

Configurazione della VPN da sito a sito basata su route compatibile con VRF su FTD Gestito da FDM

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurare l'FTD](#)

[Configurazione dell'ASA](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Riferimento](#)

Introduzione

Questo documento descrive come configurare la VPN da sito a sito basata su route con supporto VRF su FTD gestito da FDM.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di VPN
- Conoscenze base di VRF (Virtual Routing and Forwarding)
- 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

- Cisco ASA versione 9.20.3

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.

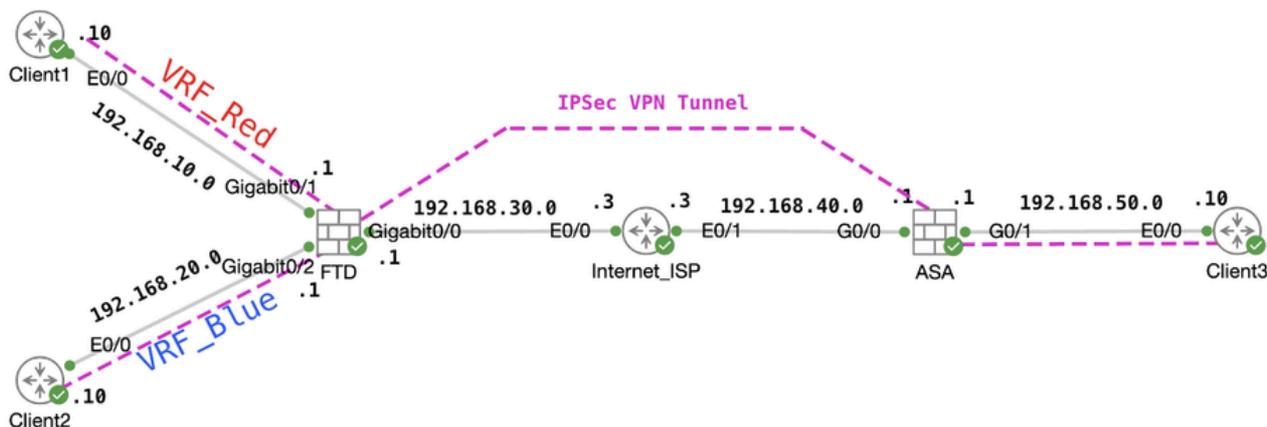
Premesse

Virtual Routing and Forwarding (VRF) su Firepower Device Manager (FDM) consente di creare più istanze di routing isolate su un singolo dispositivo Firepower Threat Defense (FTD). Ogni istanza VRF opera come un router virtuale separato con una tabella di routing specifica, consentendo la separazione logica del traffico di rete e fornendo funzionalità avanzate di sicurezza e gestione del traffico.

In questo documento viene spiegato come configurare una VPN IPsec con supporto VRF con VTI. VRF Red network e VRF Blue network sono dietro FTD. Il client 1 nella rete rossa VRF e il client 2 nel blu VRF comunicano con il client 3 dietro l'ASA tramite il tunnel VPN IPsec.

Configurazione

Esempio di rete

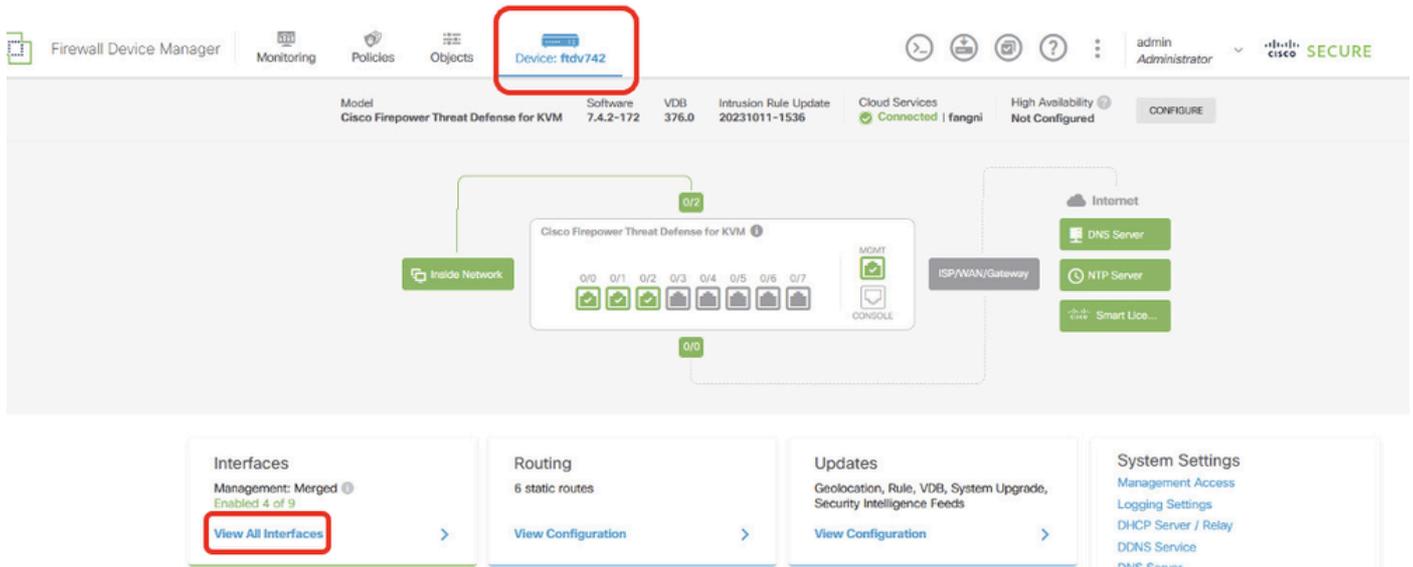


Topologia

Configurare l'FTD

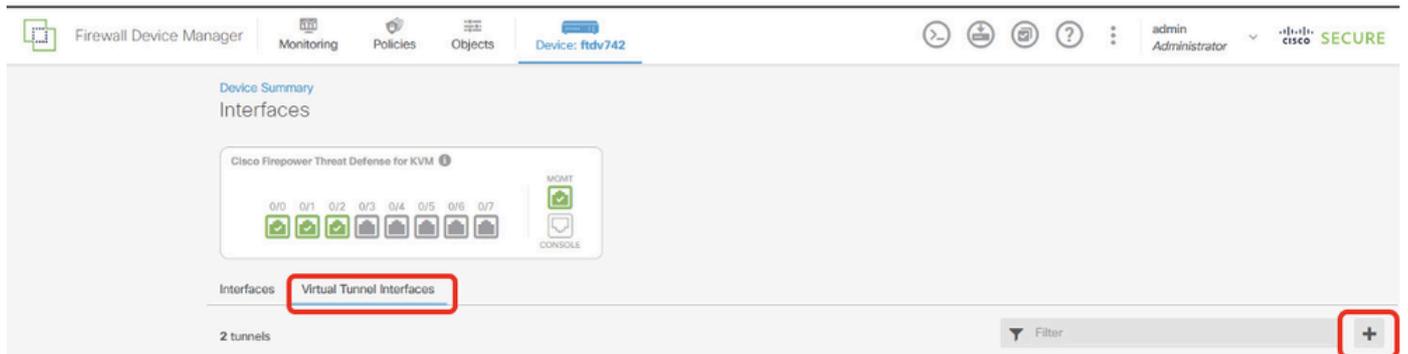
Passaggio 1. È essenziale verificare che la configurazione preliminare dell'interconnettività IP tra i nodi sia stata debitamente completata. Client1 e Client2 hanno indirizzo IP interno FTD come gateway. Il client 3 ha come gateway l'indirizzo IP interno dell'appliance ASA.

