

Configureer VRF-bewuste routegebaseerde site-to-site VPN op FTD beheerde via FDM

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Het FTD configureren](#)

[ASA configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Referentie](#)

Inleiding

Dit document beschrijft hoe u VRF-bewuste route-gebaseerde site-to-site VPN kunt configureren op basis van FTD die wordt beheerd door FDM.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van VPN
- Basis begrip van Virtual Routing and Forwarding (VRF)
- Ervaring met FDM

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco FTDv versie 7.4.2
- Cisco FDM versie 7.4.2
- Cisco ASA v versie 9.20.3

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.

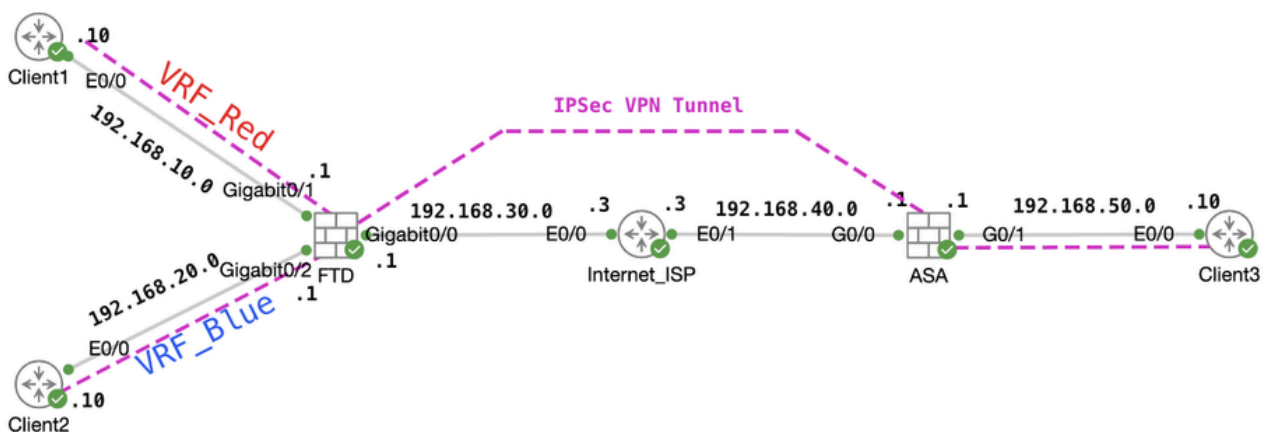
Achtergrondinformatie

Met Virtual Routing and Forwarding (VRF) op Firepower Device Manager (FDM) kunt u meerdere geïsoleerde routing-instanties maken op één FTD-apparaat (Firepower Threat Defence). Elke VRF-instantie werkt als een afzonderlijke virtuele router met een eigen routingstapel, wat een logische scheiding van netwerkverkeer mogelijk maakt en verbeterde beveiliging en mogelijkheden voor verkeersbeheer biedt.

Dit document legt uit hoe u VRF-bewuste IPSec VPN met VTI kunt configureren. VRF Rood netwerk en VRF Blauw netwerk zijn achter FTD. Client1 in VRF Rood netwerk en Client2 in VRF Blauw zou communiceren met client 3 achter ASA via de IPSec VPN-tunnel.

