

Configurazione di due VTI ISP su FTD Gestito da FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti di base](#)

[Componenti usati](#)

[Configurazioni su FMC](#)

[Configurazione topologia](#)

[Configurazione degli endpoint](#)

[Configurazione IKE](#)

[Configurazione IPSec](#)

[Configurazione del routing](#)

Introduzione

In questo documento viene descritta la distribuzione di una configurazione con due ISP utilizzando le interfacce tunnel virtuali su un dispositivo FTD gestito da FMC.

Prerequisiti

Requisiti di base

- Una conoscenza di base delle VPN da sito a sito sarebbe vantaggiosa. Questo background aiuta a comprendere il processo di configurazione della VTI, inclusi i concetti e le configurazioni chiave coinvolti.
- È essenziale comprendere i fondamenti della configurazione e della gestione delle VTI sulla piattaforma Cisco Firepower. Ciò comprende la conoscenza del funzionamento delle VTI all'interno dell'FTD e del modo in cui sono controllate tramite l'interfaccia FMC.

Componenti usati

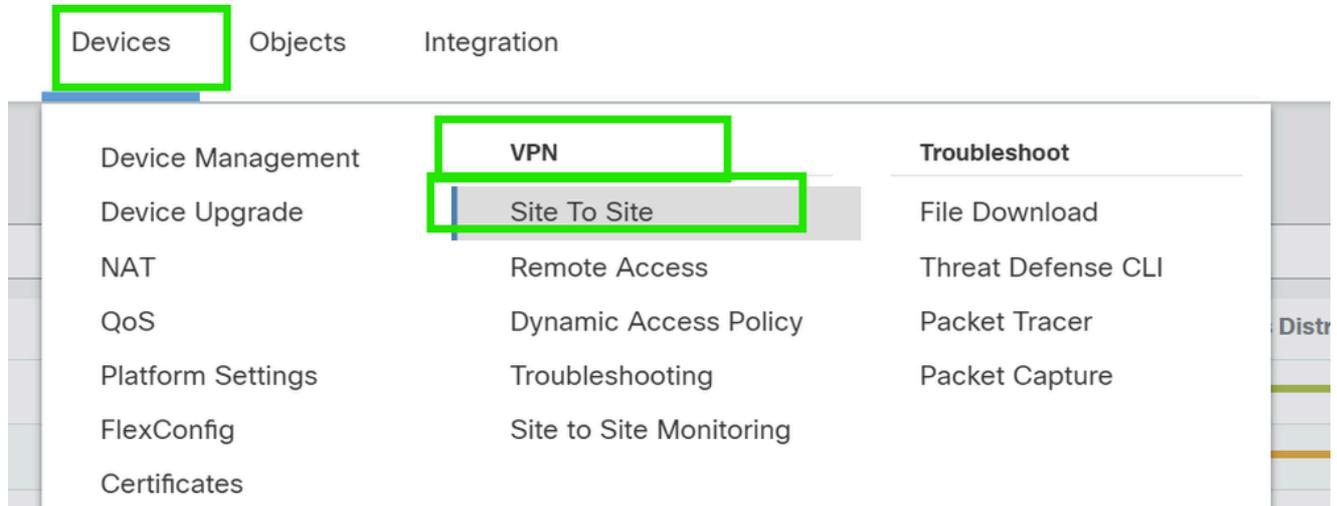
- Cisco Firepower Threat Defense (FTD) per VMware: versione 7.0.0
- Firepower Management Center (FMC): versione 7.2.4 (build 169)

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.

