

Begrijp VRF (Virtual Router) op Secure Firewall Threat Defence

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Licentie](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Overzicht van functies](#)

[VRF-ondersteuning](#)

[Routing-beleid](#)

[Overlappende netwerken](#)

[Configuratie](#)

[VCC](#)

[FDM](#)

[REST API](#)

[VCC](#)

[FDM](#)

[Use cases](#)

[Serviceprovider](#)

[Gedeelde bronnen](#)

[Overlap Netwerk met hosts communiceren met elkaar](#)

[BGP-routelekkage](#)

[Verificatie](#)

[Probleemoplossing](#)

[Verwante links](#)

Inleiding

Dit document beschrijft de Virtual Routing and Forwarding (VRF) functionaliteit in de Cisco **Secure Firewall Threat Defence (FTD)**.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco-software **Secure Firewall Threat Defense (FTD)**
- **Secure Firewall Threat Defence (FTD)**
- **Virtual Routing and Forwarding (VRF)**
- Dynamische routingprotocollen (OSPF, BGP)

Licentie

Geen specifieke vergunningsvereiste, is de basisvergunning voldoende

Gebruikte componenten

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

- Cisco-software **Secure Firewall Threat Defense (FTD)**, **Secure Firewall Management Center (FMC)** versie 7.2.

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

Het **Virtual Routing and Forwarding (VRF)** Deze functie is toegevoegd in FTD-software release 6.6.

De voordelen van deze functie zijn:

- Segregatie van routingstabellen
- Netwerksegmenten met overlappingen in IP-adresruimten
- VRF-lite
- FXOS Multi-instance ondersteuning voor multi-context migratie use cases
- BGP **Route Leak Support-v4v6** en **BGPv6 VTI Support** functies zijn toegevoegd in FTD-software release 7.1.

Overzicht van functies

VRF-ondersteuning

Apparaat	Maximum aantal virtuele routers
ASA	10-20
FirePOWER-applicatie 1000*	5-10 *1010 (7,2+)
Firepower 2100	10-40
Firepower 3100	15-100
Firepower 4100	60-100
Firepower 9300	60-100
Virtuele FTD	30
ISA 3000	10(7,0+)

VRF-limieten per blade met native modus

Routing-beleid

Beleid	Wereldwijde VRF	Gebruiker VRF
Statische route	✓	✓
OSPF V2-software	✓	✓
OSPF V3	✓	✗

RIP	✓	✗
BGP4 router	✓	✓
BGP2	✓	✓ (7,1+)
IRB (BVI)	✓	✓
EIGRP	✓	✗

Overlappende netwerken

	Beleid	Niet-overlappend	Overlappende netwerken
	Routing en IRB	✓	✓
	AVC	✓	✓
	SSL-decryptie	✓	✓
	Inbraakdetectiesysteem en malware (IPS en bestandsbeleid)	✓	✓
	VPN	✓	✓
	Malware Events Analysis (hostprofielen, IoC, bestandstrajecten)	✓	✗
	Threat Intelligence (TID)	✓	✗

Configuratie

VCC

Stap 1. Naar navigeren **Devices > Device Management** en het te configureren FTD bewerken.

Stap 2. Naar het tabblad navigeren **Routing**

Stap 3. Klik **Manage Virtual Routers** .

Stap 4. Klik **Add Virtual Router** .

Stap 5. Voer in het vak **Add Virtual Router** een naam en beschrijving in voor de virtuele router.

Stap 6. Klik **ok** .

Stap 7. Als u interfaces wilt toevoegen, selecteert u de interface onder de **Available Interfaces** en klik vervolgens op **Add** .

Stap 8. Configureer de routing in de virtuele router.

- OSPF
- RIP
- BGP
- Statische routing
- Multicast

FDM

Stap 1. Naar navigeren **Device > Routing** .

Stap 2.