Configureren

Netwerkdigram

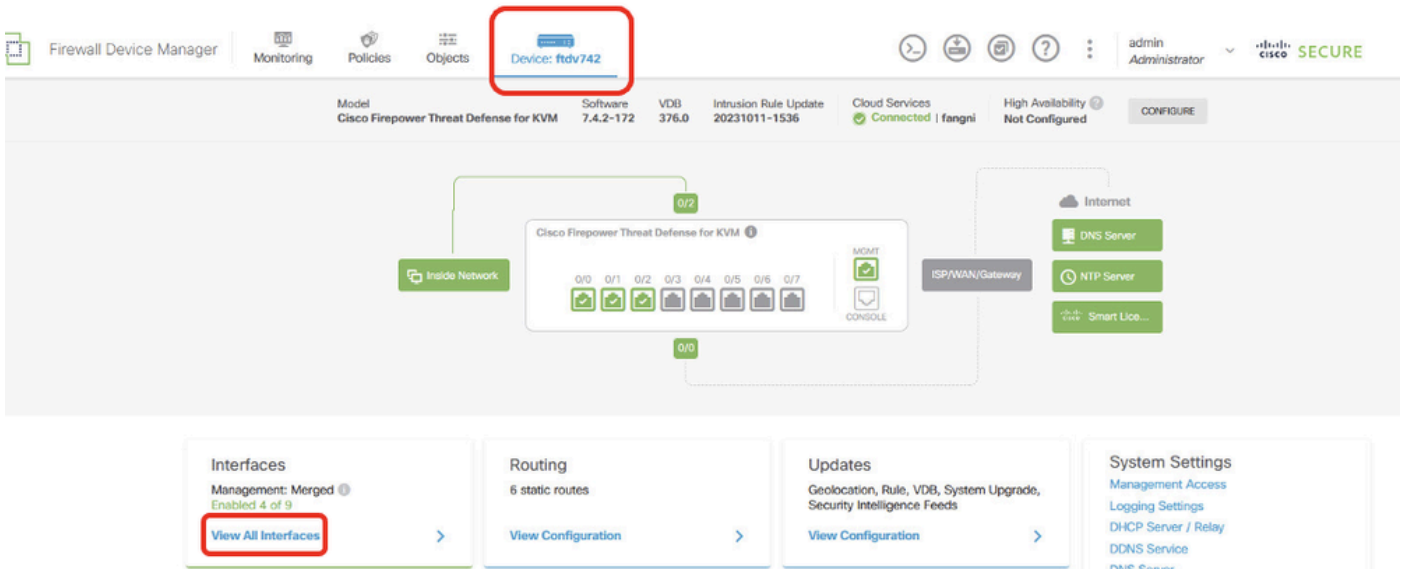


Topologie

Het FTD configureren

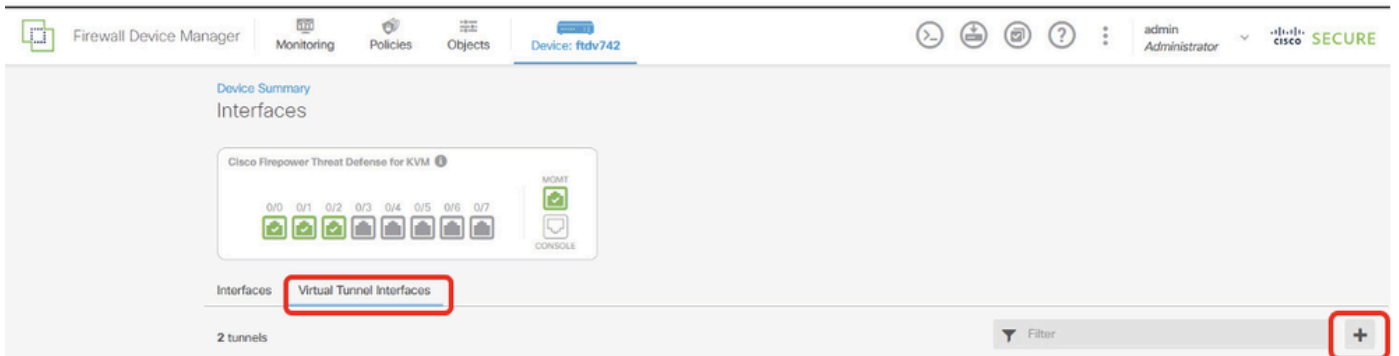
Stap 1. Het is van essentieel belang dat de voorlopige configuratie van IP-interconnectiviteit tussen knooppunten naar behoren is voltooid. Client1 en Client2 zijn met FTD Inside IP adres als gateway. Client3 is met ASA binnen IP adres als gateway.

Stap 2. Maak een virtuele tunnelinterface. Login in de FDM GUI van FTD. Navigeer naar apparaat > Interfaces . Klik op Alle interfaces weergeven .



FTD_View_interfaces

Stap 2.1. Klik op het tabblad Virtuele tunnelinterfaces. Klik op + knop.



FTD_Creatie_VTI

Stap 2.2. Verstrek de nodige informatie. Klik op de knop OK.

- Naam: demovti
- Tunnel-ID: 1
- Tunnelbron: buiten (Gigabit Ethernet0/0)
- IP-adres en subnetmasker: 169.254.10.1/24
- Status: klik op de schuifschakelaar om de positie Ingeschakeld te selecteren

Name
demovti

Status

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

Description

Tunnel ID ⓘ
1
0 - 10413

Tunnel Source ⓘ
outside (GigabitEthernet0/0)

IP Address and Subnet Mask
169.254.10.1 / 24

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

CANCEL

OK

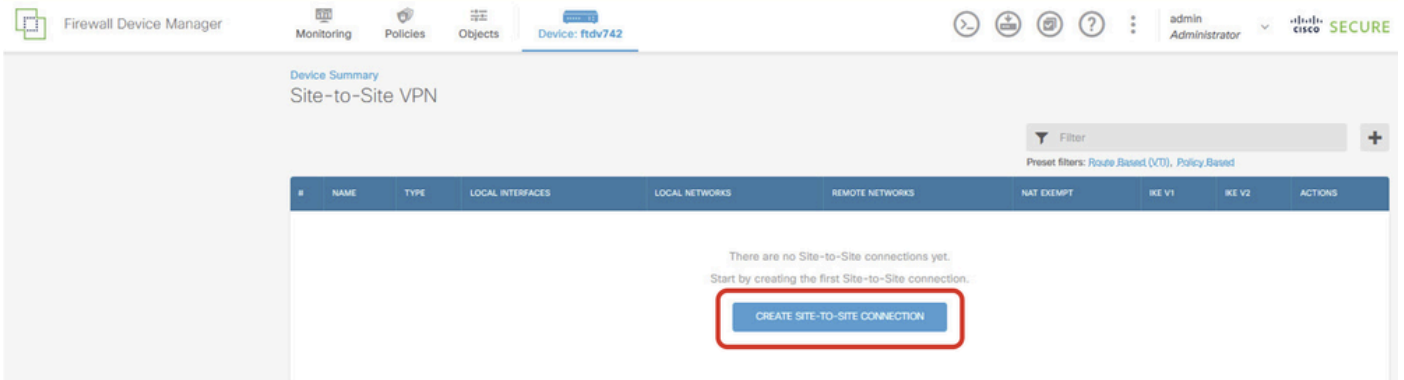
FTD_Create_VTI_Details

Step 3. Navigeer naar apparaat > Site-to-Site VPN . Klik op de knop Configuratie bekijken.