Passaggio 2. Creare l'interfaccia del tunnel virtuale. Accedere alla GUI FDM di FTD. Passare a Dispositivo > Interfacce. Fare clic su Visualizza tutte le interfacce.



Interfacce FTD_View

Passaggio 2.1. Fare clic sulla scheda Interfacce tunnel virtuale. Fare clic sul pulsante +.



FTD_Create_VTI

Passaggio 2.2. Fornire le informazioni necessarie. 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 Status

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

Description

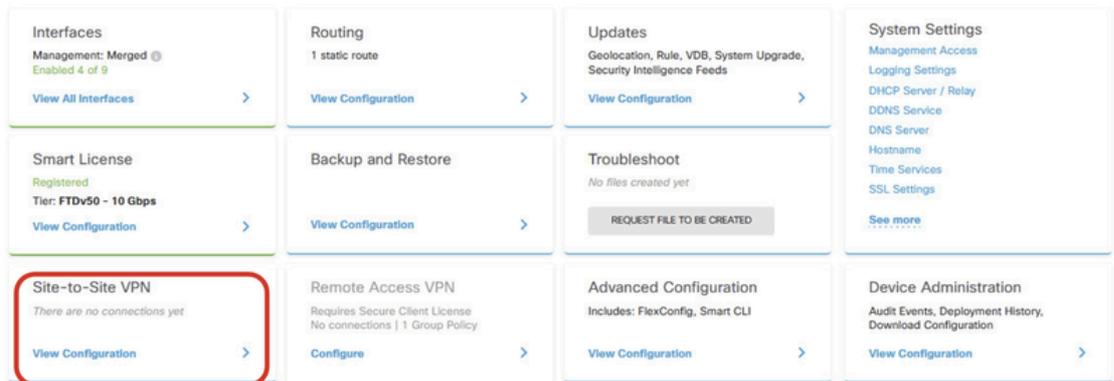
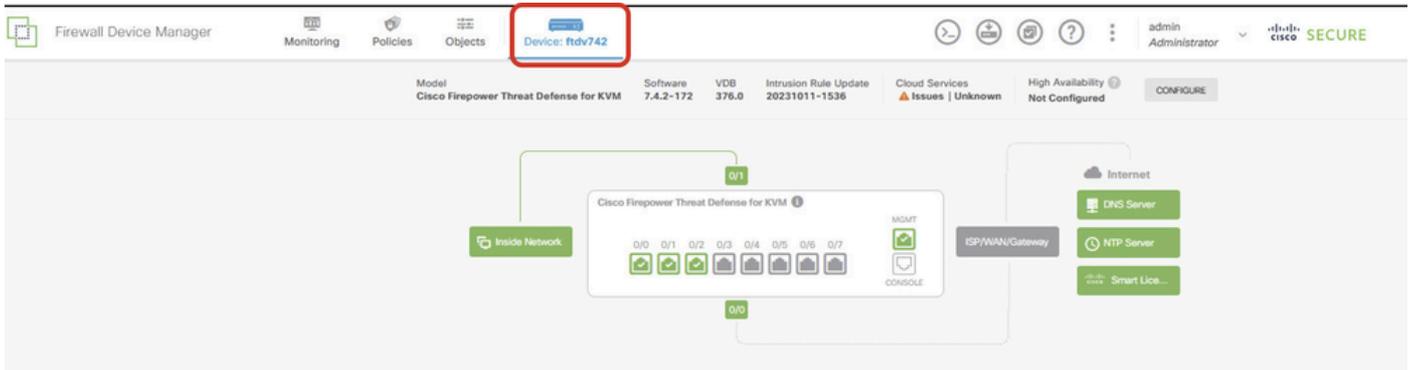
Tunnel ID 0 - 10413 Tunnel Source

IP Address and Subnet Mask /

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

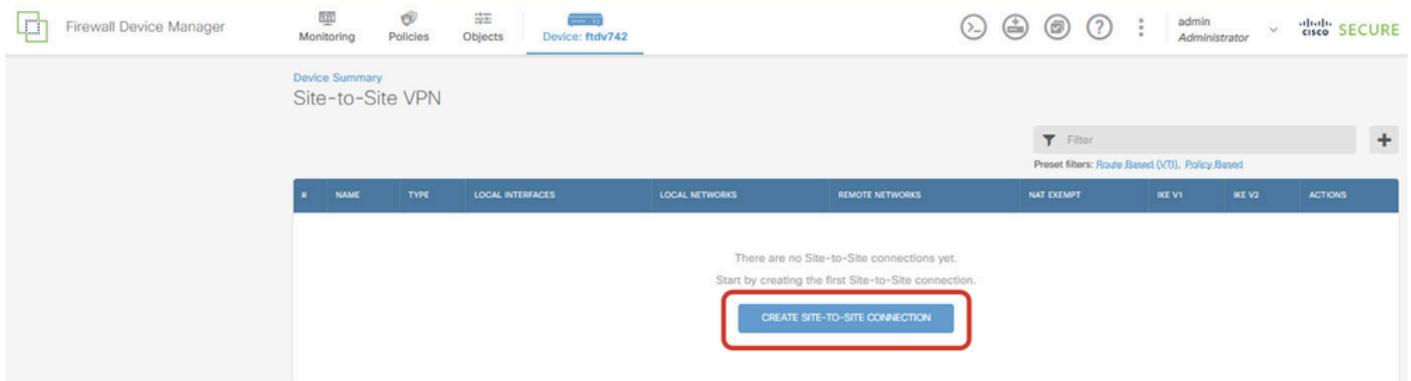
FTD_Create_VTI_Details

Passaggio 3. Passare a Dispositivo > VPN da sito a sito . Fare clic sul pulsante View Configuration (Visualizza configurazione).



FTD_Site-to-Site_VPN_View_Configurations

Passaggio 3.1. Iniziare a creare una nuova VPN da sito a sito. Fare clic sul pulsante CREA CONNESSIONE DA SITO A SITO. In alternativa, fare clic sul pulsante +.



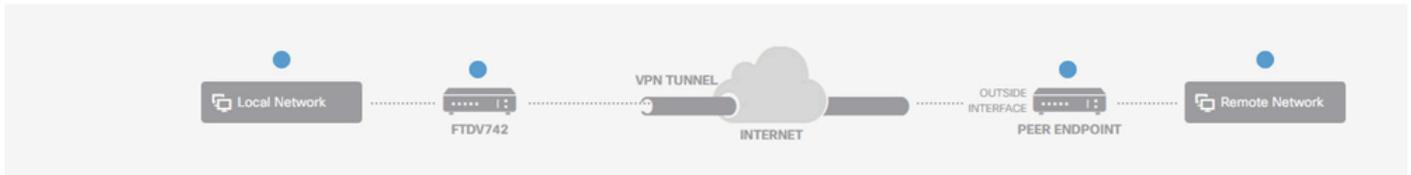
FTD_Create_Site2Site_Connection

Passaggio 3.2. Fornire informazioni necessarie. Fare clic sul pulsante NEXT.

