Understand VRF (Virtual Router) on Secure Firewall Threat Defense

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Licensing](#)
[Components Used](#)
[Background Information](#)
[Feature Overview](#)
[VRF Support](#)
[Routing Policies](#)
[Overlapping Networks](#)
[Configuration](#)
[FMC](#)
[FDM](#)
[REST API](#)
[FMC](#)
[FDM](#)
[Use cases](#)
[Service provider](#)
[Resources shared](#)
[Overlap Network with hosts communicate with each other](#)
[BGP route leaking](#)
[Verification](#)
[Troubleshooting](#)
[Related Links](#)

Introduction

This document describes the **Virtual Routing and Forwarding (VRF)** functionality in the Cisco **Secure Firewall Threat Defense (FTD)**.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco **Secure Firewall Threat Defense (FTD)****Secure Firewall Threat Defense (FTD)**
- **Virtual Routing and Forwarding (VRF)**
- Dynamic routing protocols (OSPF, BGP)

Licensing

No specific license requirement, the base license is sufficient

Components Used

The information in this document is based on these software and hardware versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The **Virtual Routing and Forwarding (VRF)** feature was added in the FTD software release 6.6.

The advantages this feature offers are:

- Segregation of routing tables
- Network segments with overlaps in IP address spaces
- VRF-lite
- FXOS Multi-instance support for multiple-context migration use cases
- BGP **Route Leak Support-v4v6** and BGPv6 **VTI Support** features were added in the FTD software release 7.1.

Feature Overview

VRF Support

Device	Maximum Virtual Routers
ASA	10-20
Firepower 1000*	5-10 *1010(7.2+)
Firepower 2100	10-40
Firepower 3100	15-100
Firepower 4100	60-100
Firepower 9300	60-100
Virtual FTD	30
ISA 3000	10(7.0+)

VRF limits per blade with native mode

Routing Policies

Policies	Global VRF	User VRF
Static Route		
OSPPFv2		
OSPFv3		
RIP		

BGPv4 BGPv6 IRB (BVI) EIGRP	(7.1+)

Overlapping Networks

Policies Routing & IRB AVC SSL Decryption Intrusion and Malware Detection (IPS and File Policy) VPN Malware Events Analysis (Host Profiles, IoC, File Trajectory) Threat Intelligence (TID)	Non-overlapping Overlapping Networks

Configuration

FMC

Step 1. Navigate to **Devices > Device Management** , and edit the FTD to be configured.

Step 2. Navigate to the tab **Routing**

Step 3. Click **Manage Virtual Routers .**

Step 4. Click **Add Virtual Router .**

Step 5. In the Add Virtual Router box, enter a name and description for the virtual router.

Step 6. Click **Ok** .

Step 7. To add interfaces, select the interface under the **Available Interfaces** box, and then click **Add** .

Step 8. Configure routing in the Virtual Router.

- OSPF
- RIP
- BGP
- Static Routing
- Multicast

FDM

Step 1. Navigate to **Device > Routing** .

Step 2.

- If there are no virtual routers created, click on **Add Multiple Virtual Routers** , then click **Create First Customer Virtual Router .**

- Click the **+** button at the top of the list of virtual routers to create a new one.

Step 3. In the **Add Virtual Router** box. Enter the name and description of the virtual router.

Step 4. Click **+** to select each interface that needs to be part of the virtual router.

Step 5. Click **Ok** .

Step 6. Configure routing in the **Virtual Router**.

- OSPF
- RIP
- BGP
- Static Routing
- Multicast

REST API

FMC

The FMC supports full CRUD operations on virtual routers.