- Als er geen virtuele routers zijn gemaakt, klikt u op **Add Multiple Virtual Routers** klikt u vervolgens op **Create First Customer Virtual Router** .
- Klik op de **+**-knop boven aan de lijst met virtuele routers om een nieuwe router te maken.

Stap 3. In het **Add Virtual Router** doos. Voer de naam en beschrijving van de virtuele router in.

Stap 4. Klik op **+** om elke interface te selecteren die deel moet uitmaken van de virtuele router.

Stap 5. Klik **ok** .

Stap 6. Routing configureren in de **Virtual Router**.

- OSPF
- RIP
- BGP
- Statische routing
- Multicast

REST API

VCC

Het VCC ondersteunt volledige CRUD bewerkingen op virtuele routers.

Het pad van de virtuele routeroproepen valt onder **Devices > Routing > virtualrouters**

FDM

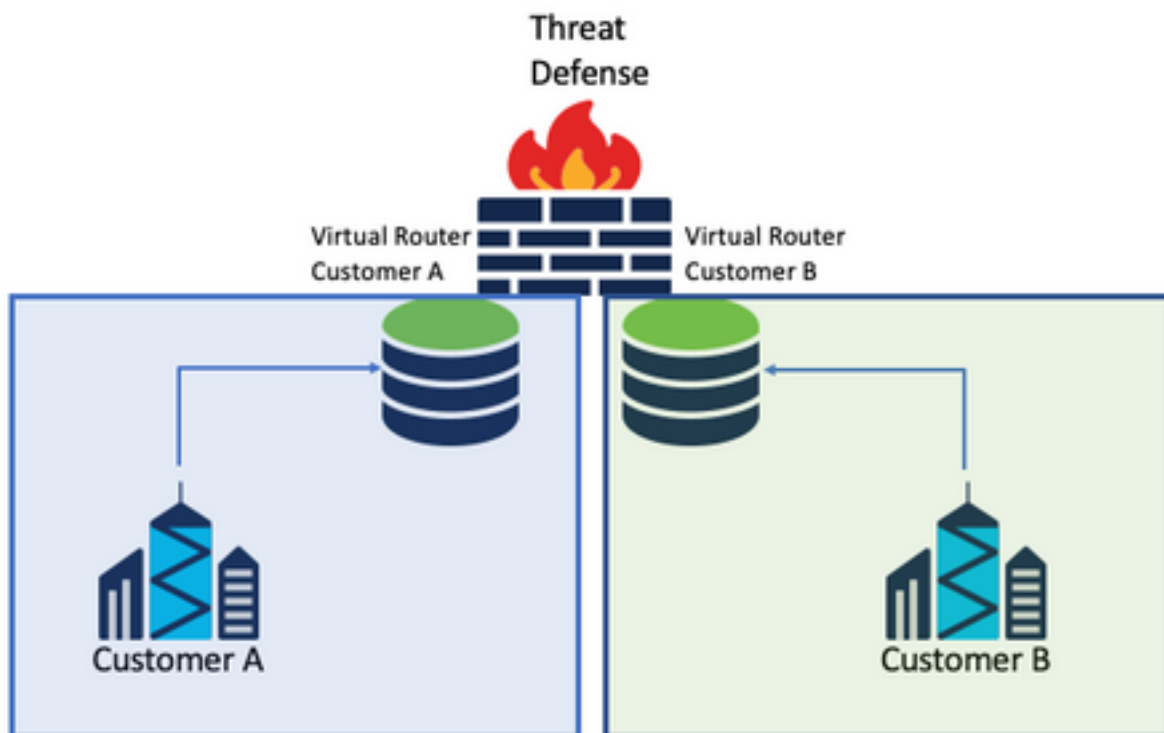
De FDM ondersteunt volledige CRUD-bewerkingen op virtuele routers.

Het pad van de virtuele routeroproepen valt onder **Devices > Routing > virtualrouters**

Use cases

Serviceprovider

In afzonderlijke routingstabellen zijn twee netwerken niet met elkaar verbonden en is er geen communicatie tussen hen.