- Nome profilo connessione: Demo_S2S
- Tipo: VTI (Route Based)
- Interfaccia di accesso VPN locale: rimozione (creata nel passaggio 2)
- Indirizzo IP remoto: 192.168.40.1 (si tratta dell'indirizzo IP esterno dell'ASA peer)

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:

Type: Policy Based

Sites Configuration

LOCAL SITE	REMOTE SITE
Local VPN Access Interface: <input type="text" value="demovti (Tunnel1)"/>	Remote IP Address: <input type="text" value="192.168.40.1"/>

CANCEL

FTD_Site-to-Site_VPN_Endpoints

Passaggio 3.3. Passare al criterio IKE. Fare clic sul pulsante EDIT.

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 configuration with the 'Configuration' step highlighted. It includes 'Local Network', 'FTDV742', 'VPN TUNNEL', 'INTERNET', 'OUTSIDE 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

IPSec Proposal

None selected !

FTD_Edit_IKE_Policy

Passaggio 3.4. Per i criteri IKE, è possibile utilizzare valori predefiniti oppure crearne uno nuovo facendo clic su Crea nuovo criterio IKE .

In questo esempio, attivare o disattivare il nome di un criterio IKE esistente AES-SHA-SHA. Fare clic sul pulsante OK per salvare.

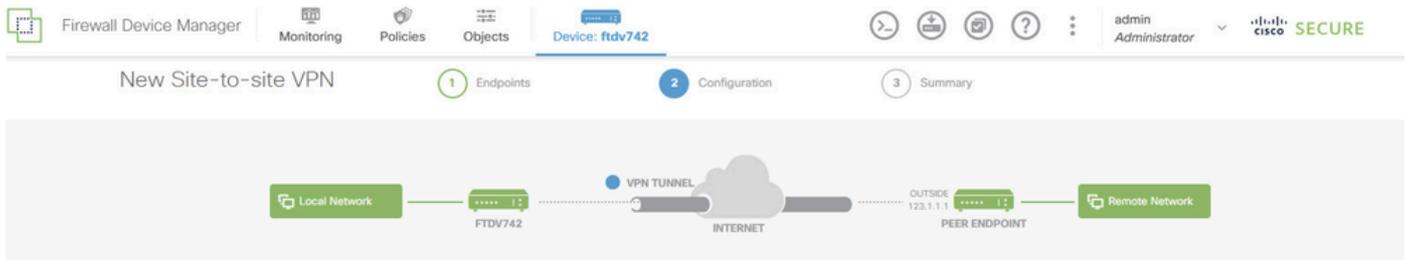
The screenshot shows a configuration window titled "Create New IKE Policy". At the top, there is a "Filter" input field. Below it, a list of IKE policies is displayed, each with a toggle switch and an information icon (i). The "AES-SHA-SHA" policy is highlighted with a red rectangular box, and its toggle switch is turned on. The "OK" button at the bottom right is also highlighted with a red rectangular box.

Policy Name	Status	Info Icon
AES-GCM-NULL-SHA	Off	i
AES-SHA-SHA	On	i
DES-SHA-SHA	Off	i

Buttons: [Create New IKE Policy](#), [OK](#)

FTD_Enable_IKE_Policy

Passaggio 3.5. Passare alla proposta IPSec. Fare clic sul pulsante EDIT.



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

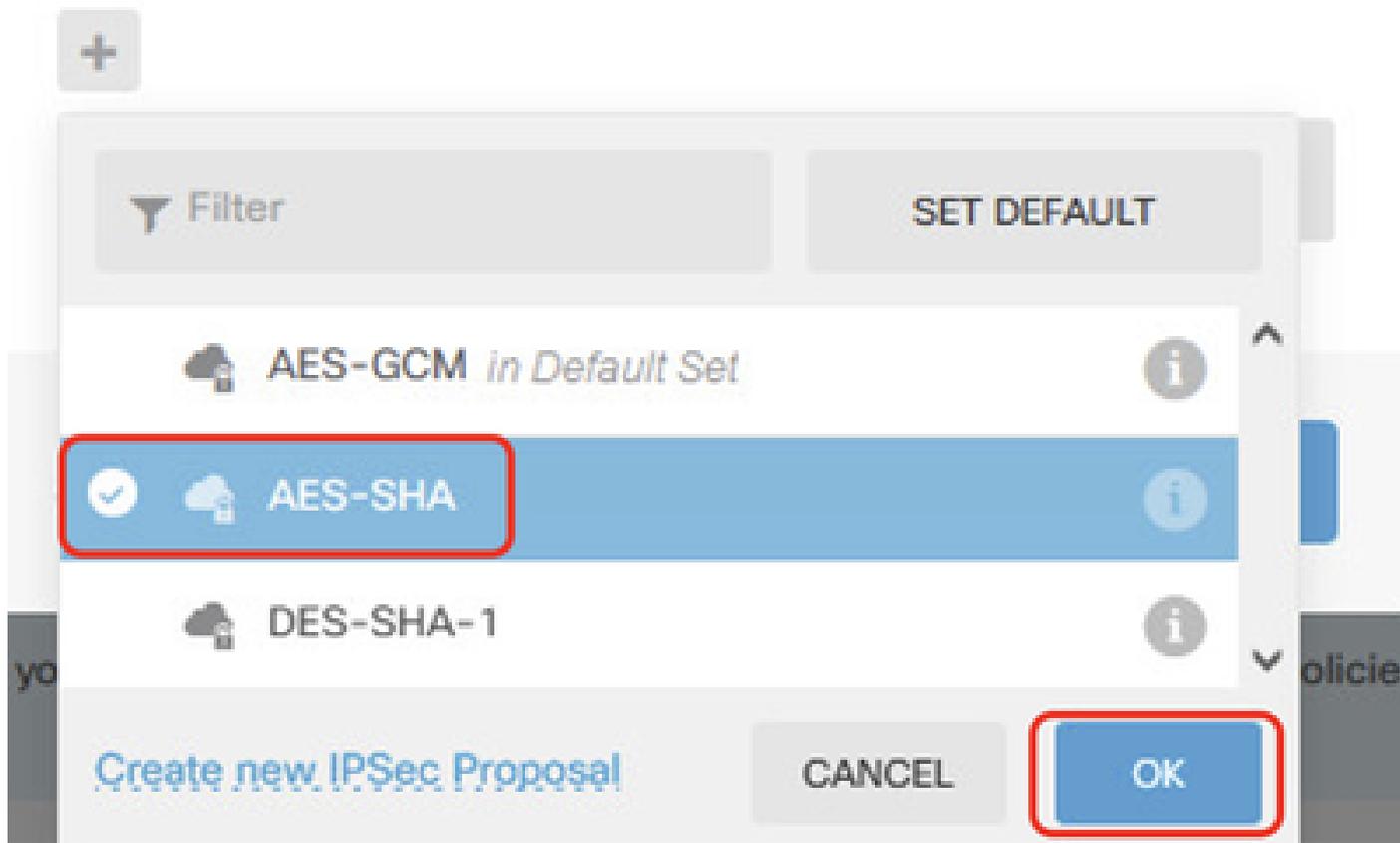
None selected 1

Proposta_FTD_Edit_IPSec

Passaggio 3.6. Per una proposta IPSec, è possibile utilizzare una proposta predefinita oppure crearne una nuova facendo clic su Crea nuova proposta IPSec.

