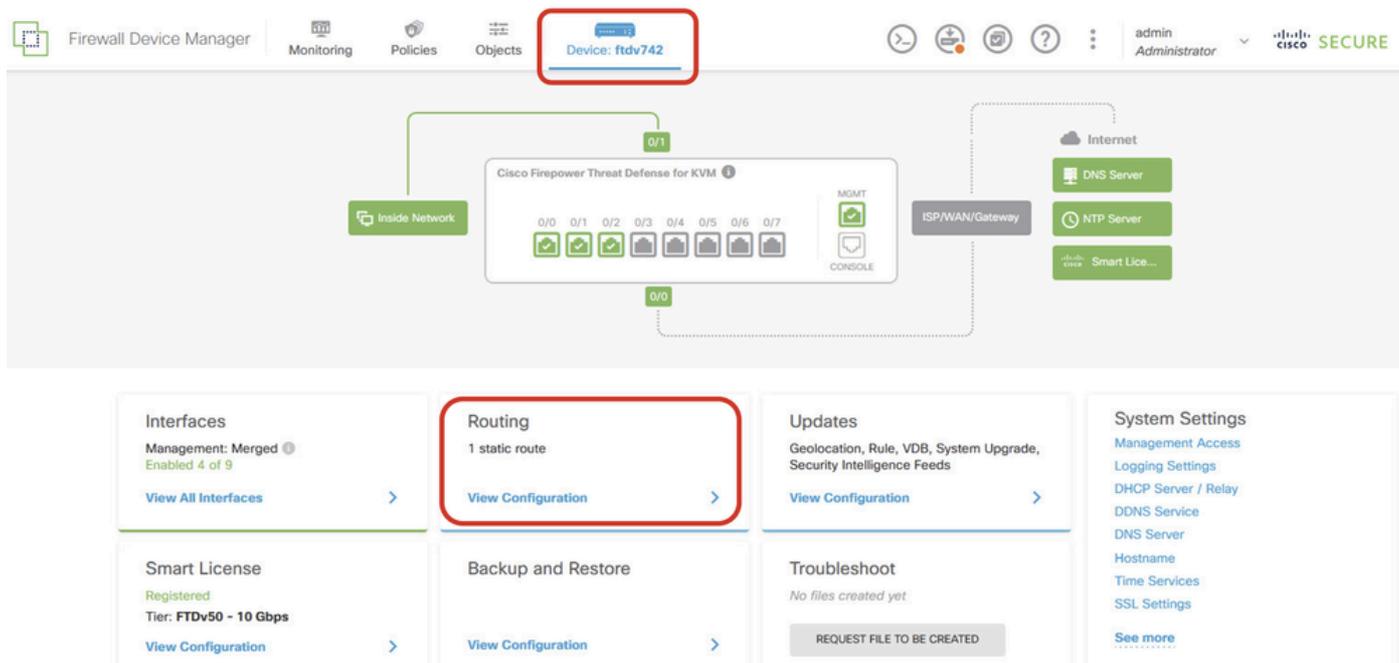
Passaggio 3.16. Distribuire le modifiche alla configurazione.