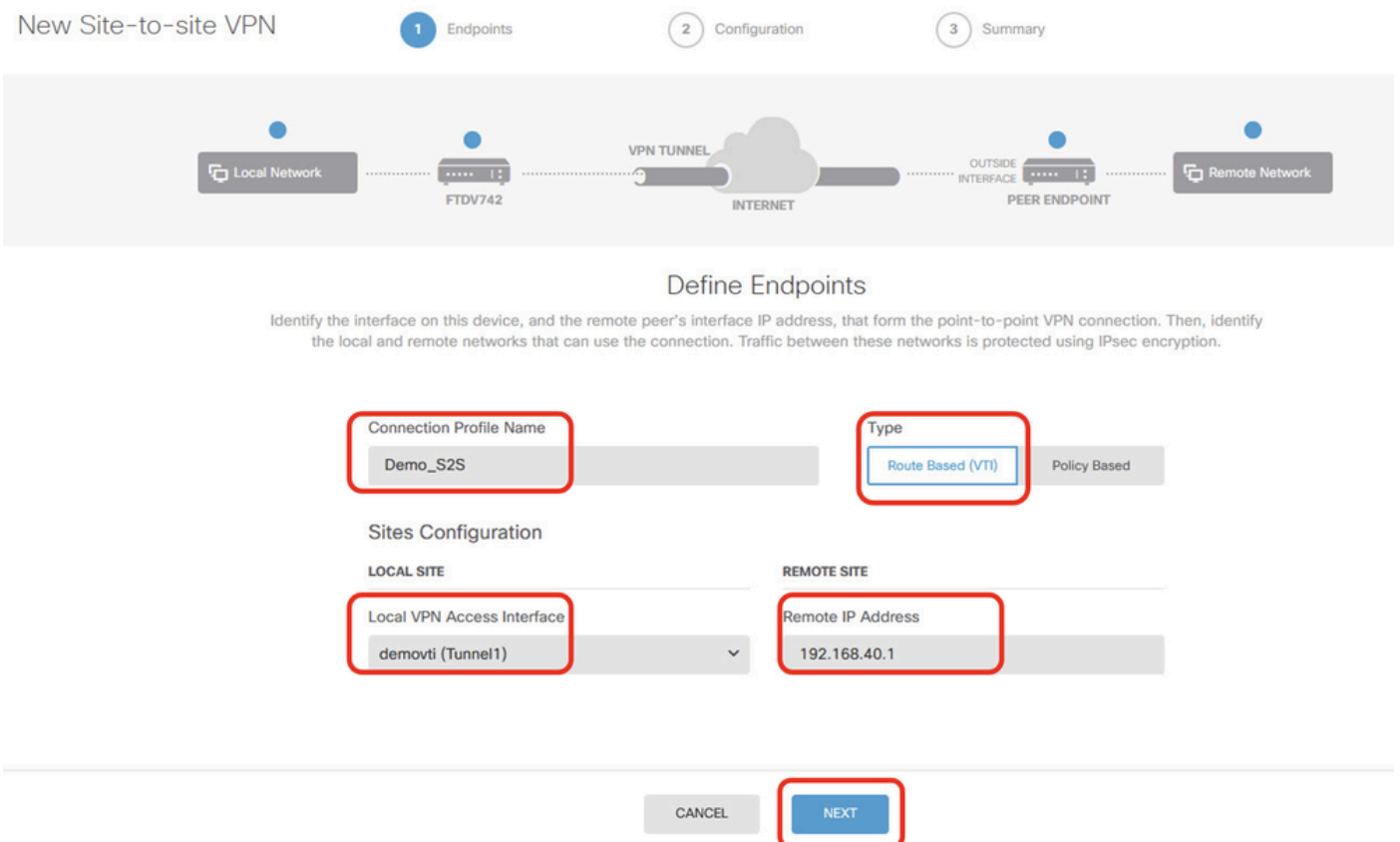
Interfaces Management: Merged ⓘ Enabled 4 of 9 View All Interfaces >	Routing 1 static route View Configuration >	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration >	System Settings Management Access Logging Settings DHCP Server / Relay DDNS Service DNS Server Hostname Time Services SSL Settings See more
Smart License Registered Tier: FTDv50 - 10 Gbps View Configuration >	Backup and Restore View Configuration >	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	
Site-to-Site VPN There are no connections yet View Configuration >	Remote Access VPN Requires Secure Client License No connections 1 Group Policy Configure >	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration >	Device Administration Audit Events, Deployment History, Download Configuration View Configuration >

Stap 3.1. Start het maken van nieuwe site-to-site VPN. Klik op SITE-TO-SITE VERBINDING maken. Of klik op +.

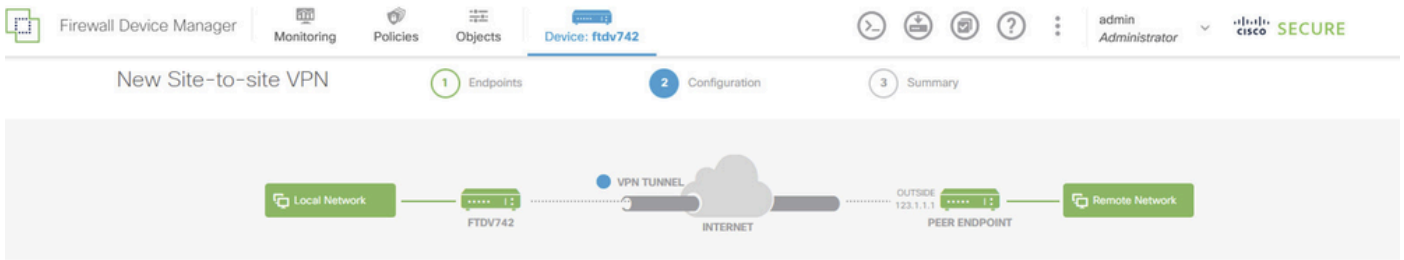


Stap 3.2. verschaffen noodzakelijke informatie. Klik op VOLGENDE knop.

- Naam verbindingsprofiel: Demo_S2S
- Type: Routegebaseerde (VTI)
- Lokale VPN-toegangsinterface: demovti (gemaakt in stap 2)
- Remote IP-adres: 192.168.40.1 (dit is peer-ASA buiten IP-adres)



Stap 3.3. Navigeren naar IKE-beleid. Klik op DE knop BEWERKEN.