In questo esempio, attivare o disattivare il nome di una proposta IPSec esistente AES-SHA. Fare clic su OK per salvare.

Select IPsec Proposals



Proposta FTD_Enable_IPsec

Passaggio 3.7. Scorrere la pagina e configurare la chiave già condivisa. Fare clic sul pulsante NEXT.

Prendere nota della chiave già condivisa e configurarla sull'appliance ASA in un secondo momento.

Firewall Device Manager | Monitoring | Policies | Objects | Device: ftdv742 | admin Administrator | Cisco Security

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:

FTD_Configura_Chiave_già_condivisa

Passaggio 3.8. Esaminare la configurazione VPN. Se è necessario apportare modifiche, fare clic sul pulsante INDIETRO. Se tutto funziona, fare clic sul pulsante FINISH (Fine).

Demo_S2S Connection Profile

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

VPN Access Interface demovti (169.254.10.1) ↔ **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

IPSec Proposal aes,aes-192,aes-256-sha-512,sha-384,sha-256,sha-1

Authentication Type Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration 28800 seconds

Lifetime Size 4608000 kilobytes

ADDITIONAL OPTIONS

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: Null (not selected)
Group:

BACK **FINISH**

FTD_Review_VPN_Configuration

Passaggio 3.9. Creare una regola di controllo dell'accesso per consentire il passaggio del traffico attraverso l'FTD. In questo esempio, consenti tutto per scopo dimostrativo. Modifica i criteri in base alle tue esigenze.

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

Security Policies

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

1 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		

Default Action: Access Control **Block**

Esemplio_FTD_ACP

Passaggio 3.10. (Facoltativo) Configurare la regola di esenzione NAT per il traffico client su FTD

se è presente un NAT dinamico configurato per l'accesso del client a Internet. In questo esempio, non è necessario configurare una regola di esenzione NAT perché non è presente un NAT dinamico configurato su FTD.

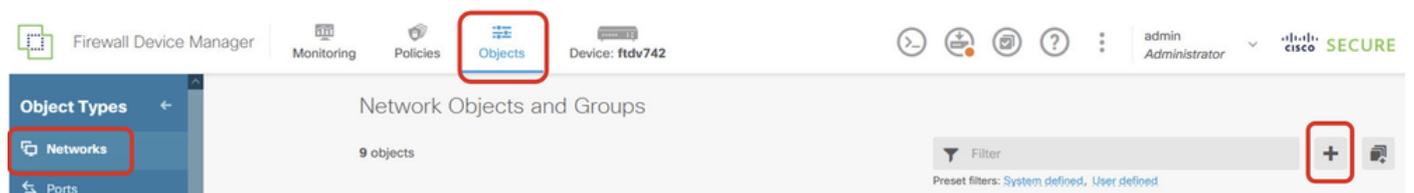
Passaggio 3.11. Distribuire le modifiche alla configurazione.



FTD_Deployment_Changes

Passaggio 4. Configurare i router virtuali.

Passaggio 4.1. Creare gli oggetti di rete per l'instradamento statico. Passare a Oggetti > Reti , quindi fare clic sul pulsante +.



FTD_Create_NetObjects

Passaggio 4.2. Fornire le informazioni necessarie su ciascun oggetto di rete. Fare clic sul pulsante OK.

- Nome: local_blue_192.168.20.0
- Tipo: Rete
- Rete: 192.168.20.0/24

Add Network Object



Name

local_blue_192.168.20.0

Description

Type



Network



Host

Network

192.168.20.0/24

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

CANCEL

OK

FTD_VRF_Blue_Network

- Nome: local_red_192.168.10.0
- Tipo: Rete
- Rete: 192.168.10.0/24

Add Network Object



Name

local_red_192.168.10.0

Description

Type



Network



Host

Network

192.168.10.0/24

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

CANCEL

OK

FTD_VRF_Red_Network

- Nome: remote_192.168.50.0
- Tipo: Rete
- Rete: 192.168.50.0/24

Add Network Object



Name

remote_192.168.50.0

Description

Type



Network



Host



FQDN



Range

Network

192.168.50.0/24

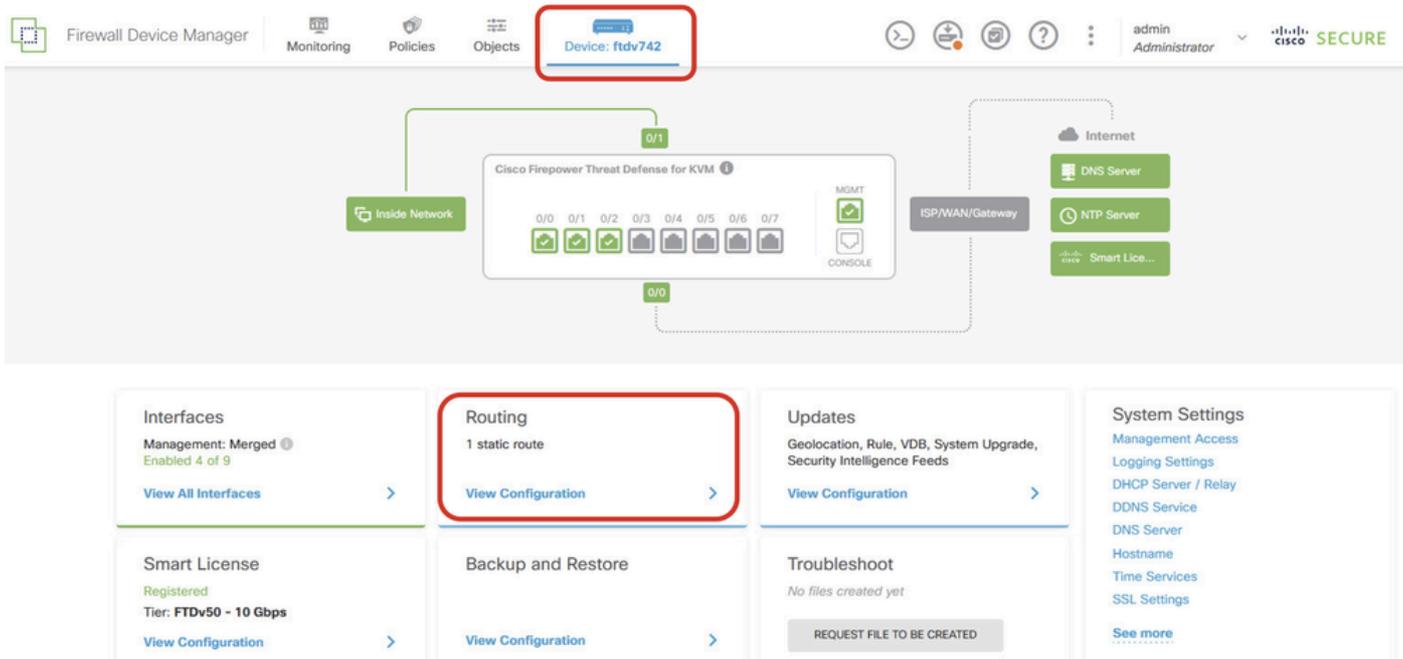
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