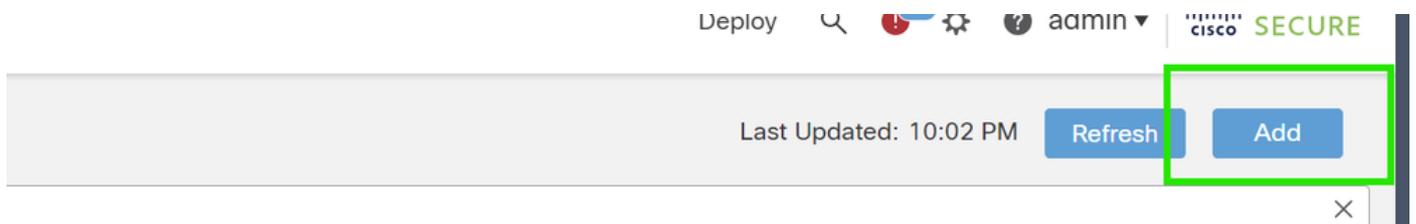
Configurazioni su FMC

Configurazione topologia

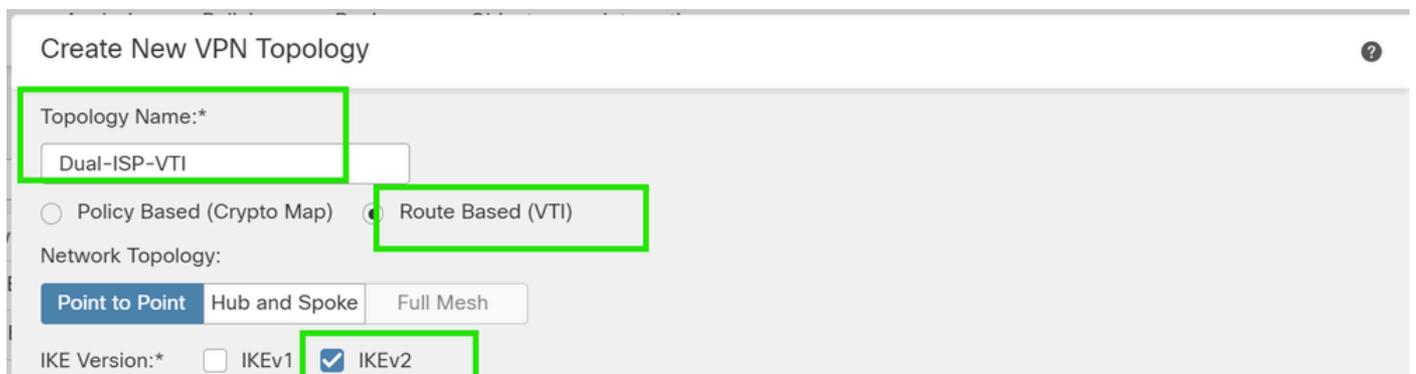
1. Passare a Dispositivi >VPN > Da sito a sito.



2. Fare clic su Aggiungi per aggiungere la topologia VPN.



3. Assegnare un nome alla topologia, scegliere VTI e Point-to-Point, quindi selezionare una versione IKE (in questo caso IKEv2).



Configurazione degli endpoint

1. Scegliere il dispositivo su cui configurare il tunnel.

Aggiungere i dettagli del peer remoto.

È possibile aggiungere una nuova interfaccia di modello virtuale facendo clic sull'icona "+" oppure selezionarne una dall'elenco esistente.

The screenshot shows the configuration page for an IPsec peer. At the top, there are tabs for 'Endpoints', 'IKE', 'IPsec', and 'Advanced'. The 'Endpoints' tab is selected. The configuration is divided into two main sections: 'Node A' and 'Node B', each enclosed in a green box.

Node A configuration:

- Device*: New_FTD (dropdown menu)
- Virtual Tunnel Interface*: [empty] (dropdown menu) with a '+' icon to its right.
- Tunnel Source IP is Private [Edit VTI](#)
- Send Local Identity to Peers
- [+ Add Backup VTI \(optional\)](#)
- Connection Type*: Bidirectional (dropdown menu)

Node B configuration:

- Device*: Extranet (dropdown menu)
- Device Name*: VTI-Peer (text input)
- Endpoint IP Address*: 10.10.10.2 (text input)

At the bottom right of the page, there are two buttons: 'Cancel' and 'Save'.

Se si sta creando una nuova interfaccia VTI, aggiungere i parametri corretti, attivarla e fare clic su "OK".

NOTA: questa diventa la VTI principale.

Add Virtual Tunnel Interface



General

Name:*

VTI-1

Enabled

Description:

This is the primary VTI tunnel.
This VTI goes through ISP 1.

Security Zone:

OUT

Priority:

0

(0 - 65535)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*

1

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/0 (outside1)

10.106.52.104

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

IPv4 IPv6

192.168.10.1/30



Cancel

OK

3. Fare clic su "+ ". Add Backup VIT" (Aggiungi VIT di backup) per aggiungere una VIT secondaria.

Device:*

10.106.50.55 ▼

Virtual Tunnel Interface:*

VTI-1 (IP: 192.168.10.1) ▼ +

Tunnel Source: outside1 (IP: 10.106.52.104) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

+ Add Backup VTI (optional)

Connection Type:*

Bidirectional ▼

Additional Configuration ⓘ

Route traffic to the VTI : [Routing Policy](#)