Distribuisci_configurazione_VPN

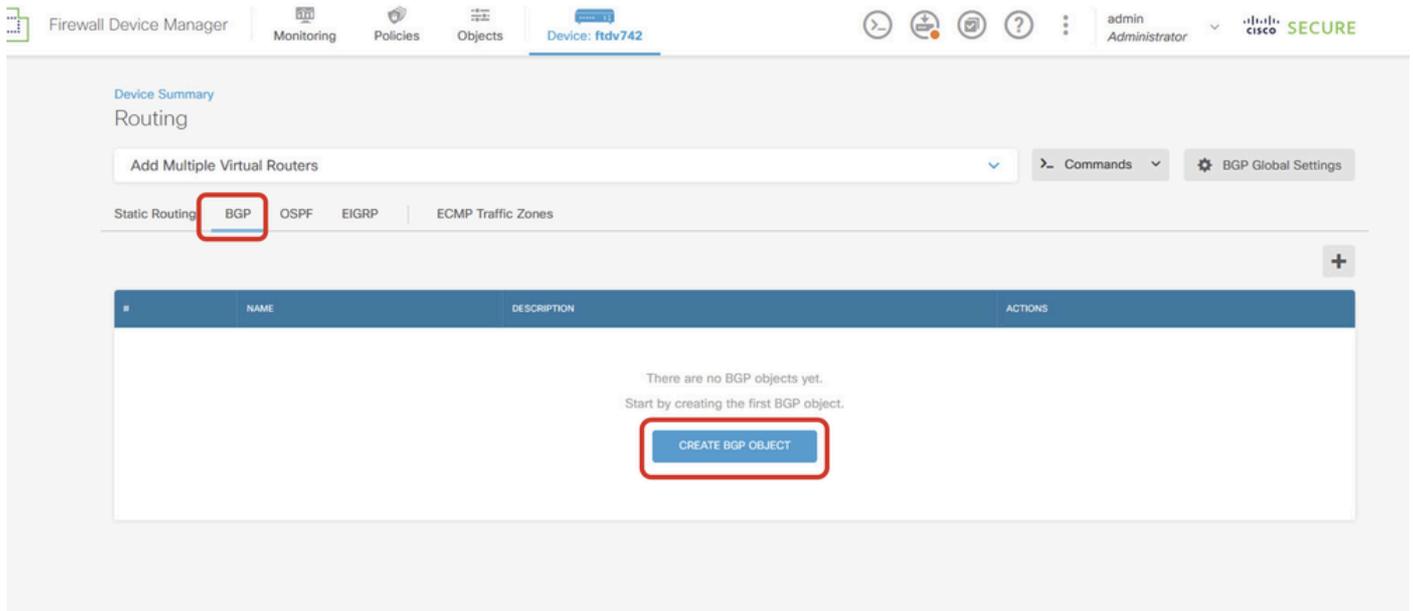
Configurazioni su BGP

Passaggio 4. Selezionare Periferica > Instradamento. Fare clic su Visualizza configurazione.



Configurazione_instradamento_vista

Passaggio 5. Fare clic sulla scheda BGP, quindi su CREATE BGP OBJECT.



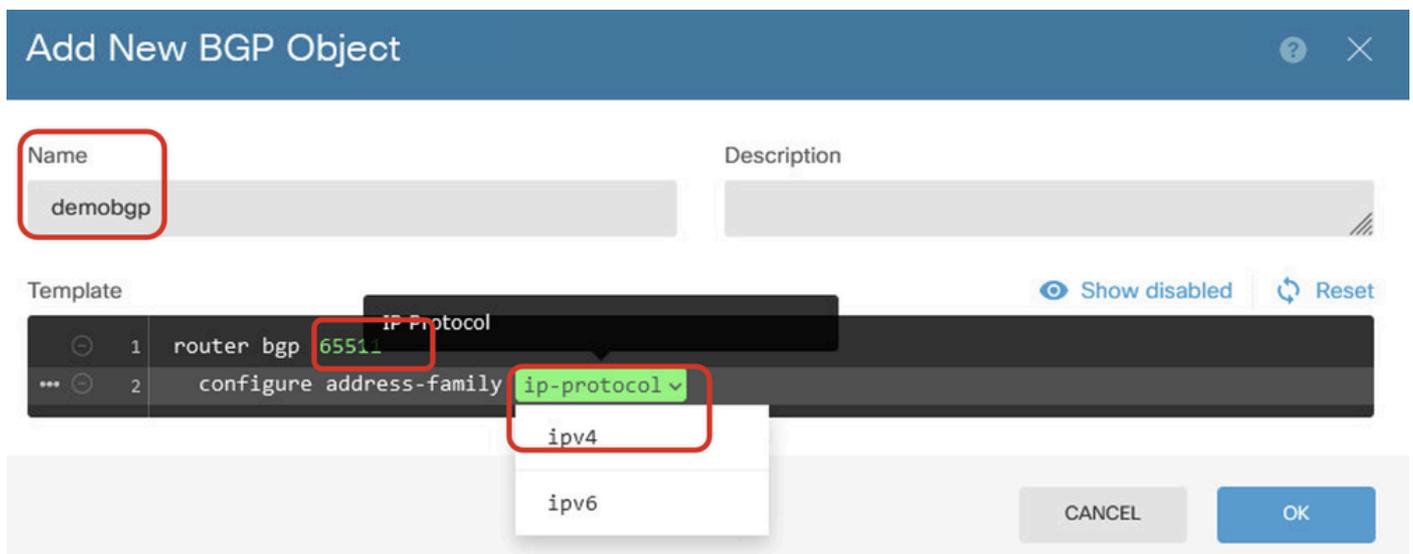
Crea_BGP_Object

Passaggio 6. Specificare il nome dell'oggetto. Passare a Modello e configurare. Fare clic sul pulsante OK per salvare.

Nome: demobgp

Riga 1: configurare il numero AS. Fare clic su come numero. Numero AS locale di input manuale. In questo esempio, il numero AS 65511 per Site1 FTD.

Riga 2: configurare il protocollo IP. Fare clic su ip-protocol. Selezionare ipv4.



Create_BGP_Object_ASNumber_Protocol

Riga 4: configurare altre impostazioni. Fare clic su Impostazioni, scegliere Generale e quindi fare clic su Mostra disattivato.

Add New BGP Object

Name: demobgp

Description:

Template: Show disabled Reset

```

1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4     configure address-family ipv4 settings

```

Address Family IPv4 Settings

- general
- advanced

CANCEL OK

Impostazione Create_BGP_Object_Address

Riga 6: fare clic sull'icona + per abilitare la linea per configurare la rete BGP. Fare clic su network-object. Potete visualizzare gli oggetti disponibili esistenti e sceglierne uno. In questo esempio, scegliere il nome dell'oggetto inside_192.168.70.0 (creato al punto 3.2).