Rete_remota_FTD

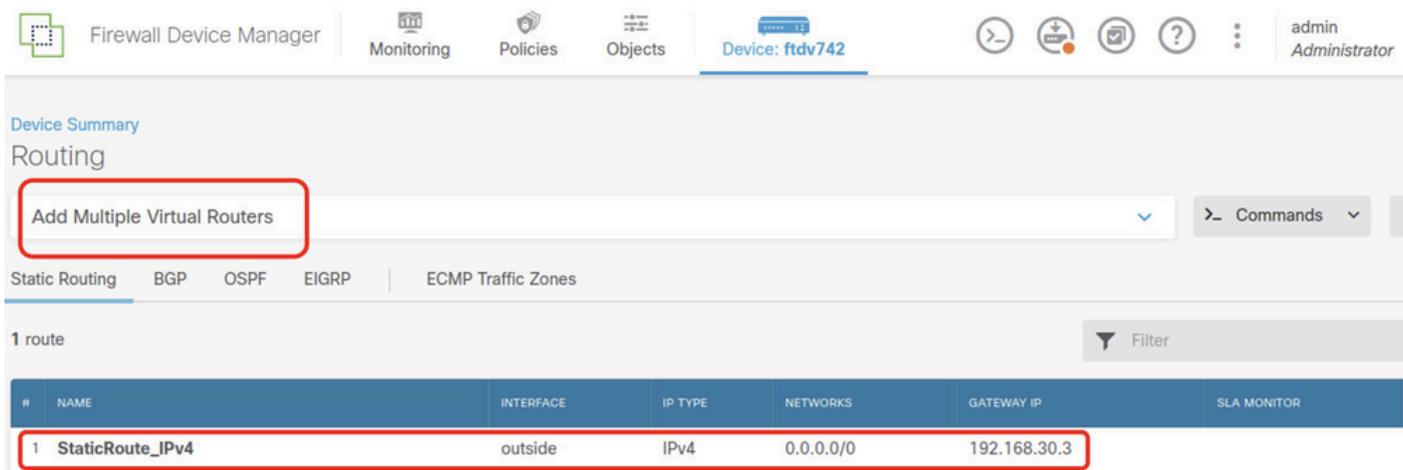
Passaggio 4.3. Creare il primo router virtuale. Selezionare Periferica > Instradamento. Fare clic su View Configuration (Visualizza configurazione).



FTD_View_Routing_Configuration

Passaggio 4.4. Fare clic su Add Multiple Virtual Router (Aggiungi più router virtuali).

Nota: è già stata configurata una route statica tramite interfaccia esterna durante l'inizializzazione di FDM. Se non è disponibile, configurarlo manualmente.



FTD_Add_First_Virtual_Router1

Passaggio 4.5. Fare clic su CREATE FIRST CUSTOM VIRTUAL ROUTER.

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

Device Summary

Routing

Virtual Route Forwarding (Virtual Routing) Description

You can create multiple virtual routing and forwarding instances, called virtual routers, to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device.

Thus, you can provide support to two or more distinct customers over a common set of networking equipment. You can also use virtual routers to provide more separation for elements of your own network, for example, by isolating a development network from your general-purpose corporate network.

How Multiple Virtual Routers Work

Multiple Virtual Router mode is enabled automatically if there is at least one custom Virtual Router.

Diagram illustrating how multiple virtual routers work. It shows a central 'THREAT DEFENSE' module connected to multiple 'VIRTUAL ROUTER' instances (A, B, N). Each virtual router is connected to its own set of customer networks (CUSTOMER A NETWORK 1 & 2, CUSTOMER B NETWORK 1 & 2, etc.). A red box highlights the 'CREATE FIRST CUSTOM VIRTUAL ROUTER' button at the bottom.

Commands

FTD_Add_First_Virtual_Router2

Passaggio 4.6. Fornire le informazioni necessarie sul primo router virtuale. Fare clic sul pulsante OK. Dopo la creazione del primo router virtuale, viene visualizzato automaticamente il nome globale del file vrf.

- Nome: vrf_red
- Interfacce: inside_red (Gigabit Ethernet0/1)

Firewall Device Manager | admin Administrator

Device Summary

Routing

Add Virtual Router

Name: vrf_red

Description:

Interfaces: inside_red (GigabitEthernet0/1)

CANCEL OK

CREATE FIRST CUSTOM VIRTUAL ROUTER

FTD_Add_First_Virtual_Router3

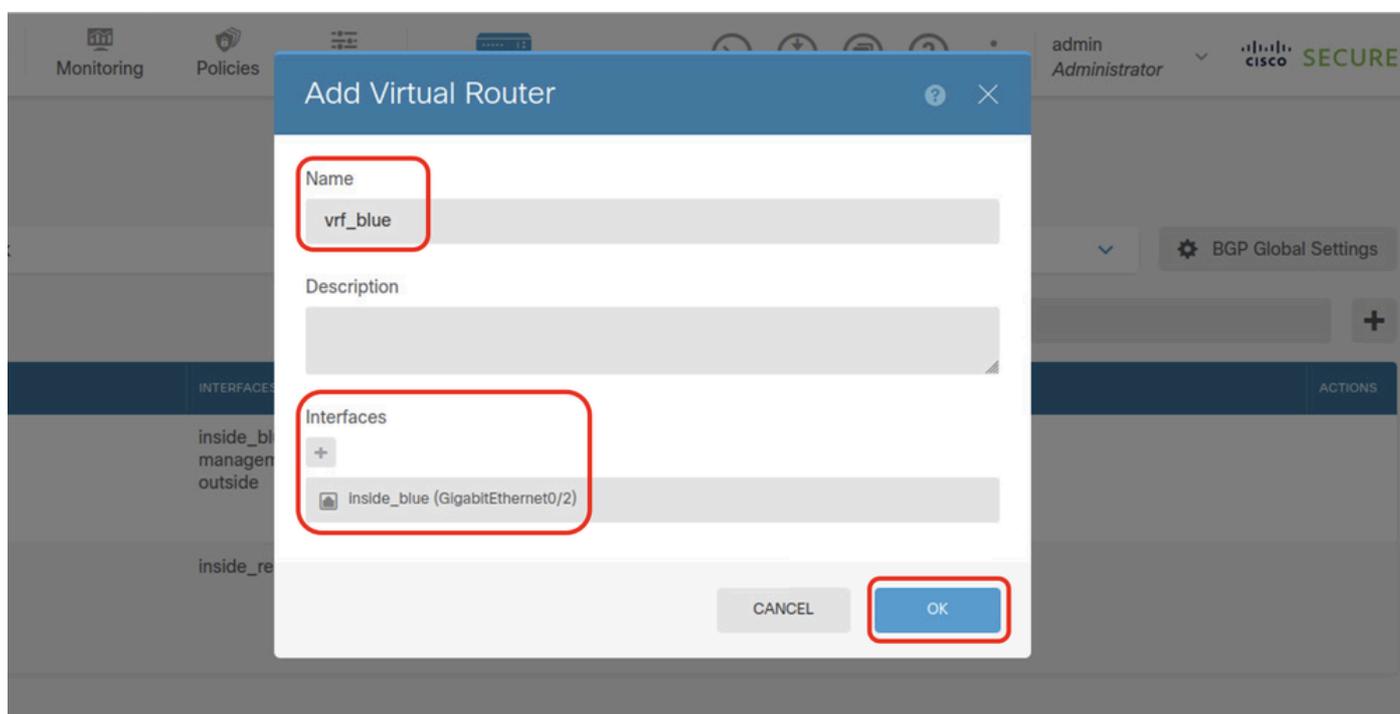
Passaggio 4.7. Creare il secondo router virtuale. Passare a Dispositivo > Routing. Fare clic su View Configuration (Visualizza configurazione). Fare clic sul pulsante +.