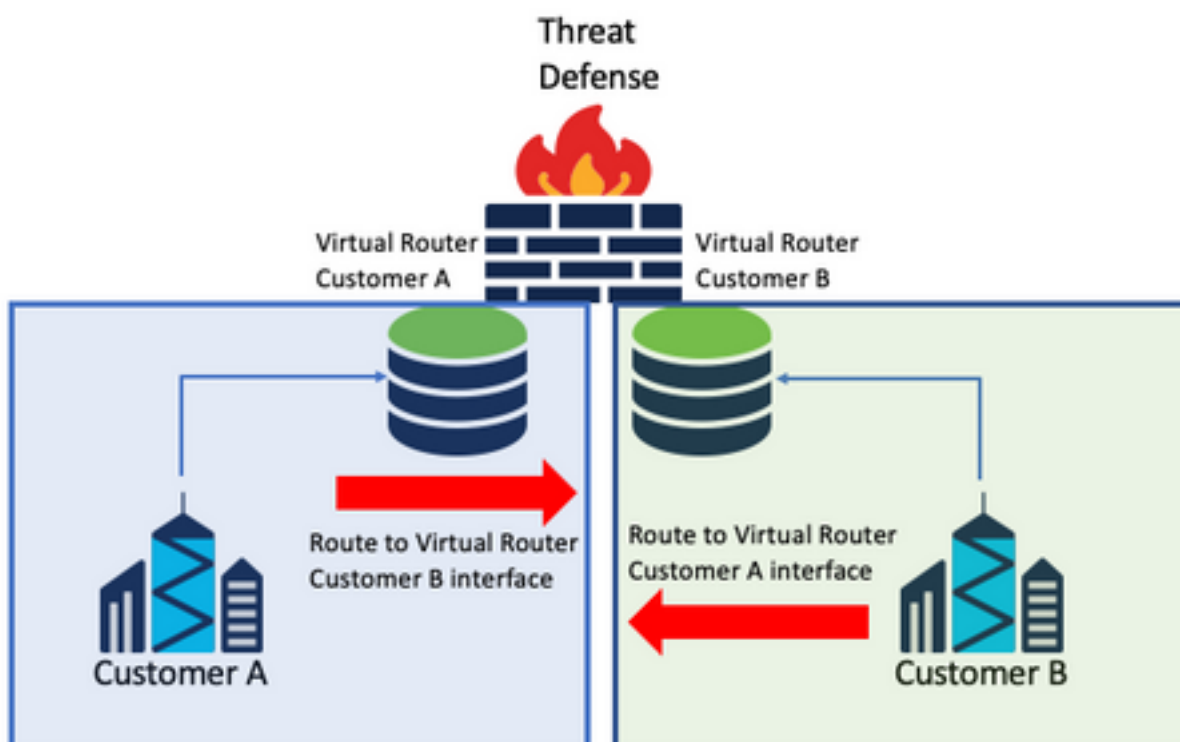


Overwegingen:

- Er zijn geen speciale overwegingen in dit scenario.

Gedeelde bronnen

Koppel twee virtuele routers onderling om bronnen van elk van hen te delen en heb connectiviteit van Customer A in Customer B en vice versa.



Overwegingen:

- In elke virtuele router, vorm een statische route die aan het bestemmingsnetwerk met de interface van de andere virtuele router richt.