Permit VPN traffic : [AC Policy](#)

4. Fare clic su "+" per aggiungere il parametro per la VTI secondaria (se non è già stato configurato).

10.106.50.55 ▼

Virtual Tunnel Interface:*

VTI-1 (IP: 192.168.10.1) ▼



Tunnel Source: outside1 (IP: 10.106.52.104) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Backup VTI:

[Remove](#)

Virtual Tunnel Interface:*

▼



Tunnel Source IP is Private

[Edit VTI](#)

Send Local Identity to Peers

Connection Type:*

5. Se si sta creando una nuova interfaccia VTI, aggiungere i parametri corretti, abilitarla e fare clic su "OK".

NOTA: questa diventa la VTI secondaria.

Add Virtual Tunnel Interface



General

Name:

VTI-2

Enabled

Description:

This is the secondary VTI tunnel..
VTI goes through ISP 2.

Security Zone:

OUT

Priority:

0

(0 - 65535)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*

2

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/1 (outside2)

10.106.53.10

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

IPv4 IPv6

192.168.20.1/30



Cancel

OK

Configurazione IKE

1. Passare alla scheda IKE. È possibile scegliere di utilizzare un criterio predefinito oppure fare clic sul pulsante a forma di matita accanto alla scheda Criterio per crearne uno nuovo oppure selezionare un altro criterio disponibile in base alle proprie esigenze.

Endpoints **IKE** IPsec Advanced

Authentication Type: Pre-shared Automatic Key

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

IKEv2 Settings

Policies:* AES-GCM-NULL-SHA-LATEST 

Authentication Type: Pre-shared Automatic Key

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

Cancel Save

IKEv2 Policy ?

Available IKEv2 Policy  

- AES-GCM-NULL-SHA
- AES-GCM-NULL-SHA-LAT...
- AES-SHA-SHA
- AES-SHA-SHA-LATEST
- Arko_Test_IKEv2
- DES-SHA-SHA

Add

Selected IKEv2 Policy

AES-GCM-NULL-SHA-LATEST 

Cancel OK

2. Selezionare il tipo di autenticazione. Se viene utilizzata una chiave manuale già condivisa, specificare la chiave nelle caselle Chiave e Conferma chiave.

Endpoints **IKE** IPsec Advanced

IKEv2 Settings

Policies:* AES-GCM-NULL-SHA-LATEST 

Authentication Type: Pre-shared Manual Key ▼

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Cancel Save

Configurazione IPsec

Passare alla scheda IPsec. È possibile scegliere di utilizzare una proposta predefinita facendo clic sul pulsante a matita accanto alla scheda proposta per crearne una nuova oppure selezionare un'altra proposta disponibile in base alle proprie esigenze.

Endpoints IKE **IPsec** Advanced

IKEv2 Mode: Tunnel ▼

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

tunnel_aes256_sha AES-GCM

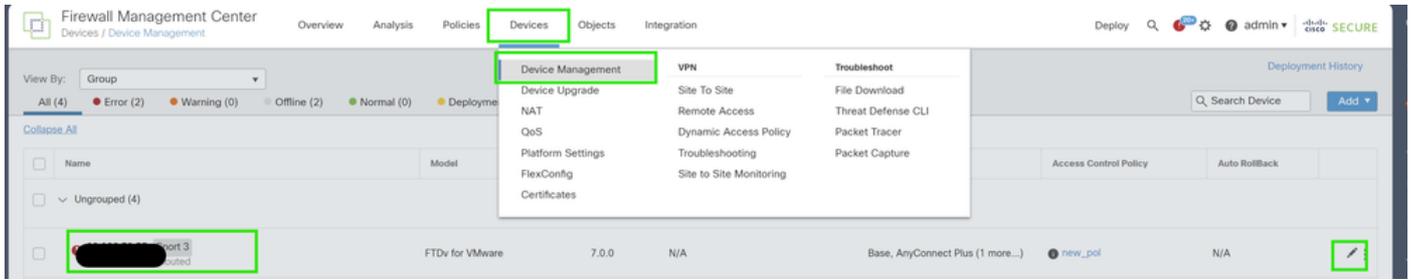
Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