FTD_Add_Second_Virtual_Router

Passaggio 4.8. Fornire le informazioni necessarie sul secondo router virtuale. Fare clic su OK pulsante

- Nome: vrf_blue
- Interfacce: inside_blue (Gigabit Ethernet0/2)



FTD_Add_Second_Virtual_Router2

Passaggio 5. Creare una perdita di route da vrf_blue a Global. Questa route consente agli endpoint nella rete 192.168.20.0/24 di avviare connessioni che attraversano il tunnel VPN da sito a sito. Per questo esempio, l'endpoint remoto sta proteggendo la rete 192.168.50.0/24.

Selezionare Periferica > Instradamento. Fare clic su Visualizza configurazione. fare clic sull'icona Visualizza nella cella Action del router virtuale vrf_blue.

Device Summary
Virtual Routers

How Multiple Virtual Routers Work

3 virtual routers

#	NAME	INTERFACES	SHOW/TROUBLESHOOT	ACTIONS
1	Global	management outside	Routes Ipv6 routes BGP OSPF	
2	vrf_blue	inside_blue	Routes Ipv6 routes BGP OSPF	View
3	vrf_red	inside_red	Routes Ipv6 routes BGP OSPF	

FTD_Visualizza_VRF_Blue

Passaggio 5.1. Fare clic sulla scheda Instradamento statico. Fare clic sul pulsante +.

Device Summary / Virtual Routers
vrf_blue

How Multiple Virtual Routers Work

Virtual Router Properties | **Static Routing** | BGP | OSPF | ECMP Traffic Zones

Commands

Filter +

FTD_Create_Static_Route_VRF_Blue

Passaggio 5.2. Fornire le informazioni necessarie. Fare clic sul pulsante OK.

- Nome: Blue_to_ASA
- Interfaccia: demovti (Tunnel1)
- Reti: remote_192.168.50.0
- Gateway: lascia vuoto questo elemento.

Name
Blue_to_ASA

Description

Interface
demovti (Tunnel1) Belongs to current Router
N/A

Protocol
 IPv4 IPv6

Networks
+
remote_192.168.50.0

Gateway
Please select a gateway Metric
1

SLA Monitor *Applicable only for IPv4 Protocol type*
Please select an SLA Monitor

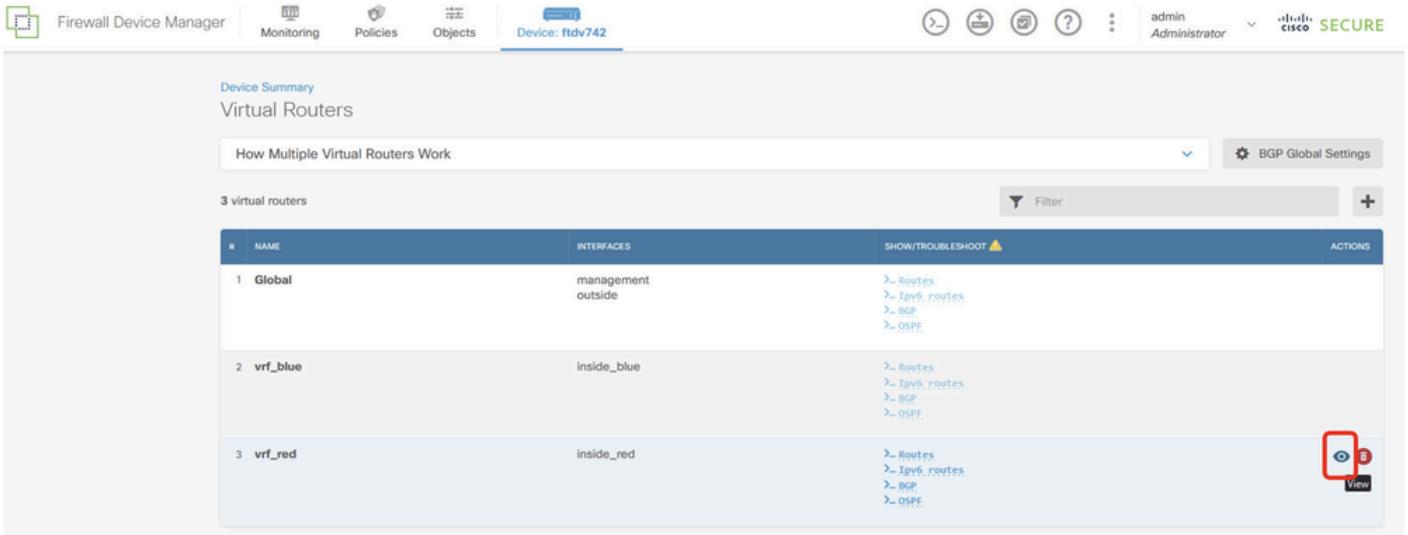
CANCEL OK

FTD_Create_Static_Route_VRF_Blue_Details

Passaggio 6. Creare una perdita di route da vrf_red a Global. Questa route consente agli endpoint nella rete 192.168.10.0/24 di avviare connessioni che attraversano il tunnel VPN da sito a sito. Per

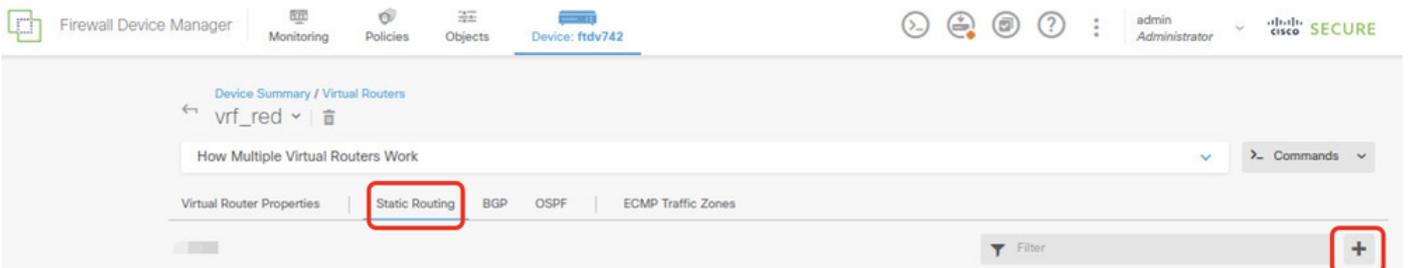
questo esempio, l'endpoint remoto sta proteggendo la rete 192.168.50.0/24.