The path of the virtual routers calls is under **Devices > Routing > virtualrouters**

FDM

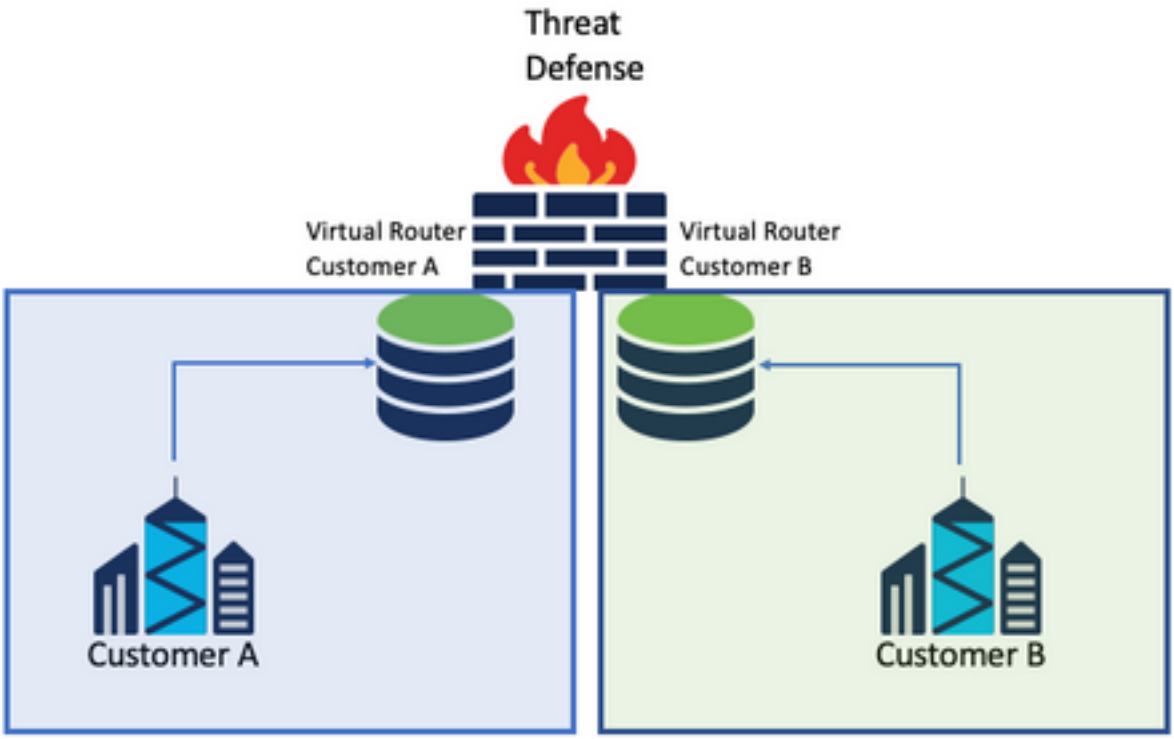
The FDM supports full CRUD operations on virtual routers.

The path of the virtual routers calls is under **Devices > Routing > virtualrouters**

Use cases

Service provider

In separate routing tables, two networks are not related to each other and there is no communication between them.