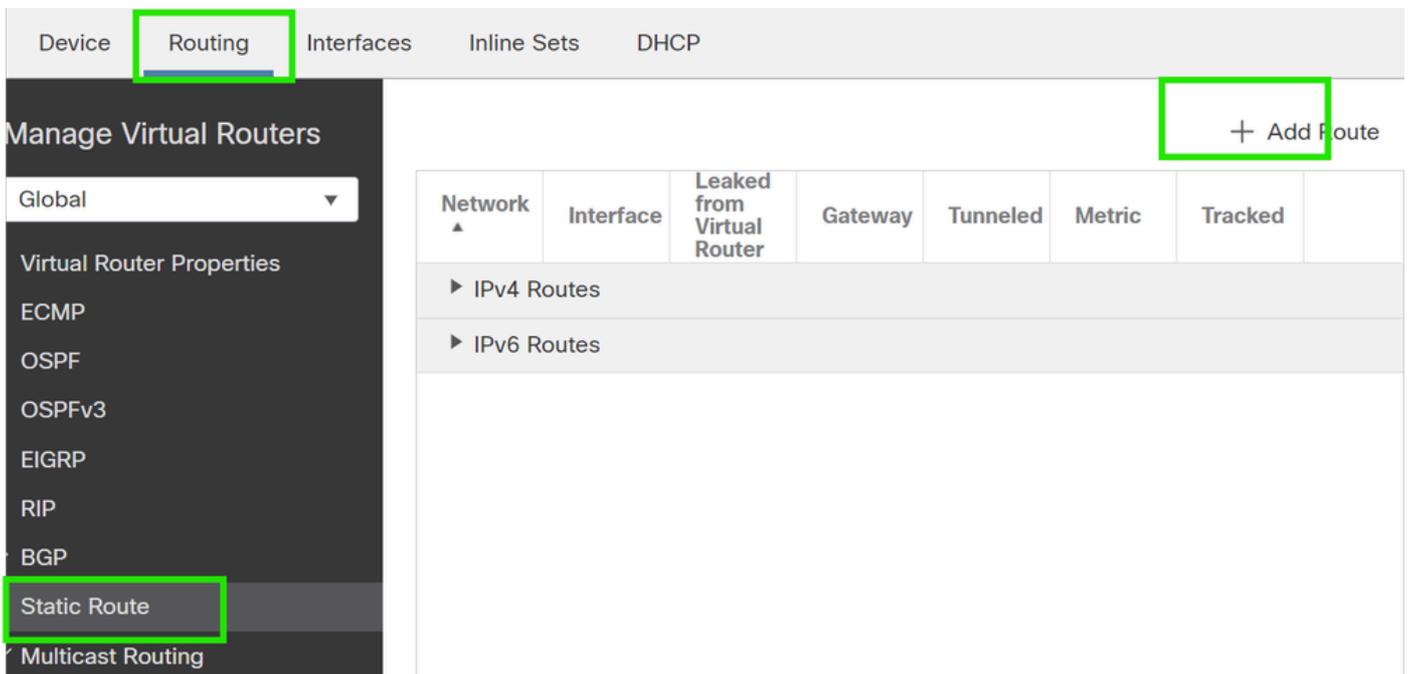
Configurazione del routing

1. Selezionare Device > Device Management e fare clic sull'icona a forma di matita per modificare il dispositivo (FTD).



2. Andare a Intradamento > Intradamento statico e fare clic sul pulsante "+" per aggiungere un instradamento alla VTI principale e secondaria.

NOTA: è possibile configurare il metodo di routing appropriato affinché il traffico passi attraverso l'interfaccia del tunnel. In questo caso, sono state utilizzate route statiche.



3. Aggiungere due route per la rete protetta e impostare un valore AD superiore (in questo caso 2) per la route secondaria.

La prima route utilizza l'interfaccia VTI-1, la seconda l'interfaccia VTI-2.

Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric
▼ IPv4 Routes					
protected-network	VTI-1	Global	VTI-1-Gateway	false	1
protected-network	VTI-2	Global	VTI-2-Gateway	false	2

Verifica

1. Accedere a Dispositivi > VPN > Monitoraggio da sito a sito .

Devices

Objects

Integration

Device Management

Device Upgrade

NAT

QoS

Platform Settings

FlexConfig

Certificates

VPN

Site To Site

Remote Access

Dynamic Access Policy

Troubleshooting

Site to Site Monitoring

Troubleshoot

File Download

Threat Defense CLI

Packet Tracer

Packet Capture

2. Fai clic sull'occhio per controllare ulteriori dettagli sullo stato del tunnel.



View full information

Dual-ISP-VTI

Active

2024-06-11 06:55:26

Dual-ISP-VTI

Active

2024-06-12 14:27:22

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).