Selezionare Periferica > Instradamento. Fare clic su Visualizza configurazione. fare clic sull'icona Visualizza nella cella Action del router virtuale vrf_red.



FTD_Visualizza_VRF_Red

Passaggio 6.1. Fare clic sulla scheda Instradamento statico. Fare clic sul pulsante +.



FTD_Create_Static_Route_VRF_Red

Passaggio 6.2. Fornire le informazioni necessarie. Fare clic sul pulsante OK.

- Nome: Rosso_su_ASA
- Interfaccia: demovti (Tunnel1)
- Reti: remote_192.168.50.0
- Gateway: lascia vuoto questo elemento.

vrf_red

Add Static Route



Name

Red_to_ASA

Description

Interface

demovti (Tunnel1)

Belongs to current Router

N/A

Protocol



IPv4



IPv6

Networks



remote_192.168.50.0

Gateway

Please select a gateway

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

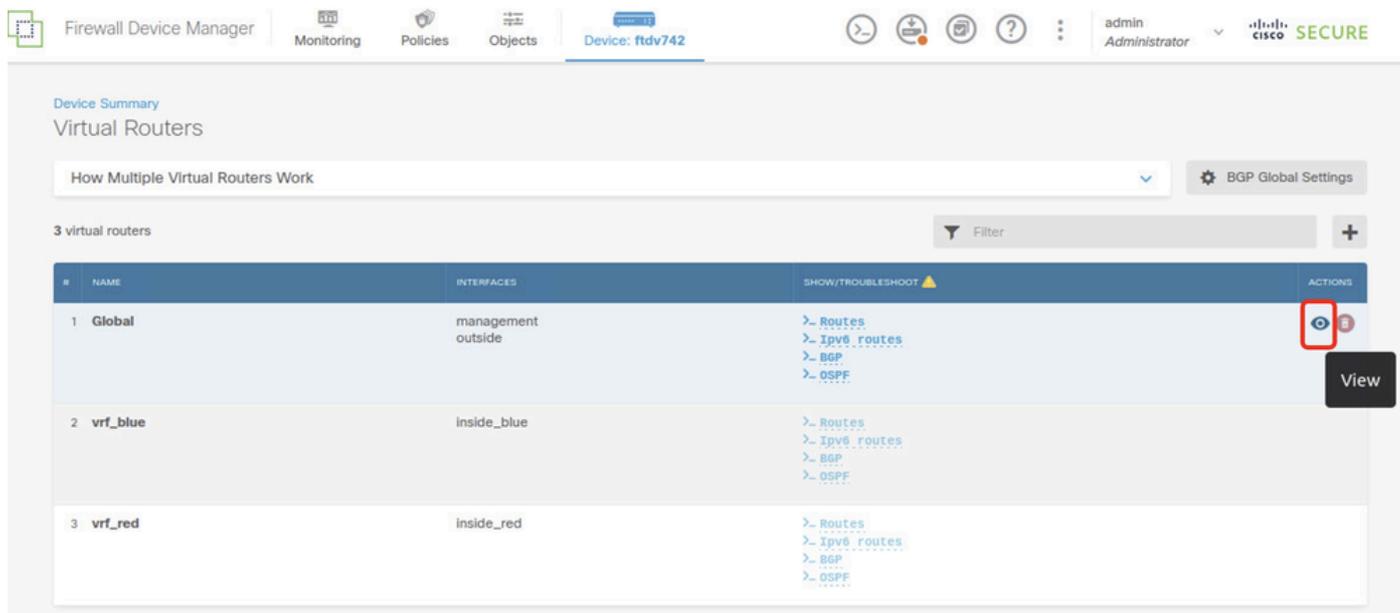
OK

FTD_Create_Static_Route_VRF_Red_Details

Passaggio 7. Creare una perdita del percorso dai router globali a quelli virtuali. Le route consentono agli endpoint protetti dall'estremità remota della VPN da sito a sito di accedere alla

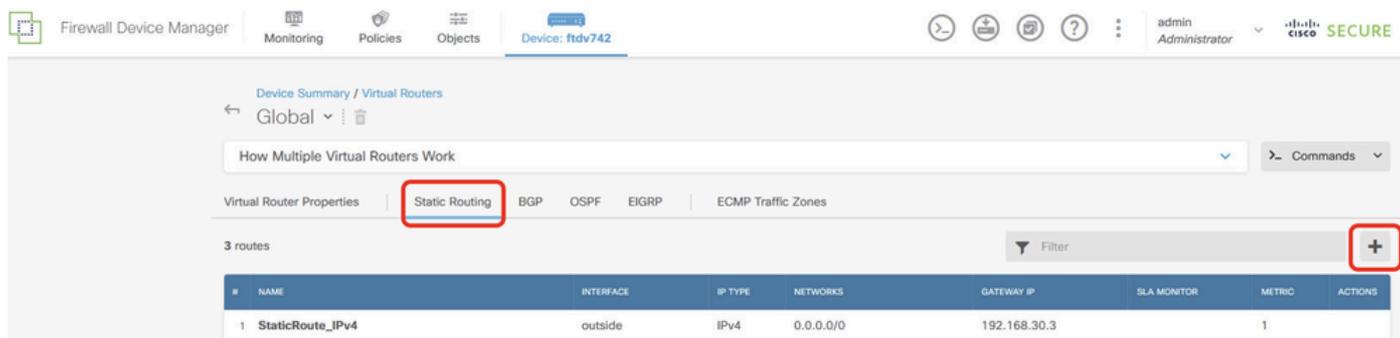
rete 192.168.10.0/24 nel router virtuale vrf_red e alla rete 192.168.20.0/24 nel router virtuale vrf_blue.

Selezionare Periferica > Instradamento. Fare clic su Visualizza configurazione. fare clic sull'icona Visualizza nella cella Azione del router virtuale globale.



FTD_Visualizza_VRF_Global

Passaggio 7.1. Fare clic sulla scheda Instradamento statico. Fare clic sul pulsante +.



FTD_Create_Static_Route_VRF_Global

Passaggio 7.2. Fornire le informazioni necessarie. Fare clic sul pulsante OK.

- Nome: S2S_leak_blue
- Interfaccia: inside_blue (Gigabit Ethernet0/2)
- Reti: local_blue_192.168.20.0
- Gateway: lascia vuoto questo elemento.

Global Add Static Route



Name

S25_leak_blue

Description



The selected interface belongs to a different virtual router. If you create this static route, the route will cross virtual router boundaries, with the risk that traffic from this virtual router will leak into another virtual router. Proceed with caution.

