

Configureer de dubbele ISP VTI op FTD die door FMC wordt beheerd

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Basisvereisten](#)

[Gebruikte componenten](#)

[Configuraties op VCC](#)

[Configuratie van topologie](#)

[Endpoint configuratie](#)

[IKE-configuratie](#)

[IPsec-configuratie](#)

[Routingconfiguratie](#)

Inleiding

Dit document beschrijft de implementatie van dubbele ISP-instellingen met behulp van virtuele tunnelinterfaces op een FTD-apparaat dat door FMC wordt beheerd.

Voorwaarden

Basisvereisten

- Een fundamenteel begrip van site-to-site VPN's zou nuttig zijn. Deze achtergrond helpt bij het begrijpen van het VTI setup proces, inclusief de belangrijkste concepten en configuraties die erbij betrokken zijn.
- De basiskennis over het configureren en beheren van VTI's op het Cisco Firepower platform is essentieel. Dit omvat kennis over de werking van VTI's in het FTD en over de wijze waarop zij via de FMC-interface worden bestuurd.

Gebruikte componenten

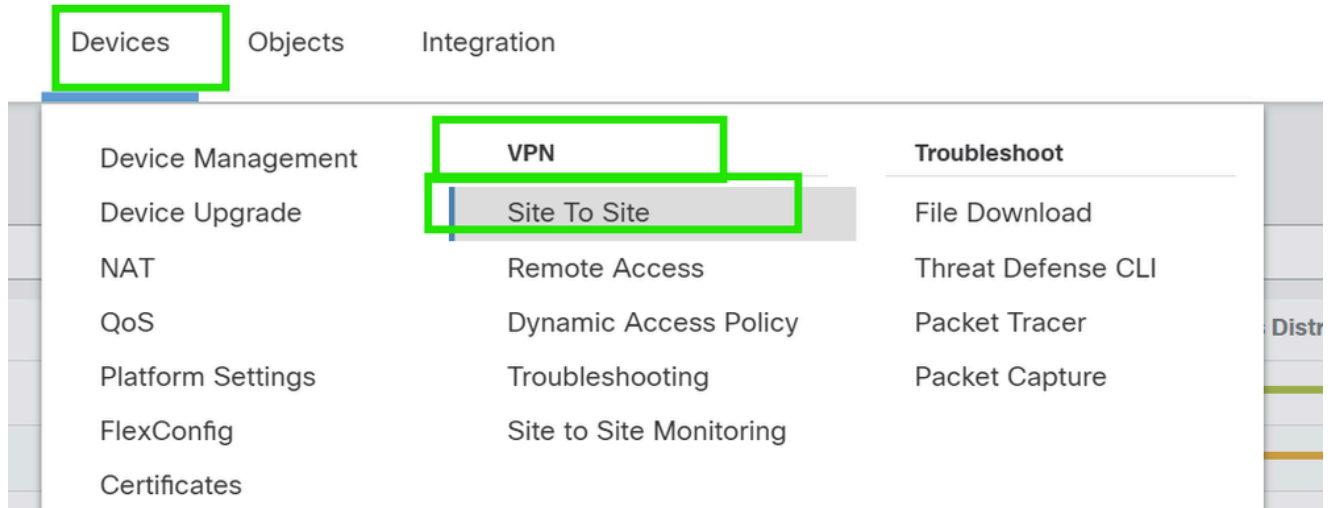
- Cisco Firepower Threat Defence (FTD) voor VMware: versie 7.0.0
- Firepower Management Center (FMC): versie 7.2.4 (build 169)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