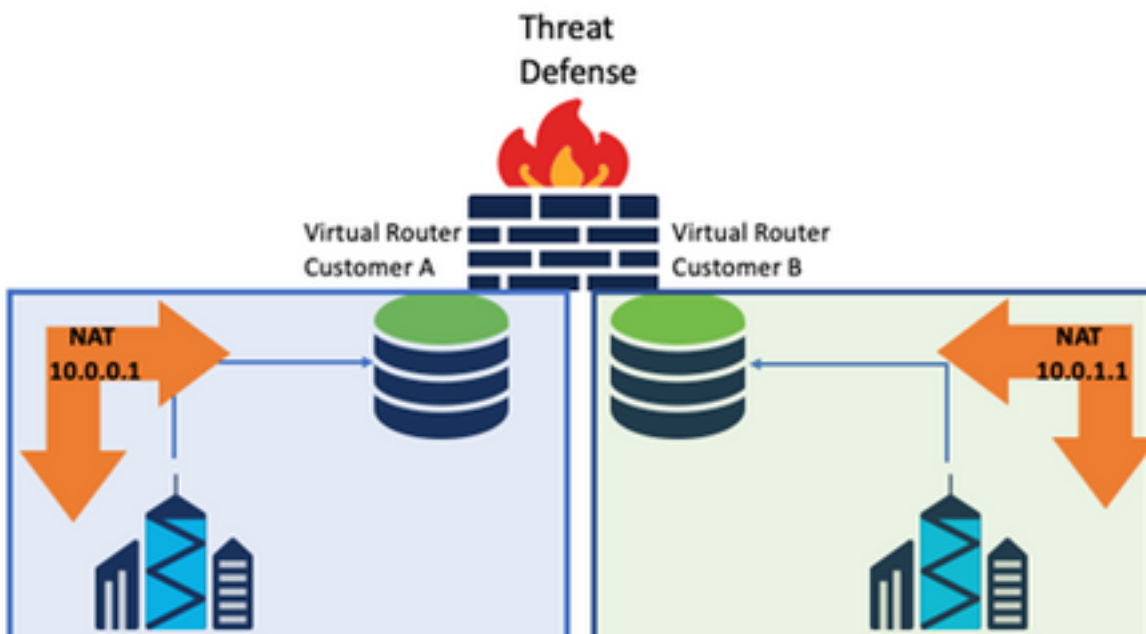
Voorbeeld:

In de virtuele router voor **Customer A**, voeg een route toe met als bestemming de **Customer B** interface zonder IP-adres als gateway (niet nodig, dit staat bekend als *route leaking*).

Herhaal hetzelfde proces voor **Customer B**.

Overlap Netwerk met hosts communiceren met elkaar

Er zijn 2 virtuele routers met dezelfde netwerkadressen en verkeer uitwisseling tussen hen.



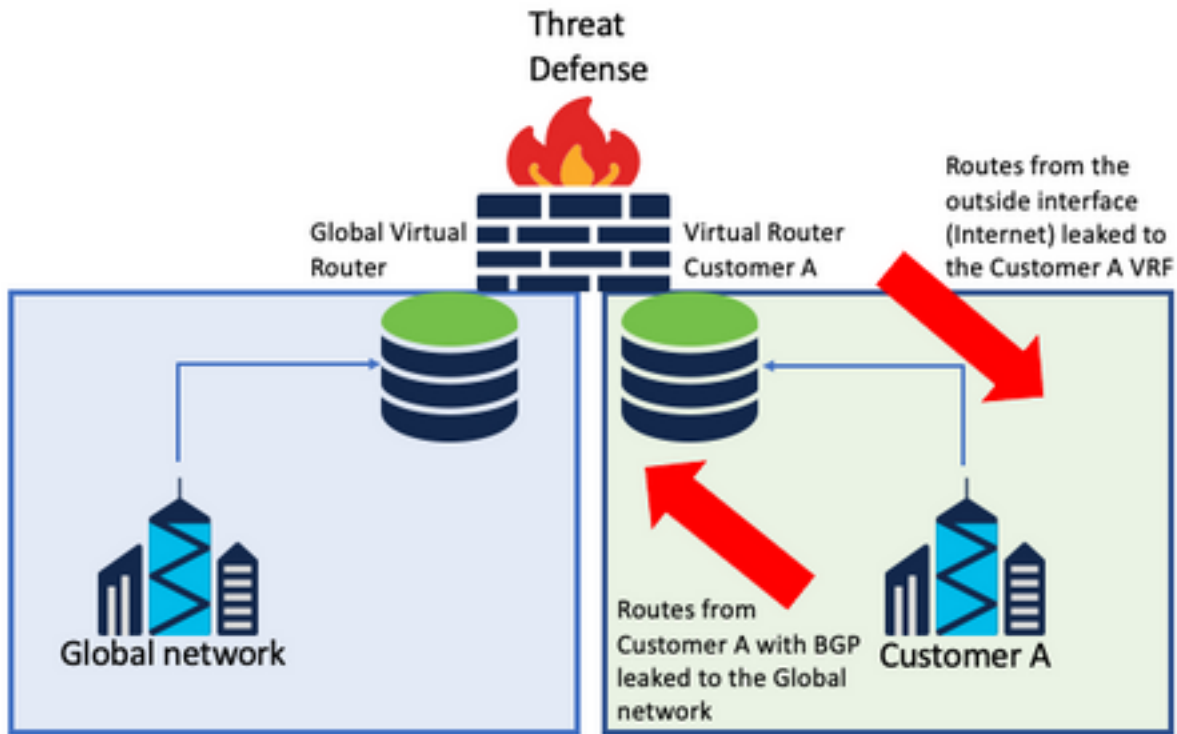
Overwegingen:

Om communicatie tussen de 2 netwerken te hebben, moet u tweemaal een NAT configureren om het IP-bronadres te negeren en een nep IP-adres in te stellen.

BGP-routelekkage

Er is één door de gebruiker gedefinieerde virtuele router en de routes van die virtuele router moeten worden uitgelekt naar de wereldwijde virtuele router.

De buiteninterface routeert van de globale interface die naar de door de gebruiker gedefinieerde virtuele router moet worden gelekt.



Overwegingen:

- Controleer of de FTD versie 7.1+ is.
- Gebruik de opties **Importeren/exporteren** in de **BGP > IPv4** -menu.
- Gebruik routekaart voor distributie.

Verificatie

De manier om te verifiëren dat de virtuele router is gemaakt, is met de opdrachten:

```
firepower# show vrf
```

Name	VRF ID	Description	Interfaces
VRF_A	1	VRF A	DMZ

```
firepower# show vrf detail
```

```
VRF Name: VRF_A; VRF id = 1 (0x1)
```

```
VRF VRF_A (VRF Id = 1);
```

```
Description: This is VRF for customer A
```

```
Interfaces:
```

```
Gi0/2
```

```
Address family ipv4 (Table ID = 1 (0x1)):
```

```
...
```

```
Address family ipv6 (Table ID = 503316481 (0x1e000001)):
```

```
...
```

```
VRF Name: single_vf; VRF id = 0 (0x0)
```

```
VRF single_vf (VRF Id = 0);
```

```
No interfaces
```

```
Address family ipv4 (Table ID = 65535 (0xffff)):
```

```
...
```

```
Address family ipv6 (Table ID = 65535 (0xffff)):
```

```
...
```

Probleemoplossing

De opdrachten die nodig zijn om informatie over VRF te verzamelen en te diagnosticeren, zijn:

Alle VRF's

- `show route all`
- `show asp table routing all`
- `packet tracer`

Wereldwijde VRF

- `show route`
- `show [bgp|ospf] [subcommands]`

Door gebruiker gedefinieerde VRF

- `show route [bgp|ospf] vrf {name}`

Verwante links

[Cisco Secure Firewall Management Center - apparaatconfiguratiehandleiding, 7.2 - virtuele routers en Cisco Secure Firewall Management Center - Cisco](#)

[Cisco Secure Firewall Device Manager-configuratiehandleiding, versie 7.2 - virtuele routers en Cisco Secure Firewall Threat Defense - Cisco](#)

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.