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_Bewerken_IKE_Policy

Stap 3.4. Voor IKE-beleid kunt u vooraf gedefinieerde afbeeldingen gebruiken of een nieuwe maken door op te klikken Nieuw IKE-beleid maken .

In dit voorbeeld, schakel een bestaande IKE beleidsnaam AES-SHA-SHA om. Klik op OK om op te slaan.

Filter

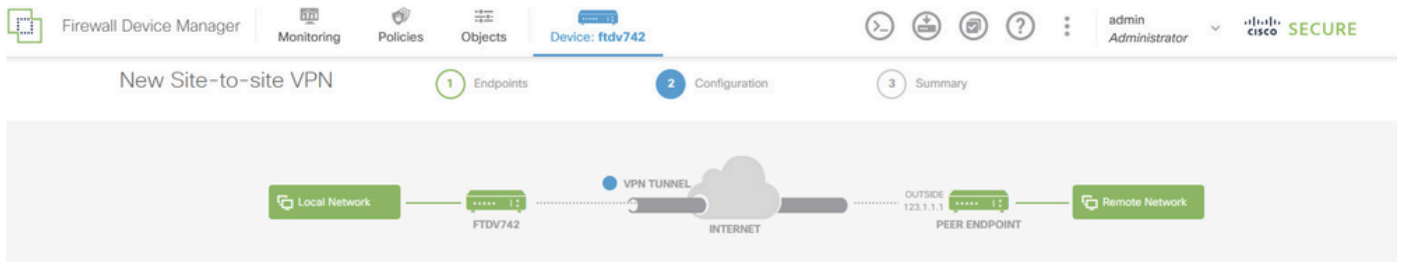
<input type="checkbox"/>	AES-GCM-NULL-SHA	i
<input checked="" type="checkbox"/>	AES-SHA-SHA	i
<input type="checkbox"/>	DES-SHA-SHA	i

Create New IKE Policy

OK

FTD_Enable_IKE_Policy

Stap 3.5. Navigeren naar het IPSec-voorstel. Klik op DE knop BEWERKEN.



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

FTD_Edit_IPSec_voorstel

Stap 3.6. Voor een IPSec-voorstel kunt u vooraf gedefinieerde bestanden gebruiken of een nieuwe maken door op Nieuw IPSec-voorstel maken te klikken.

In dit voorbeeld kunt u een bestaande naam voor een IPSec-voorstel AES-SHA omschakelen. Klik op de knop OK om op te slaan.

Select IPsec Proposals



The screenshot shows a dialog box titled "Select IPsec Proposals". At the top left is a plus sign icon. Below it is a "Filter" input field and a "SET DEFAULT" button. The main area contains a list of proposals:

- AES-GCM *In Default Set* (with an information icon)
- AES-SHA** (checked with a white checkmark, highlighted in blue, and with an information icon)
- DES-SHA-1 (with an information icon)

At the bottom, there are three buttons: "Create new IPsec Proposal" (in blue), "CANCEL", and "OK" (highlighted with a red box).

FTD_Enable_IPSec_voorstel

Stap 3.7. Scroll naar beneden op de pagina en configureer de vooraf gedeelde sleutel. Klik op VOLGENDE knop.

Let op deze vooraf gedeelde sleutel en configureer deze later op ASA.

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_Configure_Pre_Shared_Key

Stap 3.8. Controleer de VPN-configuratie. Als er iets moet worden gewijzigd, klikt u op de knop TERUG. Als alles goed is, klikt u op de knop VOLTOOIEN.

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

Stap 3.9. Maak toegangscontroleregels om verkeer door de FTD te laten passeren. In dit voorbeeld, sta allen voor demoverkeer toe. Wijzig uw beleid op basis van uw werkelijke behoeften.

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**

FTD_ACS_Voorbeeld

Stap 3.10. (Optioneel) Configureer NAT-vrijstellingsregel voor het clientverkeer op FTD als er dynamische NAT is geconfigureerd voor de client om toegang tot internet te krijgen. In dit

voorbeeld is het niet nodig om een NAT-vrijstellingsregel te configureren omdat er geen dynamische NAT op FTD is geconfigureerd.

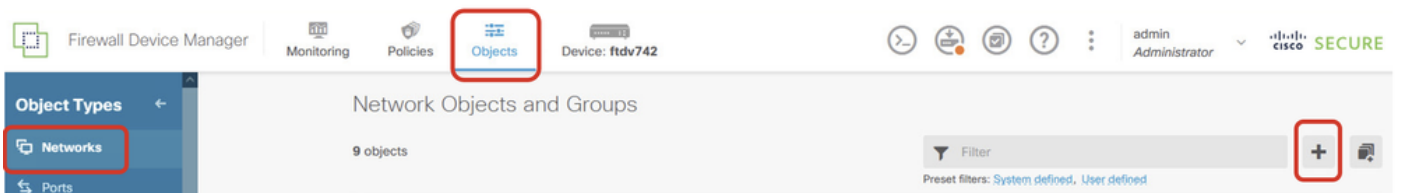
Stap 3.1. Implementeer de configuratiewijzigingen.



FTD_Implementatie_Wijzigingen

Stap 4. Virtuele routers configureren.

Stap 4.1. Maak netwerkobjecten voor statische route. Navigeer naar objecten > Netwerken en klik op +.



FTD_Create_NetObjects

Stap 4.2. Geef de benodigde informatie over elk netwerkobject. Klik op de knop OK.