Add New BGP Object

Name: demobgp

Description:

Template: Hide disabled Reset

```

1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4     configure address-family ipv4 general
5     distance bgp 20 200 200
6     network network-object
7     network network-object route-map map-tag
8     bgp inject-map inject-map exist-map exist-map options
9     configure aggregate-address map-type
10    configure filter-rules direction
11    configure neighbor neighbor-address remote-as as-number config-options
12    configure ipv4 redistribution protocol identifier none
13    bgp router-id router-id

```

Create_BGP_Object_Add_Network

Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4     configure address-family ipv4 general
5     distance bgp 20 200 200
6   network
7   network
8   bgp inje
9   configur
10  configur
11  configur
12  configur
13  bgp router-i
```

IPV4 Network address

- OutsidelPv4DefaultRoute Network
- OutsidelPv4Gateway Host
- any-ipv4 Network
- any-ipv6 Network
- inside_192.168.70.0 Network

inside_192.168.70.0

Create_BGP_Object_Add_Network2

Riga 11: fare clic sull'icona + per abilitare la linea a configurare le informazioni relative ai nodi adiacenti BGP. Fare clic su neighbor-address e immettere manualmente l'indirizzo adiacente BGP del peer. Nell'esempio, questo valore è 169.254.10.2 (indirizzo IP VTI di FTD Sito2). Fare clic su as-number e immettere manualmente il numero AS del peer. In questo esempio, 65510 è per Site2 FTD. Fare clic su config-options (opzioni di configurazione), quindi selezionare properties (proprietà).

Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6         network inside_192.168.70.0
7         network network-object route-map map-tag
8         bgp inject-map inject-map exist-map exist-map options
9         configure aggregate-address map-type
10        configure filter-rules direction
11        configure neighbor 169.254.10.2 remote-as 65510 config-options
12        configure ipv4 redistribution protocol identifier
13        bgp router-id router-id
```

Select Configuration Option

properties

Create_BGP_Object_NeighborSetting

Riga 14: fare clic sull'icona + per abilitare la linea a configurare alcune proprietà della risorsa adiacente. Fare clic su activate-options e selezionare properties (proprietà).

Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6         network inside_192.168.70.0
7         network network-object route-map map-tag
8         bgp inject-map inject-map exist-map exist-map options
9         configure aggregate-address map-type
10        configure filter-rules direction
11        configure neighbor 169.254.10.2 remote-as 65510 properties
12          neighbor 169.254.10.2 remote-as 65510
13          configure neighbor 169.254.10.2 remote-as setting
14          configure neighbor 169.254.10.2 activate activate-options
15          configure ipv4 redistribution protocol id
16        bgp router-id router-id
```

Create_BGP_Object_NeighborSetting_Properties

Riga 13: fare clic sull'icona + per abilitare la linea per la visualizzazione delle opzioni avanzate. Fare clic su Settings (Impostazioni), quindi selezionare Advanced (Avanzate).

Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6         network inside_192.168.70.0
7         network network-object route-map map-tag
8         bgp inject-map inject-map exist-map exist-map options
9         configure aggregate-address map-type
10        configure filter-rules direction
11        configure neighbor 169.254.10.2 remote-as 65511 properties
12        neighbor 169.254.10.2 remote-as 65511
13        configure neighbor 169.254.10.2 remote-as 65511 settings
14        configure neighbor 169.254.10.2 activate
15        neighbor 169.254.10.2 activate
16        configure neighbor 169.254.10.2 activate
17        configure ipv4 redistribution protocol identifier
18        bgp router-id router-id
```

Select Neighbor Settings

settings

general

advanced

migration

ha-mode

CANCEL

OK

Create_BGP_Object_NeighborSetting_Properties_Advanced

Riga 18: Fare clic su options (Opzioni), quindi selezionare disable (Disattiva) per disabilitare il rilevamento dell'MTU del percorso.

Add New BGP Object



Name

Description

demobgp

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6         network inside_192.168.70.0
7         network network-object route-map map-tag
8         bgp inject-map inject-map exist-map exist-map options
9         configure aggregate-address map-type
10        configure filter-rules direction
11        configure neighbor 169.254.10.2 remote-as 65510 properties
12        neighbor 169.254.10.2 remote-as 65510
13        configure neighbor 169.254.10.2 remote-as advanced
14        neighbor 169.254.10.2 password secret
15        configure neighbor 169.254.10.2 hops options
16        neighbor 169.254.10.2 version version-number options (optional)
17        neighbor 169.254.10.2 transport connection-mode options
18        neighbor 169.254.10.2 transport path-mtu-discovery options
19        configure neighbor 169.254.10.2 activate properties
20        neighbor 169.254.10.2 activate
21        configure neighbor 169.254.10.2 activate settings
22        configure ipv4 redistribution protocol identifier none
23        bgp router-id router-id
```

Create_BGP_Object_NeighborSetting_Properties_Advanced_PMD

Riga 14, 15, 16, 17: fare clic sul pulsante - per disattivare le linee. Fare quindi clic sul pulsante OK per salvare l'oggetto BGP.

Add New BGP Object



Name

demobgp

Description

Template

Hide disabled

Reset