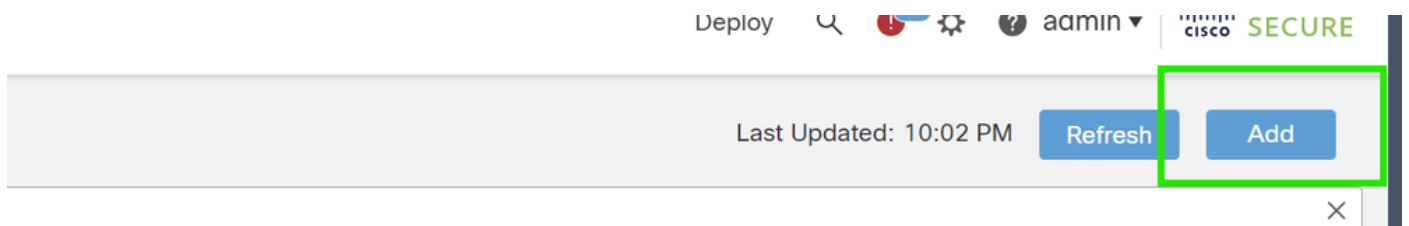
Configuraties op VCC

Configuratie van topologie

1. Ga naar Apparaten > VPN > Site to Site.



2. Klik op Add om VPN-topologie toe te voegen.



3. Geef een naam voor de topologie, kies VTI en Point-to-Point, en selecteer een IKE-versie (in dit geval IKEv2).



Endpoint configuratie

1. Kies het apparaat waarop de tunnel moet worden geconfigureerd.

Voeg de externe peer details toe.

U kunt een nieuwe virtuele sjablooninterface toevoegen door op het pictogram "+" te klikken of een van de bestaande lijst selecteren.

Endpoints IKE IPsec Advanced

Node A

Device:*
New_FTD

Virtual Tunnel Interface:*
 [] +

Tunnel Source IP is Private [Edit VTI](#)

Send Local Identity to Peers

[+ Add Backup VTI \(optional\)](#)

Connection Type:*
Bidirectional

Node B

Device:*
Extranet

Device Name*:
VTI-Peer

Endpoint IP Address*:
10.10.10.2

Cancel Save

Als u een nieuwe VTI-interface maakt, voegt u de juiste parameters toe, schakelt u deze in en klikt u op "OK".

LET OP: dit wordt de primaire VTI.

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. Klik op "+ ". Back-up VIT toevoegen" om een tweede VIT toe te voegen.

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 [i](#)

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

Permit VPN traffic : [AC Policy](#)

4. Klik op '+' om een parameter toe te voegen voor secundaire VTI (indien niet reeds geconfigureerd).

Endpoints IKE IPsec Advanced

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. Als u een nieuwe VTI-interface maakt, voegt u de juiste parameters toe, schakelt u deze in en klikt u op "OK".

LET OP: dit wordt de secundaire VTI.

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

IKE-configuratie


1. Navigeren naar het tabblad IKE. U kunt ervoor kiezen om een vooraf bepaald beleid te gebruiken, klik op de potloodknop naast het tabblad Beleid om een nieuw beleid te maken of selecteer een ander beschikbaar beleid dat is gebaseerd op uw behoefte.

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. Selecteer het verificatietype. Als een vooraf gedeelde handmatige toets wordt gebruikt, specificeert u de toets in de vakjes Sleutel en Bevestig de toets.

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

IPsec-configuratie

Ga naar het tabblad IPsec. U kunt ervoor kiezen om een vooraf gedefinieerd voorstel te gebruiken door op de potloodknop naast het tabblad voorstel te klikken om een nieuw voorstel te maken of een ander beschikbaar voorstel te selecteren op basis van uw vereiste.

IKEv2 Mode: Tunnel ▼

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

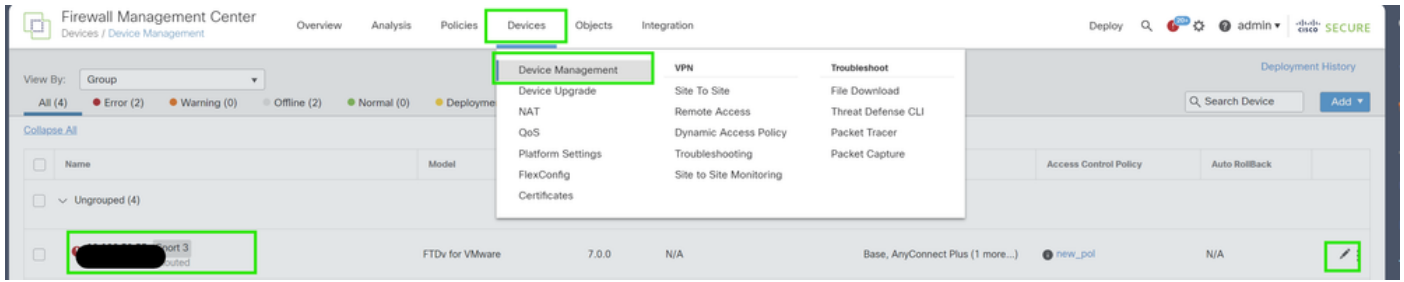
tunnel_aes256_sha

AES-GCM

- Enable Security Association (SA) Strength Enforcement
- Enable Reverse Route Injection
- Enable Perfect Forward Secrecy