- Naam: local_blue_192.168.20.0
- Type: Network
- Netwerk: 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_Blauw_Netwerk

- Naam: lokaal_rood_192.168.10.0
- Type: Network
- Network: 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_Rood_Netwerk

- Naam: afstandsbediening_192.168.50.0
- Type: Network
- Network: 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

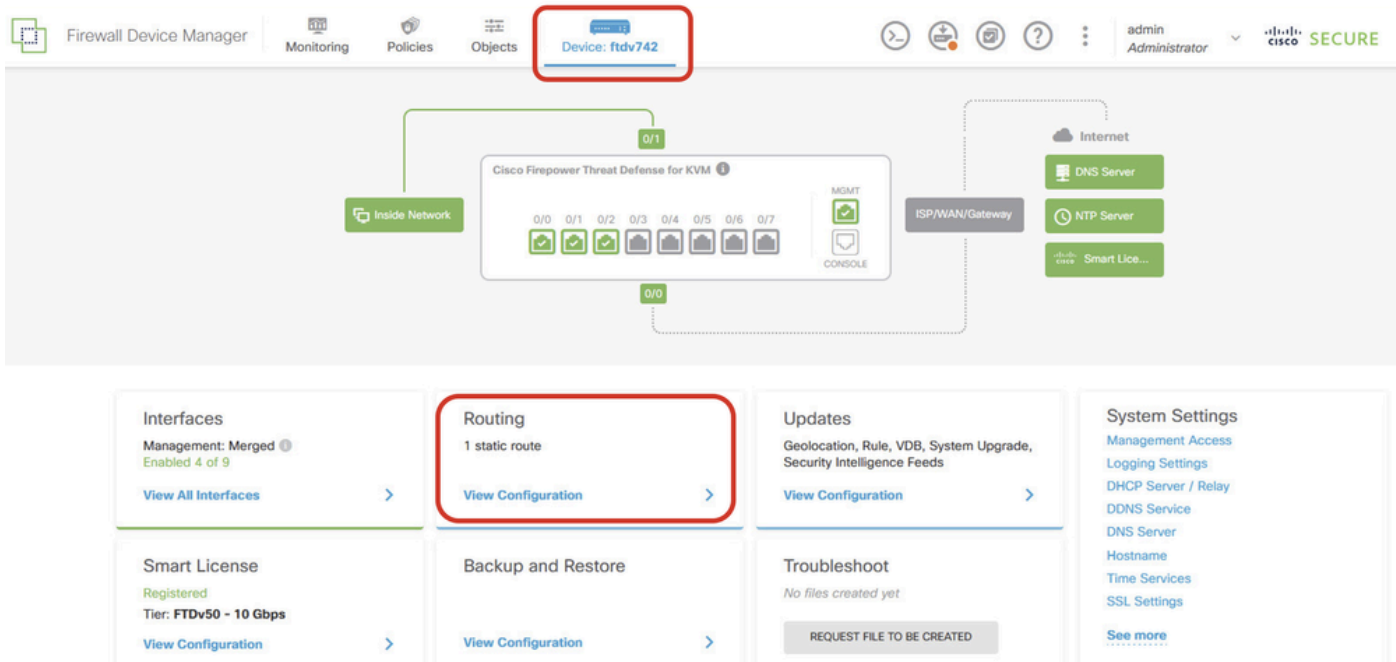
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

FTD_Remote_Network

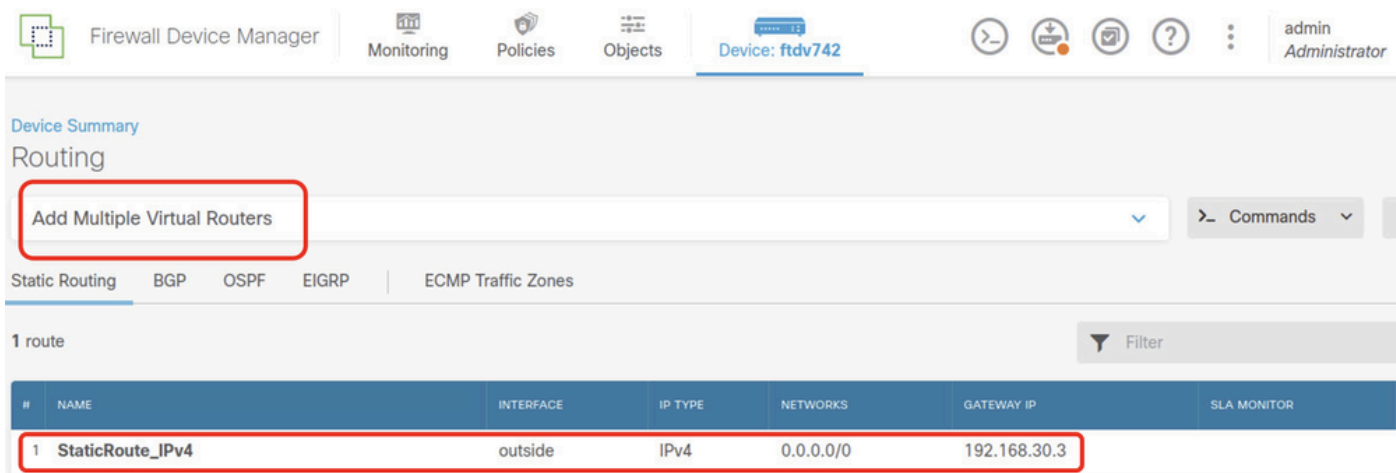
Stap 4.3. Maak de eerste virtuele router aan. Navigeer naar apparaat > routing . Klik op Configuratie weergeven .



FTD_View_Routing_Configuration

Stap 4.4. Klik op Meervoudige virtuele routers toevoegen .

Opmerking: een statische route door buiteninterface is reeds gevormd tijdens FDM initialisering. Als u het niet hebt, te configureren gelieve het handmatig.