```
1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6       network inside_192.168.70.0
7       network network-object route-map map-tag
8     bgp inject-map inject-map exist-map exist-map options
9     configure aggregate-address map-type
10    configure filter-rules direction
11    configure neighbor 169.254.10.2 remote-as 65510 properties
12    neighbor 169.254.10.2 remote-as 65510
13    configure neighbor 169.254.10.2 remote-as advanced
14    neighbor 169.254.10.2 password secret
15    configure neighbor 169.254.10.2 hops options
16    neighbor 169.254.10.2 version version-number
17    neighbor 169.254.10.2 transport connection-mode options
18    neighbor 169.254.10.2 transport path-mtu-discovery disable
19    configure neighbor 169.254.10.2 activate properties
20    neighbor 169.254.10.2 activate
21    configure neighbor 169.254.10.2 activate settings
22    configure ipv4 redistribution protocol identifier none
23  bgp router-id router-id
```

CANCEL

OK

Create_BGP_Object_DisableLines

Questa è una panoramica dell'impostazione BGP in questo esempio. È possibile configurare le altre impostazioni BGP in base alle esigenze effettive.

Name	Description
demobgp	

Template

Hide disabled

Reset

```

1 router bgp 65511
2   configure address-family ipv4
3     address-family ipv4 unicast
4       configure address-family ipv4 general
5         distance bgp 20 200 200
6       network inside_192.168.70.0
7       network network-object route-map map-tag
8       bgp inject-map inject-map exist-map exist-map options
9       configure aggregate-address map-type
10      configure filter-rules direction
11      configure neighbor 169.254.10.2 remote-as 65510 properties
12      neighbor 169.254.10.2 remote-as 65510
13      configure neighbor 169.254.10.2 remote-as advanced
14      neighbor 169.254.10.2 password secret
15      configure neighbor 169.254.10.2 hops options
16      neighbor 169.254.10.2 version version-number
17      neighbor 169.254.10.2 transport connection-mode options
18      neighbor 169.254.10.2 transport path-mtu-discovery disable
19      configure neighbor 169.254.10.2 activate properties
20      neighbor 169.254.10.2 activate
21      configure neighbor 169.254.10.2 activate settings
22      configure ipv4 redistribution protocol identifier none
23      bgp router-id router-id
  
```

CANCEL

OK

Create_BGP_Object_Final_Overview

Passaggio 7. Distribuire le modifiche alla configurazione BGP.

Firewall Device Manager

Monitoring Policies Objects Device: ftdv742

admin Administrator

CISCO SECURE

Device Summary

Routing

Add Multiple Virtual Routers

Commands BGP Global Settings

Static Routing BGP OSPF EIGRP ECMP Traffic Zones

1 object

#	NAME	DESCRIPTION	ACTIONS
1	demobgp		

Configurazione_BGP_Distribuzione

Passaggio 8. Ora la configurazione per Site1 FTD è completata.

Per configurare la VPN FTD del sito 2 e il BGP, ripetere i passaggi da 3 a 7 con i parametri corrispondenti di FTD del sito 2.

Panoramica della configurazione di Site1 FTD e Site2 FTD nella CLI.

FTD Sito1	FTD Sito2
<p>NGFW versione 7.4.2</p> <p>interfaccia Gigabit Ethernet0/0 nameif esterno manuale cat propagazione di sgt preserve-untag criterio statico sgt disabilitato attendibile livello di protezione 0 indirizzo ip 192.168.30.1 255.255.255.0</p> <p>interfaccia Gigabit Ethernet0/2 nameif inside livello di protezione 0 indirizzo ip 192.168.70.1 255.255.255.0</p> <p>interface Tunnel1 nameif demovti indirizzo ip 169.254.10.1 255.255.255.0 interfaccia di origine tunnel esterna destinazione del tunnel 192.168.10.1 modalità tunnel ipsec ipv4 protezione tunnel profilo ipsec ipsec_profile e4084d322d</p> <p>rete di oggetti OutsideIPv4Gateway host 192.168.30.3 rete di oggetti inside_192.168.70.0 subnet 192.168.70.0 255.255.255.0</p> <p>access-group globale NGFW_ONBOX_ACL access-list NGFW_ONBOX_ACL note rule-id 268435457: CRITERI DI ACCESSO: NGFW_Access_Policy access-list NGFW_ONBOX_ACL note rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object- group acSvcg-268435457 ifc all'interno di qualsiasi ifc all'esterno di qualsiasi registro eventi rule-id 268435457 entrambi access-list NGFW_ONBOX_ACL note rule-id 268435458: CRITERI DI ACCESSO: NGFW_Access_Policy</p>	<p>NGFW versione 7.4.2</p> <p>interfaccia Gigabit Ethernet0/0 nameif