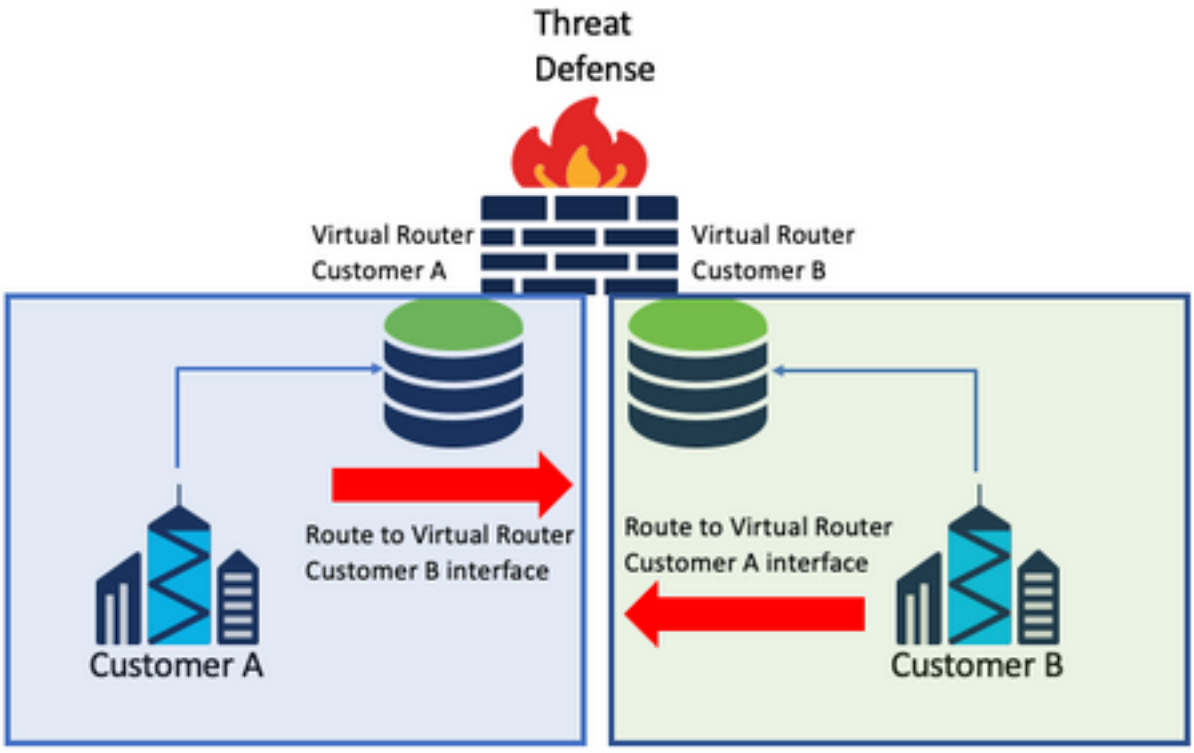


Considerations:

- There are no special considerations in this scenario.

Resources shared

Interconnect two virtual routers to share resources from each of them and have connectivity from **Customer A** to **Customer B** and vice versa.



Considerations:

- In each virtual router, configure a static route that points to the destination network with the interface of the other virtual router.

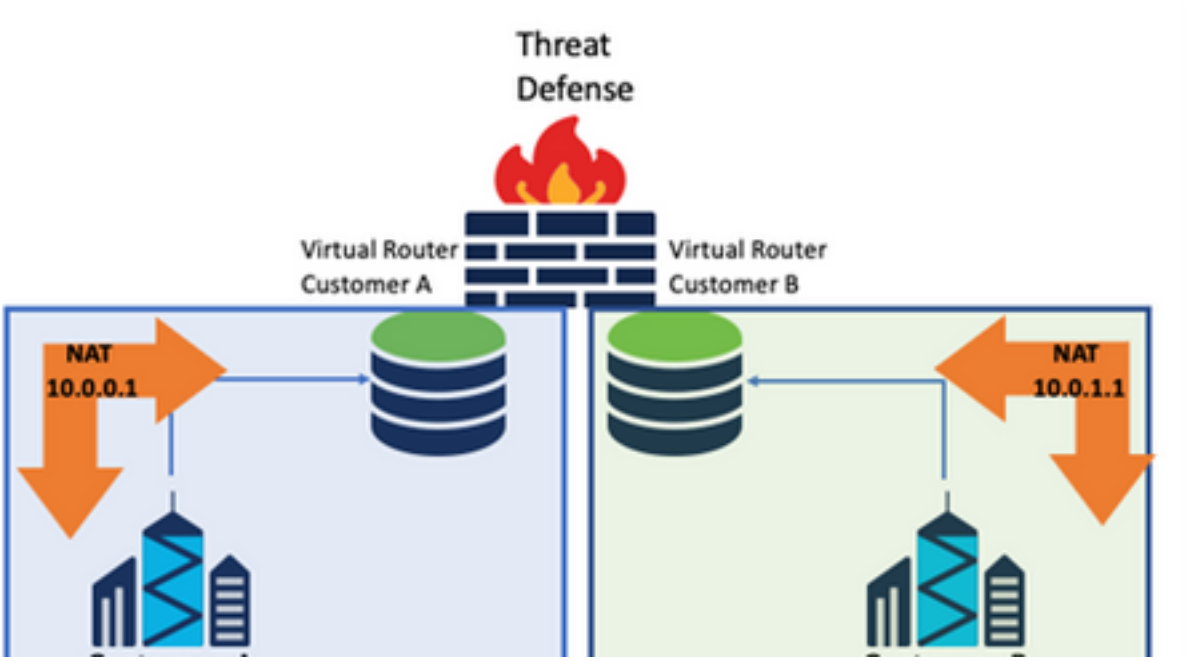
Example:

In the virtual router for **Customer A**, add a route with as a destination the **Customer B** interface without any IP address as a gateway (it is not needed, this is known as **route leaking**).