FTD_Add_First_Virtual_Router1

Stap 4.5. Klik op EERSTE AANGEPASTE VIRTUELE ROUTER MAKEN .

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 two customer networks (e.g., CUSTOMER A NETWORK 1 and 2, CUSTOMER B NETWORK 1 and 2, etc.). A red box highlights the 'CREATE FIRST CUSTOM VIRTUAL ROUTER' button at the bottom.

Commands

FTD_Add_First_Virtual_Router2

Stap 4.6. Geef de benodigde informatie over de eerste virtuele router op. Klik op OK knop. Na de eerste virtuele routercreatie, zou een vrf naam Global automatisch worden getoond.

- Naam: Vrf_rood
- Interfaces: inside_red (Gigabit Ethernet0/1)

Firewall Device Manager

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.

Add Virtual Router

Name: vrf_red

Description:

Interfaces: Inside_red (GigabitEthernet0/1)

CANCEL OK

CREATE FIRST CUSTOM VIRTUAL ROUTER

FTD_Add_First_Virtual_Router3

Stap 4.7. Maak een tweede virtuele router. Navigeer naar apparaat > Routing . Klik op

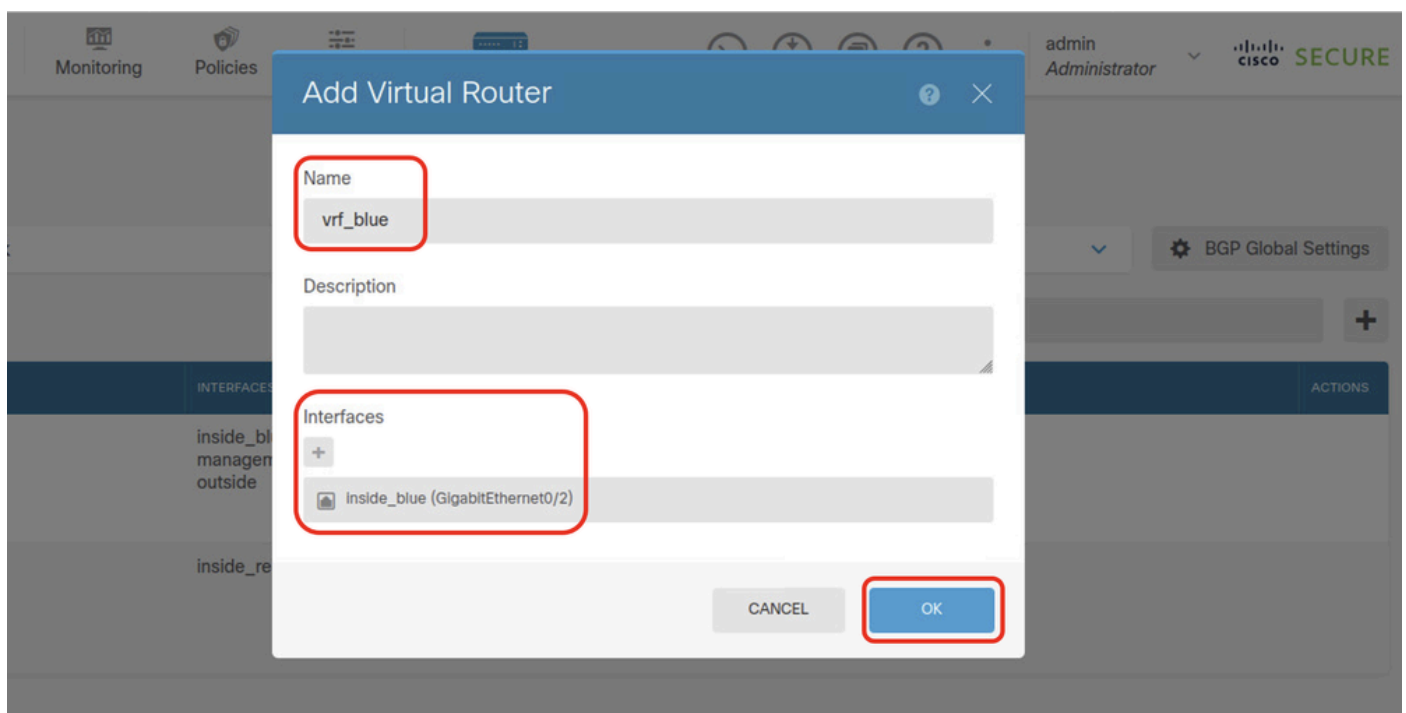
Configuratie weergeven . Klik op + knop.



FTD_Add_Second_Virtual_Router

Stap 4.8. Geef de benodigde informatie over een tweede virtuele router op. Klik op OK.

- Naam: Vrf_blauw
- Interfaces: inside_blue (Gigabit Ethernet0/2)



FTD_Add_Second_Virtual_Router2

Stap 5. Maak een lek van de route van vrf_blue naar Global. Deze route staat eindpunten op het 192.168.20.0/24 netwerk toe om verbindingen te initiëren die de site-to-site VPN-tunnel zouden doorkruisen. Dit bijvoorbeeld, beschermt het verre eindpunt het 192.168.50.0/24 netwerk.

Navigeer naar apparaat > routing . Klik op Configuratie bekijken . klik op het pictogram Weergave in de actiecel voor de virtuele router vrf_blue.

Device Summary
Virtual Routers

How Multiple Virtual Routers Work BGP Global Settings

3 virtual routers Filter +

#	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_View_VRF_Blauw

Stap 5.1. Klik op het tabblad Statische routing. Klik op + knop.

Device Summary / Virtual Routers
vrf_blue

How Multiple Virtual Routers Work Commands

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

Filter +

FTD_Creatie_Statische_Route_VRF_Blauw

Stap 5.2. Verstrek de nodige informatie. Klik op OK knop.