esterno manuale cat propagazione di sgt preserve-untag criterio statico sgt disabilitato attendibile livello di protezione 0 indirizzo ip 192.168.10.1 255.255.255.0</p> <p>interfaccia Gigabit Ethernet0/2 nameif inside livello di protezione 0 indirizzo ip 192.168.50.1 255.255.255.0</p> <p>interface Tunnel1 nameif demovti25 indirizzo ip 169.254.10.2 255.255.255.0 interfaccia di origine tunnel esterna destinazione del tunnel 192.168.30.1 modalità tunnel ipsec ipv4 protezione tunnel profilo ipsec ipsec_profile e4084d322d</p> <p>rete di oggetti OutsideIPv4Gateway host 192.168.10.3 rete di oggetti inside_192.168.50.0 subnet 192.168.50.0 255.255.255.0</p> <p>access-group globale NGFW_ONBOX_ACL access-list NGFW_ONBOX_ACL note rule-id 268435457: CRITERI DI ACCESSO: NGFW_Access_Policy access-list NGFW_ONBOX_ACL note rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL advanced trust object- group acSvcg-268435457 ifc all'interno di qualsiasi ifc all'esterno di qualsiasi registro eventi rule-id 268435457 entrambi access-list NGFW_ONBOX_ACL note rule-id 268435458: CRITERI DI ACCESSO: NGFW_Access_Policy access-list NGFW_ONBOX_ACL note rule-id 268435458:</p>

<p>access-list NGFW_ONBOX_ACL note rule-id 268435458: L5 RULE: Demo_allow</p> <p>access-list NGFW_ONBOX_ACL advanced allow object-group acSvcg-268435458 any rule-id 268435458 event-log both</p> <p>access-list NGFW_ONBOX_ACL note rule-id 1: ACCESS POLICY: NGFW_Access_Policy</p> <p>access-list NGFW_ONBOX_ACL note rule-id 1: L5 RULE: DefaultActionRule</p> <p>access-list NGFW_ONBOX_ACL advanced deny ip any rule-id 1</p> <p>router bgp 6511</p> <p>bgp log-neighbor-changes</p> <p>bgp router-id vrf auto-assign</p> <p>unicast ipv4 famiglia di indirizzi</p> <p>adiacente 169.254.10.2 remote-as 65510</p> <p>neighbor 169.254.10.2 - mtu-discovery disable</p> <p>adiacente 169.254.10.2 attivare</p> <p>rete 192.168.70.0</p> <p>nessun riepilogo automatico</p> <p>nessuna sincronizzazione</p> <p>exit-address-family</p> <p>route esterna a 0.0.0.0 0.0.0.0 192.168.30.3.1</p> <p>crypto ipsec ikev2 ipsec-proposta AES256_SHA256</p> <p>protocollo esp encryption aes-256 aes</p> <p>protocollo esp integrità sha-256 sha-1</p> <p>crypto ipsec profile ipsec_profile e4084d322d</p> <p>set ikev2 ipsec-proposta AES256_SHA256</p> <p>imposta durata associazione di protezione kilobyte 4608000</p> <p>imposta durata associazione di protezione secondi 28800</p> <p>crypto ipsec security-association pmtu-aging infinite</p> <p>criterio crypto ikev2 1</p> <p>crittografia aes-256 aes</p> <p>integrità sha256 sha</p> <p>gruppo 14</p> <p>prf sha256 sha</p> <p>secondi durata 86400</p> <p>criterio crypto ikev2 20</p> <p>crittografia aes-256 aes-192 aes</p> <p>integrità sha512 sha384 sha256 sha</p>	<p>L5 RULE: Demo_allow</p> <p>access-list NGFW_ONBOX_ACL advanced allow object-group acSvcg-268435458 any rule-id 268435458 event-log both</p> <p>access-list NGFW_ONBOX_ACL note rule-id 1: ACCESS POLICY: NGFW_Access_Policy</p> <p>access-list NGFW_ONBOX_ACL note rule-id 1: L5 RULE: DefaultActionRule</p> <p>access-list NGFW_ONBOX_ACL advanced deny ip any rule-id 1</p> <p>router bgp 6510</p> <p>bgp log-neighbor-changes</p> <p>bgp router-id vrf auto-assign</p> <p>unicast ipv4 famiglia di indirizzi</p> <p>adiacente 169.254.10.1 remoto-as 65511</p> <p>router adiacente 169.254.10.1 transport path-mtu-discovery disable</p> <p>adiacente 169.254.10.1 attivare</p> <p>rete 192.168.50.0</p> <p>nessun riepilogo automatico</p> <p>nessuna sincronizzazione</p> <p>exit-address-family</p> <p>route esterna a 0.0.0.0 0.0.0.0 192.168.10.3.1</p> <p>crypto ipsec ikev2 ipsec-proposta AES256_SHA256</p> <p>protocollo esp encryption aes-256 aes</p> <p>protocollo esp integrità sha-256 sha-1</p> <p>crypto ipsec profile ipsec_profile e4084d322d</p> <p>set ikev2 ipsec-proposta AES256_SHA256</p> <p>imposta durata associazione di protezione kilobyte 4608000</p> <p>imposta durata associazione di protezione secondi 28800</p> <p>crypto ipsec security-association pmtu-aging infinite</p> <p>criterio crypto ikev2 1</p> <p>crittografia aes-256 aes</p> <p>integrità sha256 sha</p> <p>gruppo 14</p> <p>prf sha256 sha</p> <p>secondi durata 86400</p> <p>criterio crypto ikev2 20</p> <p>crittografia aes-256 aes-192 aes</p> <p>integrità sha512 sha384 sha256 sha</p>
--	--