Interface

inside_blue (GigabitEthernet0/2)

Belongs to different Router

vt_blue

Protocol



IPv4



IPv6

Networks



local_blue_192.168.20.0

Gateway

Please select a gateway

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

```
encryption aes-256 aes-192 aes
integrity sha512 sha384 sha256 sha
group 21 20 16 15 14
prf sha512 sha384 sha256 sha
lifetime seconds 86400
```

Passaggio 10. Creare una proposta ipsec IKEv2 che definisce gli stessi parametri configurati nell'FTD.

```
<#root>
```

```
crypto ipsec ikev2 ipsec-proposal
```

```
AES-SHA
```

```
protocol esp encryption aes-256 aes-192 aes
protocol esp integrity sha-512 sha-384 sha-256 sha-1
```

Passaggio 11. Creazione di un profilo ipsec, riferimento proposta ipsec creata nel passaggio 10.

```
<#root>
```

```
crypto ipsec profile
```

```
demo_ipsec_profile
```

```
set ikev2 ipsec-proposal
```

```
AES-SHA
```

```
set security-association lifetime kilobytes 4608000
set security-association lifetime seconds 28800
```

Passaggio 12. Creare un criterio di gruppo che consenta il protocollo IKEv2.

```
<#root>
```

```
group-policy
```

```
demo_gp_192.168.30.1
```

```
internal
group-policy demo_gp_192.168.30.1 attributes
vpn-tunnel-protocol ikev2
```

Passaggio 13. Creare un gruppo di tunnel per l'FTD peer esterno all'indirizzo IP, facendo

riferimento ai criteri di gruppo creati nel passaggio 12 e configurazione della stessa chiave già condivisa con FTD (creata al passaggio 3.7).

```
<#root>
```

```
tunnel-group 192.168.30.1 type ipsec-l2l  
tunnel-group 192.168.30.1 general-attributes  
  default-group-policy  
  
demo_gp_192.168.30.1
```

```
tunnel-group 192.168.30.1 ipsec-attributes  
  ikev2 remote-authentication pre-shared-key *****  
  ikev2 local-authentication pre-shared-key *****
```

Passaggio 14. Abilitare IKEv2 sull'interfaccia esterna.

```
crypto ikev2 enable outside
```

Passaggio 15. Creare il tunnel virtuale.

```
<#root>
```

```
interface Tunnel1  
  nameif demovti_asa  
  ip address 169.254.10.2 255.255.255.0  
  tunnel source interface outside  
  tunnel destination 192.168.30.1  
  tunnel mode ipsec ipv4  
  tunnel protection ipsec profile  
  
demo_ipsec_profile
```

Passaggio 16. Creare una route statica.

```
route demovti_asa 192.168.10.0 255.255.255.0 169.254.10.1 1  
route demovti_asa 192.168.20.0 255.255.255.0 169.254.10.1 1  
route outside 0.0.0.0 0.0.0.0 192.168.40.3 1
```

Verifica

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

Passaggio 1. Passare alla CLI di FTD e ASA 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

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

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

IKEv2 SAs:

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

```
Tunnel-id Local Remote
32157565 192.168.30.1/500 192.168.40.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/67986 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: 0x4cf55637/0xa493cc83
```

```
ftdv742# show crypto ipsec sa
interface: demovti
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.1
```

```
Protected vrf (ivrf): Global
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 192.168.40.1
```

```
#pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
#pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 30, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 192.168.30.1/500, remote crypto endpt.: 192.168.40.1/500
path mtu 1500, ipsec overhead 94(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: A493CC83
current inbound spi : 4CF55637
```

```
inbound esp sas:
spi: 0x4CF55637 (1291146807)
SA State: active
transform: esp-aes-256 esp-sha-512-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, VTI, }
slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4055040/16867)
IV size: 16 bytes
```

```
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
outbound esp sas:
spi: 0xA493CC83 (2761149571)
SA State: active
transform: esp-aes-256 esp-sha-512-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, VTI, }
slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4285440/16867)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001
```

ASA:

```
ASA9203# show crypto ikev2 sa
```

```
IKEv2 SAs:
```

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

```
Tunnel-id Local Remote
26025779 192.168.40.1/500 192.168.30.1/500
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/68112 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: 0xa493cc83/0x4cf55637
```

```
ASA9203#
```

```
ASA9203# show cry
```

```
ASA9203# show crypto ipsec sa
```

```
interface: demovti_asa
```

```
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.40.1
```

```
Protected vrf (ivrf): Global
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
current_peer: 192.168.30.1
```

```
#pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
#pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 30, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 192.168.40.1/500, remote crypto endpt.: 192.168.30.1/500
path mtu 1500, ipsec overhead 94(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 4CF55637
current inbound spi : A493CC83
```

```

inbound esp sas:
  spi: 0xA493CC83 (2761149571)
    SA State: active
    transform: esp-aes-256 esp-sha-512-hmac no compression
    in use settings ={L2L, Tunnel, IKEv2, VTI, }
    slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1
    sa timing: remaining key lifetime (kB/sec): (4101120/16804)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
      0x00000000 0x00000001
outbound esp sas:
  spi: 0x4CF55637 (1291146807)
    SA State: active
    transform: esp-aes-256 esp-sha-512-hmac no compression
    in use settings ={L2L, Tunnel, IKEv2, VTI, }
    slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1
    sa timing: remaining key lifetime (kB/sec): (4055040/16804)
    IV size: 16 bytes
    replay detection support: Y
    Anti replay bitmap:
      0x00000000 0x00000001

```

Passaggio 2. Verificare il percorso di VRF e Global su 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
SI    192.168.10.0 255.255.255.0 [1/0] is directly connected, inside_red
SI    192.168.20.0 255.255.255.0 [1/0] is directly connected, inside_blue
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

```

```
ftdv742# show route vrf vrf_blue
```

```
Routing Table: vrf_blue
```

```

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 not set

```
C      192.168.20.0 255.255.255.0 is directly connected, inside_blue
L      192.168.20.1 255.255.255.255 is directly connected, inside_blue
SI     192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti
```

ftdv742# show route vrf vrf_red

Routing Table: vrf_red

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 not set

```
C      192.168.10.0 255.255.255.0 is directly connected, inside_red
L      192.168.10.1 255.255.255.255 is directly connected, inside_red
SI     192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti
```

Passaggio 3. Verificare il test ping.

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

Nell'esempio, il tunnel 1 mostra 30 pacchetti per l'incapsulamento e la decapsulamento.

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
    #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
ftdv742#
```

Client1 ping Client3 riuscito.

```
Client1#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 = 5/299/620 ms
```

Client2 ping Client3 riuscito.

```
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 = 11/297/576 ms
```

Controllare i contatori di `show crypto ipsec sa | inc interfaccia:|encap|decap` su FTD dopo il ping riuscito.

Nell'esempio, il tunnel 1 mostra 40 pacchetti per l'incapsulamento e la decapsulamento dopo un ping riuscito. Inoltre, entrambi i contatori sono aumentati di 10 pacchetti, in modo da soddisfare le 10 richieste echo del ping, a indicare che il traffico ping ha superato correttamente il tunnel IPsec.

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
    #pkts encaps: 40, #pkts encrypt: 40, #pkts digest: 40
    #pkts decaps: 40, #pkts decrypt: 40, #pkts verify: 40
    #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 utilizzare questi comandi di debug per risolvere i problemi relativi alla 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 route.

```
debug ip routing
```

Riferimento

[Guida alla configurazione di Cisco Secure Firewall Device Manager, versione 7.4](#)

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).