- Naam: Blauw_naar_ASA
- Interface: Demovti (Tunnel 1)
- Netwerken: afstandsbediening_192.168.50.0
- Gateway: Laat dit item leeg.

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 ▼

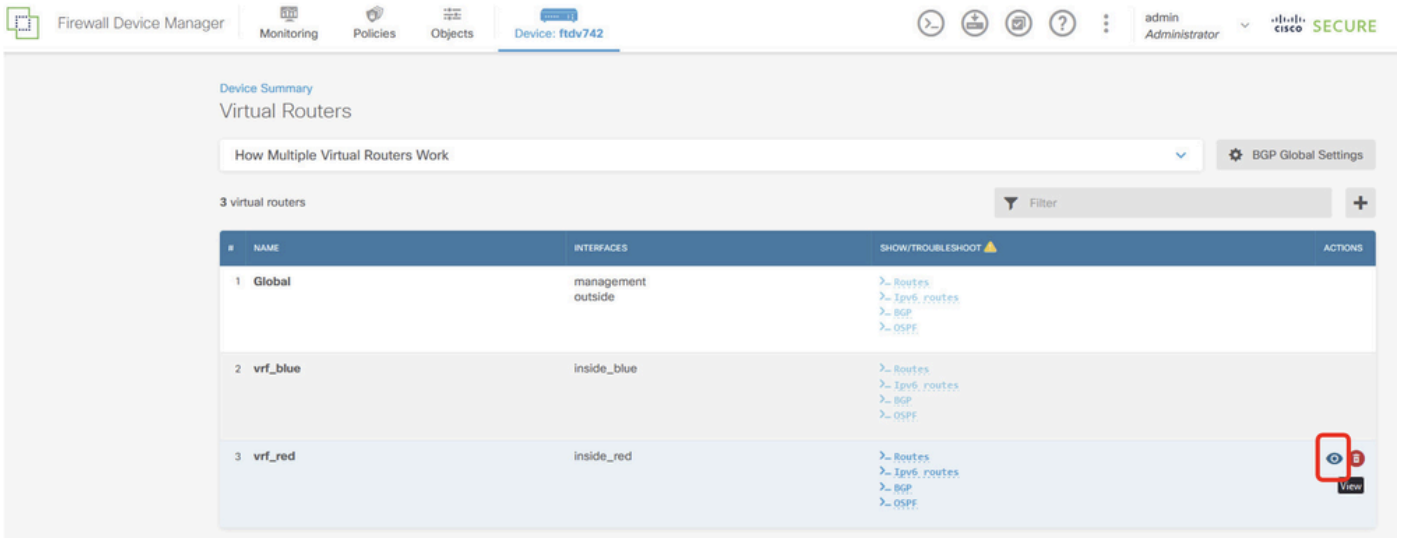
CANCEL **OK**

FTD_Create_Static_Route_VRF_Blue_Details

Stap 6. Maak routelekage van vrf_red naar Global. Deze route staat eindpunten op het 192.168.10.0/24 netwerk toe om verbindingen te initiëren die de site-to-site VPN-tunnel zouden

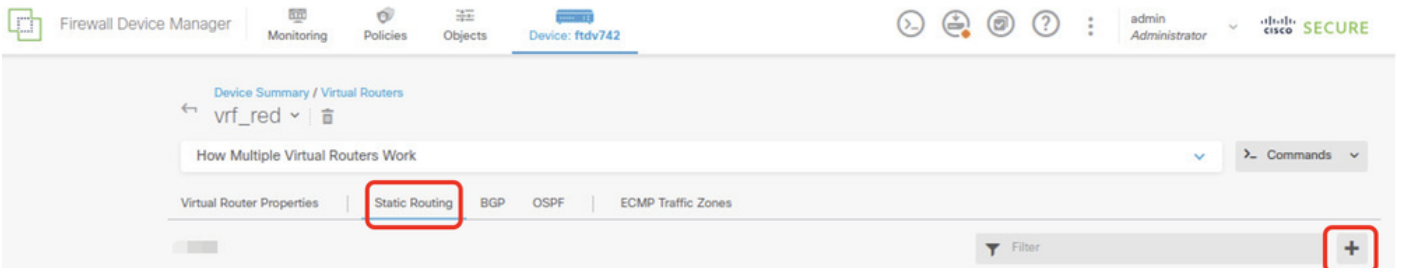
doorkruisen. Dit bijvoorbeeld, beschermt het verre eindpunt het 192.168.50.0/24 netwerk.

Navigeer naar apparaat > routing . Klik op Configuratie bekijken . klik op het pictogram Weergave in de actiecel voor de virtuele router vrf_red.



FTD_View_VRF_Rood

Stap 6.1. Klik op het tabblad Statische routing. Klik op + knop.



FTD_Creatie_Statische_Route_VRF_Rood

Stap 6.2. Verstrek de nodige informatie. Klik op OK knop.

- Naam: Rood_aan_ASA
- Interface: Demovti (Tunnel 1)
- Netwerken: afstandsbediening_192.168.50.0
- Gateway: Laat dit item leeg.