<pre> gruppo 21 20 16 15 14 prf sha512 sha384 sha256 sha secondi durata 86400 crypto ikev2 enable esterna criteri di gruppo s2sGP 192.168.10.1 interno criteri di gruppo Attributi s2sGP 192.168.10.1 vpn-tunnel-protocol ikev2 tunnel group 192.168.10.1 tipo ipsec-l2l tunnel group 192.168.10.1 general-attributes default-group-policy s2sGP 192.168.10.1 attributi ipsec 192.168.10.1 del tunnel group chiave già condivisa per l'autenticazione remota ikev2 ***** chiave pre-condivisa di autenticazione locale ikev2 ***** </pre>	<pre> gruppo 21 20 16 15 14 prf sha512 sha384 sha256 sha secondi durata 86400 crypto ikev2 enable esterna criteri di gruppo s2sGP 192.168.30.1 interno criteri di gruppo Attributi s2sGP 192.168.30.1 vpn-tunnel-protocol ikev2 tunnel group 192.168.30.1 tipo ipsec-l2l tunnel group 192.168.30.1 general-attributes default-group-policy s2sGP 192.168.30.1 attributi ipsec 192.168.30.1 del tunnel group chiave già condivisa per l'autenticazione remota ikev2 ***** chiave pre-condivisa di autenticazione locale ikev2 ***** </pre>
--	--

Verifica

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

Passaggio 1. Passare alla CLI di ciascun FTD tramite la console o SSH per verificare lo stato VPN della fase 1 e della fase 2 con i comandi `show crypto ikev2 sa` e `show crypto ipsec sa`.

FTD Sito1	FTD Sito2
<pre> ftdv742# show crypto ikev2 sa SA IKEv2: Session-id:134, Status:UP-ACTIVE, IKE count:1, CHILD count:1 Ruolo di stato fvrf/ivrf remoto locale con ID tunnel 563984431 192.168.30.1/500 192.168.10.1/500 GLOBAL/Global READY RESPONDER Encr: AES-CBC, keysize: 256, hash: SHA256, DH Grp:14, segno di autenticazione: PSK, verifica di autenticazione: PSK Durata/Tempo di attività: 86400/5145 sec Child sa: selettore locale 0.0.0.0/0 - 255.255.255.255/65535 </pre>	<pre> ftdv742# show crypto ikev2 sa SA IKEv2: Session-id:13, Status:UP-ACTIVE, conteggio IKE:1, conteggio CHILD:1 Ruolo di stato fvrf/ivrf remoto locale con ID tunnel 339797985 192.168.10.1/500 192.168.30.1/500 INIZIATORE GLOBAL/GLOBAL READY Encr: AES-CBC, keysize: 256, hash: SHA256, DH Grp:14, segno di autenticazione: PSK, verifica di autenticazione: PSK Durata/Tempo di attività: 86400/74099 sec Child sa: selettore locale 0.0.0.0/0 - 255.255.255.255/65535 remote selector 0.0.0.0/0 - 255.255.255.255/65535 Ingresso/uscita spi ESP: 0xb7b5b38b/0xf0c4239d </pre>

<p>remote selector 0.0.0.0/0 - 255.255.255.255/65535</p> <p>Ingresso/uscita spi ESP: 0xf0c4239d/0xb7b5b38b</p>	
<p>ftdv742# show crypto ipsec sa</p> <p>interfaccia: demovti Tag mappa crittografica: __vti-crypto-map-Tunnel1-0-1, numero di sequenza: 65280, indirizzo locale: 192.168.30.1</p> <p>Protected vrf (ivrf): globale ident locale (addr/mask/port/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/port/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.10.1</p> <p>#pkts incapsula: 5720, #pkts cripta: 5720, #pkts digest: 5720 decapsulamento #pkts: 5717, decrittografia #pkts: 5717, verifica #pkts: 5717 #pkts compresso: 0, #pkts decompresso: 0 #pkts non compresso: 5720, errore comp #pkts: 0, errore decomp #pkts: 0 #successi pre-frag: 0, #fallimenti pre-frag: 0, #frammenti creati: 0 #PMTU inviate: 0, #PMTUs ricevute: 0, #frg decapsulate da riassemblare: 0 #TFC ricevuto: 0, #TFC inviato: 0 #Errori ICMP validi ricevuti: 0, #Errori ICMP non validi ricevuti: 0 errori #send: 0, errori #recv: 0</p> <p>endpoint di crittografia locale: 192.168.30.1/500, endpoint di crittografia remoto: 192.168.10.1/500 path mtu 1500, ipsec overhead 78(44), media mtu 1500 Tempo PMTU rimanente (sec): 0, criterio DF: copy-df Convalida errore ICMP: disabilitata, pacchetti TFC: disabilitata spi in uscita corrente: B7B5B38B spi in ingresso corrente : F0C4239D</p>	<p>ftdv742# show crypto ipsec sa</p> <p>interfaccia: demovti25 Tag mappa crittografica: __vti-crypto-map-Tunnel1-0-1, numero di sequenza: 65280, indirizzo locale: 192.168.10.1</p> <p>Protected vrf (ivrf): globale ident locale (addr/mask/port/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/port/port): (0.0.0.0/0.0.0.0/0/0) current_peer: 192.168.30.1</p> <p>#pkts incapsula: 5721, #pkts cripta: 5721, #pkts digest: 5721 decapsulamento #pkts: 5721, decrittografia #pkts: 5721, verifica #pkts: 5721 #pkts compresso: 0, #pkts decompresso: 0 #pkts non compresso: 5721, errore