Repeat the same process for **Customer B**.

Overlap Network with hosts communicate with each other

There are 2 virtual routers with the same network addresses and with traffic exchange between them.



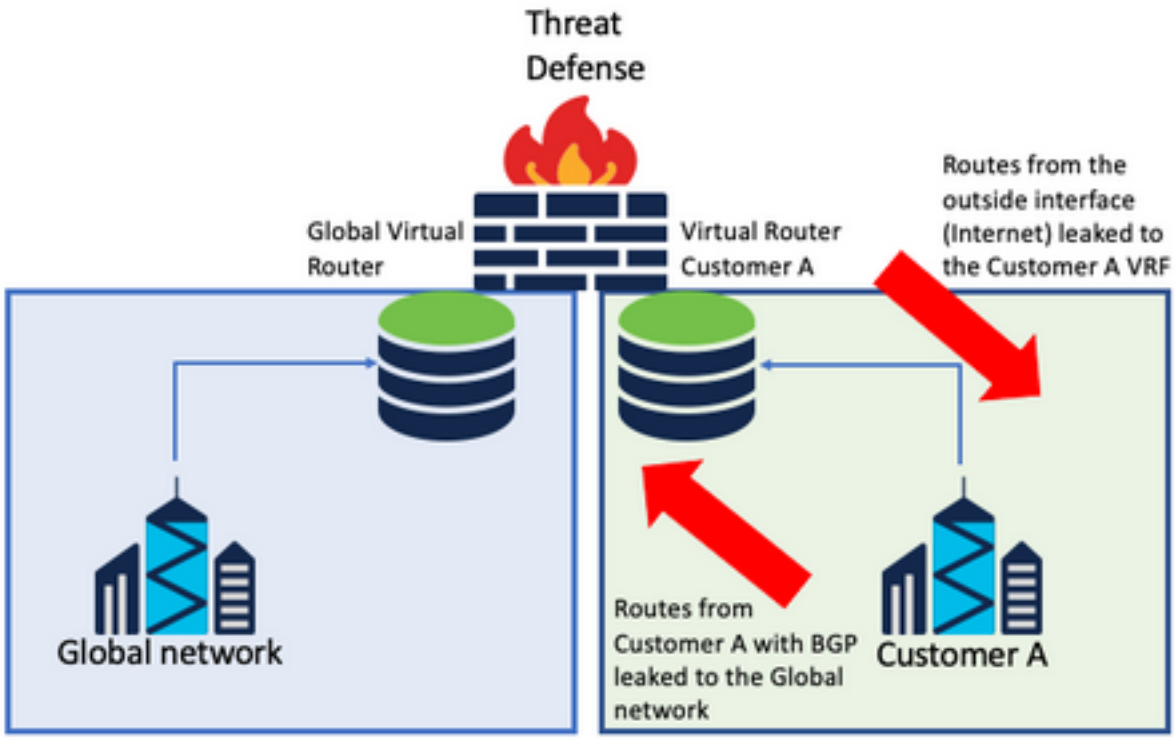
Considerations:

In order to have communication between the 2 networks, configure a twice NAT to override the source IP address and put a fake IP address.

BGP route leaking

There is one user-defined virtual router and the routes from that virtual router need to be leaked to the global virtual router.

The outside interface routes from the global interface to be leaked into the user-defined virtual router.



Considerations:

- Make sure the FTD version is 7.1+.
- Use the **Import/Export** options in the **BGP > IPv4** menu.
- Use route-map for distribution.

Verification

The way to verify the virtual router was created is with the commands:

```
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)):
  ...
```

Troubleshooting

The commands needed to collect and diagnose information about VRF are:

All VRFs

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

Global VRF

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

User-defined VRF

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

Related Links

Cisco Secure Firewall Management Center Device Configuration Guide, 7.2 - Virtual Routers
Cisco Secure Firewall Management Center - Cisco

Cisco Secure Firewall Device Manager Configuration Guide, Version 7.2 - Virtual Routers Cisco Secure Firewall Threat Defense - Cisco