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

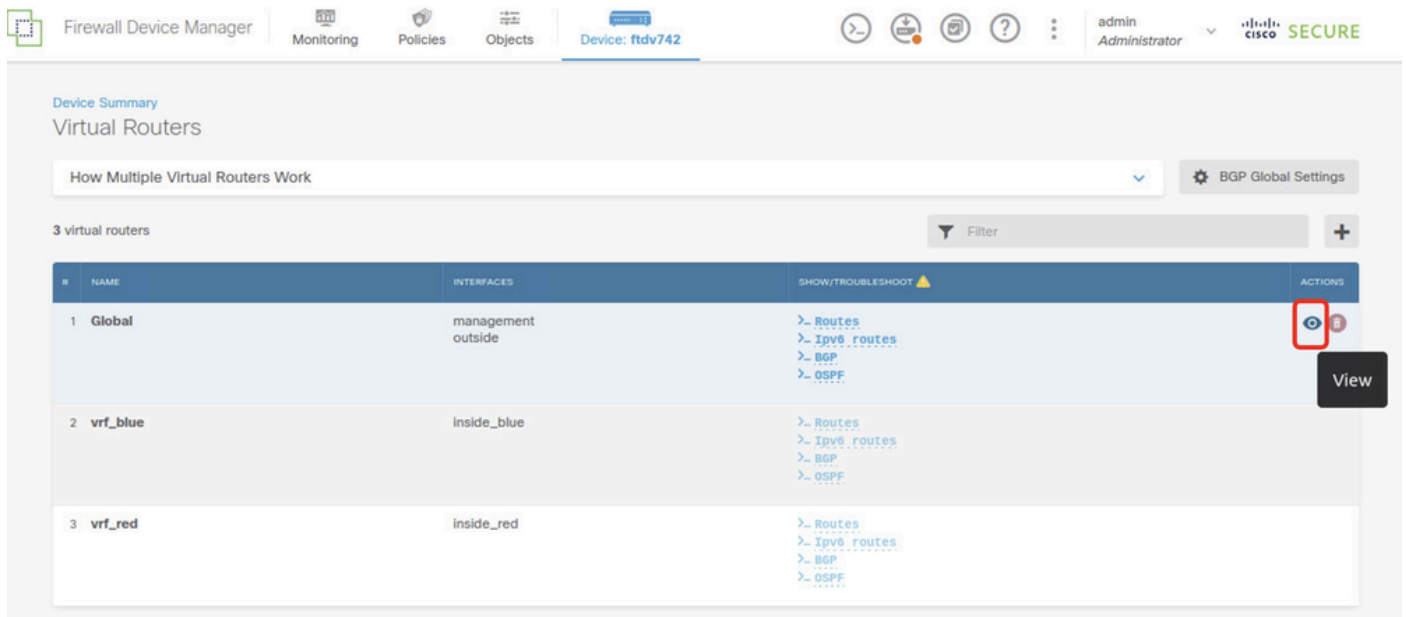
OK

FTD_Create_Static_Route_VRF_Rood_Details

Stap 7. Maak routelekkage van wereldwijde naar virtuele routers. De routes staat eindpunten toe die door het verre eind van plaats-aan-plaats VPN worden beschermd om tot het 192.168.10.0/24

netwerk in de virtuele router vrf_red en 192.168.20.0/24 netwerk in de virtuele router vrf_blue toegang te hebben.

Navigeer naar apparaat > routing . Klik op View Configuration . Klik op het pictogram View in de actiecel voor de wereldwijde virtuele router.



FTD_View_VRF_globaal

Stap 7.1. Klik op het tabblad Statische routing. Klik op + knop.



FTD_Aanmaken_Statische_Route_VRF_Globaal

Stap 7.2. Verstrek de nodige informatie. Klik op OK knop.

- Naam: S2S_lek_blauw
- Interface: inside_blue (Gigabit Ethernet0/2)
- Netwerken: local_blue_192.168.20.0
- Gateway: Laat dit item leeg.

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
```

Stap 10. Maak een IKEv2 ipsec-voorstel dat dezelfde parameters definieert als die op de FTD zijn geconfigureerd.

```
<#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
```

Stap 1. Maak een ipsec-profiel, verwijzing ipsec-voorstel gemaakt in Stap 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
```

Stap 12. Maak een groepsbeleid dat het IKEv2 protocol toestaat.

```
<#root>
```

```
group-policy
```

```
demo_gp_192.168.30.1
```

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

Stap 13. Maak een tunnelgroep voor het peer FTD buiten IP-adres, met verwijzing naar het

groepsbeleid dat in Stap 12 en dezelfde voorgedeelde sleutel configureren met FTD (gemaakt in Stap 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 *****
```

Stap 14. Schakel IKEv2 in op de buiteninterface.

```
crypto ikev2 enable outside
```

Stap 15. Maak een virtuele tunnel.

```
<#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
```

Stap 16. Maak een statische route.

```
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
```

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Stap 1. Navigeer naar de CLI van FTD en ASA via console of SSH om de VPN-status van fase 1 en fase 2 te verifiëren via opdrachten tonen crypto ikev2 sa en tonen 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

```

Stap 2. Controleer de route van VRF en Global op 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
```

Stap 3. Controleer de ping-test.

Alvorens te pingen, controleer de tellers van show crypto ipsec sa | inc-interface:|encap|decap op FTD.

In dit voorbeeld, toont Tunnel1 30 pakketten voor zowel inkapseling als decapsulation.

```
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 pingt Client3.

```
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 pingt Client3.

```
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
```

Controleer de tellers van crypto ipsec tonen | Inc-interface:|encap|decap op FTD na ping succesvol.

In dit voorbeeld, toont Tunnel1 40 pakketten voor zowel inkapseling als decapsulation na succesvol pingelen. Bovendien, beide tellers die met 10 pakketten worden verhoogd, die 10 pingelen echoverzoeken aanpassen, erop wijzend dat het pingelen verkeer met succes door de tunnel IPsec overging.

```
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
```

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

U kunt deze debug commando's gebruiken om de VPN sectie op te lossen.

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

U kunt deze debug opdrachten gebruiken om de routesectie problemen op te lossen.

```
debug ip routing
```

Referentie

[Configuratiehandleiding voor Cisco Secure Firewall Device Manager, versie 7.4](#)

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.