comp #pkts: 0, errore decomp #pkts: 0 #successi pre-frag: 0, #fallimenti pre-frag: 0, #frammenti creati: 0 #PMTU inviate: 0, #PMTUs ricevute: 0, #frg decapsulate da riassemblare: 0 #TFC ricevuto: 0, #TFC inviato: 0 #Errori ICMP validi ricevuti: 0, #Errori ICMP non validi ricevuti: 0 errori #send: 0, errori #recv: 0</p> <p>endpoint di crittografia locale: 192.168.10.1/500, endpoint di crittografia remoto: 192.168.30.1/500 path mtu 1500, ipsec overhead 78(44), media mtu 1500 Tempo PMTU rimanente (sec): 0, criterio DF: copy-df Convalida errore ICMP: disabilitata, pacchetti TFC: disabilitata spi in uscita corrente: F0C4239D spi in ingresso corrente : B7B5B38B</p>

<p> sas esp in entrata: spi: 0xF0C4239D (4039386013) Stato SA: attivo trasformazione: esp-aes-256 esp-sha-256-hmac nessuna compressione impostazioni in uso ={L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 266, mappa crittografica: __vti- crypto-map-Tunnel1-0-1 temporizzazione sa: durata chiave rimanente (kB/sec): (4285389/3722) Dimensioni IV: 16 byte supporto rilevamento riproduzione: Y Bitmap anti-replay: 0xFFFFFFFF 0xFFFFFFFF sas esp in uscita: spi: 0xB7B5B38B (3082138507) Stato SA: attivo trasformazione: esp-aes-256 esp-sha-256-hmac nessuna compressione impostazioni in uso ={L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 266, mappa crittografica: __vti- crypto-map-Tunnel1-0-1 temporizzazione sa: durata chiave rimanente (kB/sec): (4147149/3722) Dimensioni IV: 16 byte supporto rilevamento riproduzione: Y Bitmap anti-replay: 0x00000000 0x00000001 </p>	<p> sas esp in entrata: spi: 0xB7B5B38B (3082138507) Stato SA: attivo trasformazione: esp-aes-256 esp-sha-256-hmac nessuna compressione impostazioni in uso ={L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 160, mappa crittografica: __vti- crypto-map-Tunnel1-0-1 temporizzazione sa: durata chiave rimanente (kB/sec): (3962829/3626) Dimensioni IV: 16 byte supporto rilevamento riproduzione: Y Bitmap anti-replay: 0xFFFFFFFF 0xFFFFFFFF sas esp in uscita: spi: 0xF0C4239D (4039386013) Stato SA: attivo trasformazione: esp-aes-256 esp-sha-256-hmac nessuna compressione impostazioni in uso ={L2L, Tunnel, IKEv2, VTI, } slot: 0, conn_id: 160, mappa crittografica: __vti- crypto-map-Tunnel1-0-1 temporizzazione sa: durata chiave rimanente (kB/sec): (4101069/3626) Dimensioni IV: 16 byte supporto rilevamento riproduzione: Y Bitmap anti-replay: 0x00000000 0x00000001 </p>
--	--

Passaggio 2. Passare alla CLI di ciascun FTD tramite la console o SSH per verificare lo stato BGP usando i comandi show bgp neighbors e show route bgp.

FTD Sito1	FTD Sito2
<p> ftdv742# show bgp neighbors Il router BGP adiacente è 169.254.10.2, vrf single_vf, remoto AS 65510, collegamento esterno BGP versione 4, ID router remoto 192.168.50.1 Stato BGP = Stabilito, attivo per 1 d20 h Ultima lettura 00:00:25, ultima scrittura 00:00:45, tempo di attesa 180, intervallo keepalive 60 secondi Sessioni router adiacente: 1 attivo, non compatibile con multisessione </p>	<p> ftdv742# show bgp neighbors Il router BGP adiacente è 169.254.10.1, vrf single_vf, remoto AS 65511, collegamento esterno BGP versione 4, ID router remoto 192.168.70.1 Stato BGP = Stabilito, attivo per 1 d20 h Ultima lettura 00:00:11, ultima scrittura 00:00:52, tempo di attesa 180, intervallo keepalive 60 secondi Sessioni router adiacente: 1 attivo, non compatibile con multisessione </p>

<p>(disabilitato) Funzionalità router adiacenti: Aggiornamento route: annunciato e ricevuto (nuovo) Funzionalità ASN a quattro ottetti: annunciata e ricevuta Famiglia di indirizzi IPv4 Unicast: annunciati e ricevuti Funzionalità multisessione: Statistiche messaggi: Profondità InQ uguale a 0 La profondità di OutQ è 0</p> <p>Ricevuto Apertura: 1 1 Notifiche: 0 0 Aggiornamenti: 2 2 Mantenimento attività: 2423 2427 Aggiornamento route: 0 0 Totale: 2426 2430 Il tempo minimo predefinito tra le esecuzioni dell'annuncio è 30 secondi</p> <p>Per la famiglia di indirizzi: Unicast IPv4 Sessione: 169.254.10.2 Tabella BGP versione 3, router adiacente versione 3/0 Dimensione coda di output: 0 Indice 1 1 membro del gruppo di aggiornamento Ricevuto Attività prefisso: — Prefissi correnti: 1 1 (consuma 80 byte) Totale prefissi: 1 1 Ritiro implicito: 0 0 Ritiro esplicito: 0 0 Utilizzato come percorso migliore: n/d 1 Utilizzato come multipath: n/d 0</p> <p>In uscita in entrata Prefissi non consentiti criteri locali: — Percorso migliore dal peer: 1 n/d Totale: 1 0 Numero di NLRI inviati nell'aggiornamento: max 1, min 0</p>	<p>(disabilitato) Funzionalità router adiacenti: Aggiornamento route: annunciato e ricevuto (nuovo) Funzionalità ASN a quattro ottetti: annunciata e ricevuta Famiglia di indirizzi IPv4 Unicast: annunciati e ricevuti Funzionalità multisessione: Statistiche messaggi: Profondità InQ uguale a 0 La profondità di OutQ è 0</p> <p>Ricevuto Apertura: 1 1 Notifiche: 0 0 Aggiornamenti: 2 2 Mantenimento attività: 2424 2421 Aggiornamento route: 0 0 Totale: 2427 2424 Il tempo minimo predefinito tra le esecuzioni dell'annuncio è 30 secondi</p> <p>Per la famiglia di indirizzi: Unicast IPv4 Sessione: 169.254.10.1 Tabella BGP versione 9, router adiacente versione 9/0 Dimensione coda di output: 0 Indice 4 4 membro del gruppo di aggiornamento Ricevuto Attività prefisso: — Prefissi correnti: 1 1 (consuma 80 byte) Totale prefissi: 1 1 Ritiro implicito: 0 0 Ritiro esplicito: 0 0 Utilizzato come percorso migliore: n/d 1 Utilizzato come multipath: n/d 0</p> <p>In uscita in entrata Prefissi non consentiti criteri locali: — Percorso migliore dal peer: 1 n/d Totale: 1 0 Numero di NLRI inviati nell'aggiornamento: max 1, min 0</p>
---	---

<p>Il rilevamento degli indirizzi è abilitato, il RIB ha un percorso a 169.254.10.2 Connessioni stabilite 1; eliminate 0 Ultima reimpostazione mai Transport(tcp) path-mtu-discovery disabilitato Graceful-Restart disabilitato</p>	<p>Il rilevamento degli indirizzi è abilitato, il RIB ha un percorso a 169.254.10.1 Connessioni stabilite 4; interrotte 3 Ultimo reset 1d21h, a causa del flap dell'interfaccia della sessione 1 Transport(tcp) path-mtu-discovery disabilitato Graceful-Restart disabilitato</p>
<p>ftdv742# show route bgp</p> <p>Codici: L - locale, C - connesso, S - statico, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP esterno, O - OSPF, IA - OSPF interarea N1 - Tipo esterno NSSA OSPF 1, N2 - Tipo esterno NSSA OSPF 2 E1 - OSPF tipo esterno 1, E2 - OSPF tipo esterno 2, V - VPN i - IS-IS, su - IS-IS riepilogo, L1 - IS-IS livello-1, L2 - IS livello-2 ia - IS-IS inter area, * - valore predefinito candidato, U - route statica per utente o - ODR, P - route statica scaricata periodicamente, + - route replicata SI - Static InterVRF, BI - BGP InterVRF Il gateway di ultima istanza è 192.168.30.3 alla rete 0.0.0.0</p> <p>B 192.168.50.0 255.255.255.0 [20/0] via 169.254.10.2, 1d20h</p>	<p>ftdv742# show route bgp</p> <p>Codici: L - locale, C - connesso, S - statico, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP esterno, O - OSPF, IA - OSPF interarea N1 - Tipo esterno NSSA OSPF 1, N2 - Tipo esterno NSSA OSPF 2 E1 - OSPF tipo esterno 1, E2 - OSPF tipo esterno 2, V - VPN i - IS-IS, su - IS-IS riepilogo, L1 - IS-IS livello-1, L2 - IS livello-2 ia - IS-IS inter area, * - valore predefinito candidato, U - route statica per utente o - ODR, P - route statica scaricata periodicamente, + - route replicata SI - Static InterVRF, BI - BGP InterVRF Il gateway di ultima istanza è 192.168.10.3 alla rete 0.0.0.0</p> <p>B 192.168.70.0 255.255.255.0 [20/0] via 169.254.10.1, 1d20h</p>

Passaggio 3. Il ping tra il client Site1 e il client Site2 è riuscito.

Client Sito1:

```
Site1_Client#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 = 31/56/90 ms
```

Client Site2:

```
Site2_Client#ping 192.168.70.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.70.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/39/71 ms
```

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 usare questi comandi di debug per risolvere i problemi relativi alla sezione BGP.

```
ftdv742# debug ip bgp ?
```

```
A.B.C.D    BGP neighbor address
all All    address families
events     BGP events
import     BGP path import across topologies, VRFs or AFs in BGP Inbound information
ipv4       Address family
ipv6       Address family
keepalives BGP keepalives
out        BGP Outbound information
range     BGP dynamic range
rib-filter Next hop route watch filter events
updates    BGP updates
vpn4       Address family
vpn6       Address family
vrf        VRF scope
<cr>
```

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).