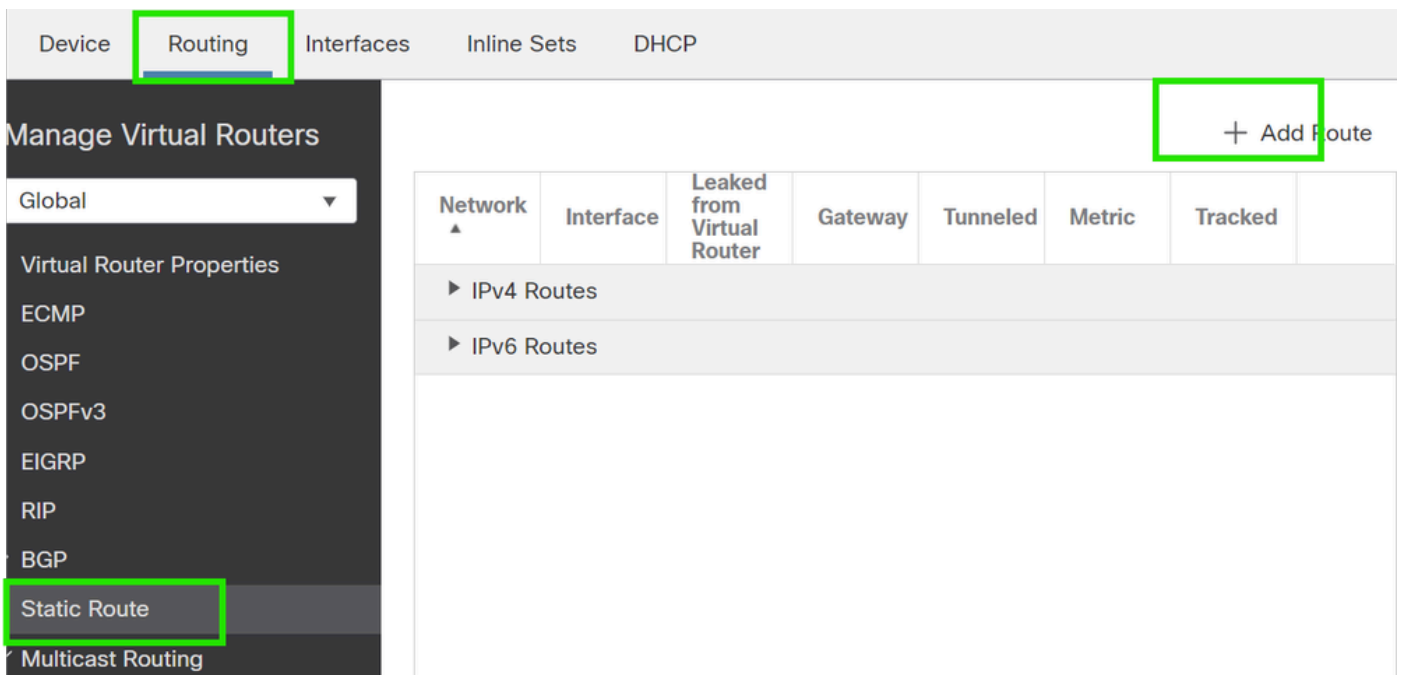
Routingconfiguratie

1. Ga naar Apparaat > Apparaatbeheer en klik op het potloodpictogram om het apparaat (FTD) te bewerken.



2. Ga naar Routing > Statische Route en klik op de knop "+" om een route toe te voegen aan het primaire en secundaire VTI.

OPMERKING: U kunt de juiste routeringsmethode voor uw verkeer configureren om door de tunnelinterface te gaan. In dit geval zijn statische routes gebruikt.



3. Voeg twee routes toe voor uw beveiligd netwerk en stel een hogere AD-waarde (in dit geval 2) in voor de secundaire route.

De eerste route gebruikt de VTI-1 interface, en de tweede gebruikt de VTI-2 interface.

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

Verifiëren

1. Ga naar Apparaten > VPN > Site to Site Monitoring .

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. Klik op het oog om meer details over de status van de tunnel te controleren.

	Dual-ISP-VTI	Active	2024-06-11 06:55:26
View full information	Dual-ISP-VTI	Active	2024-06-12 14:27:22

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.