了解安全防火墙威胁防御中的VRF（虚拟路由器）

目录

简介

本文档介绍 **Virtual Routing and Forwarding (VRF)** 思科安全防火**墙威胁防御(FTD)的功能**。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科 **Secure Firewall Threat Defense (FTD)安全防火墙威胁防御(FTD)**
- **Virtual Routing and Forwarding (VRF)**
- 动态路由协议(OSPF、BGP)

许可

无特定许可证要求，基本许可证就足够了

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

此 **Virtual Routing and Forwarding (VRF)** 功能已添加到FTD软件版本6.6。

此功能提供的优势包括：

- 路由表分离
- 在IP地址空间中有重叠的网段
- VRF-lite
- FXOS多实例支持多情景迁移使用案例
- 调试输出中显示“BGP **Route Leak Support-v4v6** 和BGPv6 **VTI Support** ftd软件版本7.1中添加了功能。

功能概述

VRF支持

设备	最大虚拟路由器数量
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
虚拟FTD	30
ISA 3000	10(7.0+)

使用本机模式时每个刀片的VRF限制

路由策略

策略	全球VRF	用户VRF
静态路由	✓	✓
OSPPFv2	✓	✓
OSPFv3	✓	✖
RIP	✓	✖
BGPv4	✓	✓
BGPv6	✓	✓(7.1+)

IRB(BVI)	✓	✓
EIGRP	✓	✖

重叠网络

策略	非重叠	重叠网络
路由和IRB	✓	✓
AVC	✓	✓
SSL解密	✓	✓
入侵和恶意软件检测（IPS和文件策略）	✓	✓
VPN	✓	✓
恶意软件事件分析（主机配置文件、IoC、文件轨迹）	✓	✖
威胁情报(TID)	✓	✖

配置

FMC

步骤1:导航至 **Devices > Device Management** ，并编辑要配置的FTD。

第二步：导航到选项卡 **Routing**

第三步：点击 **Manage Virtual Routers** .

第四步：点击 **Add Virtual Router** .

第五步：在Add Virtual Router（添加虚拟路由器）框中，输入虚拟路由器的名称和说明。

第六步：点击 **Ok** .

步骤 7.要添加接口，请在 **Available Interfaces** 框，然后单击 **Add** .

步骤 8在虚拟路由器中配置路由。

- OSPF
- RIP
- 调试输出中显示“BGP
- 静态路由
- 组播

FDM

步骤1:导航至 **Device > Routing** .

第二步：

- 如果未创建虚拟路由器，请点击 **Add Multiple Virtual Routers** ，然后单击 **Create First Customer Virtual Router** .
- 单击虚拟路由器列表顶部的+按钮以创建一个新的虚拟路由器。

第三步：如果 **Add Virtual Router** 包装盒.输入虚拟路由器的名称和说明。

第四步：单击**+**选择需要作为虚拟路由器一部分的每个接口。

第五步：点击 **Ok** .

第六步：在中配置路由 **Virtual Router**.

- OSPF
- RIP
- 调试输出中显示“BGP
- 静态路由
- 组播

REST API

FMC

FMC支持全双工 CRUD 虚拟路由器上的操作。

虚拟路由器呼叫的路径位于 **Devices > Routing > virtualrouters**

FDM

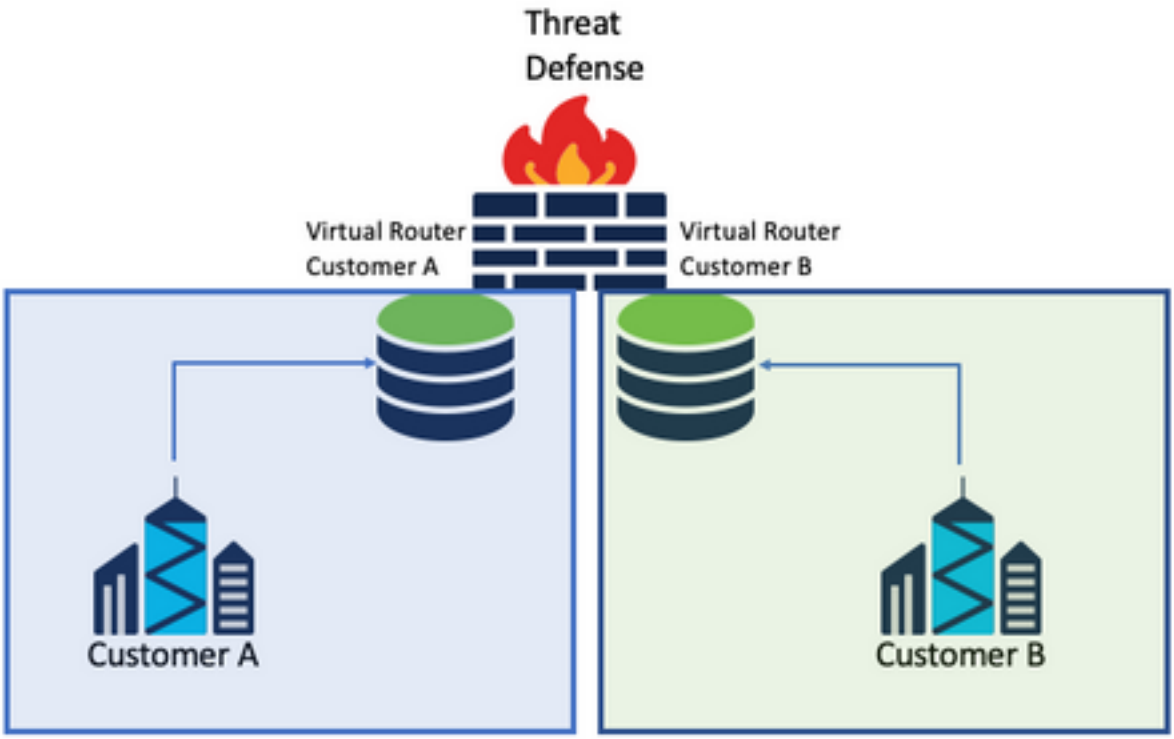
FDM支持虚拟路由器上的完全CRUD操作。

虚拟路由器呼叫的路径位于 **Devices > Routing > virtualrouters**

使用案例

Service Provider

在单独的路由表中，两个网络之间并不相关，也没有通信。

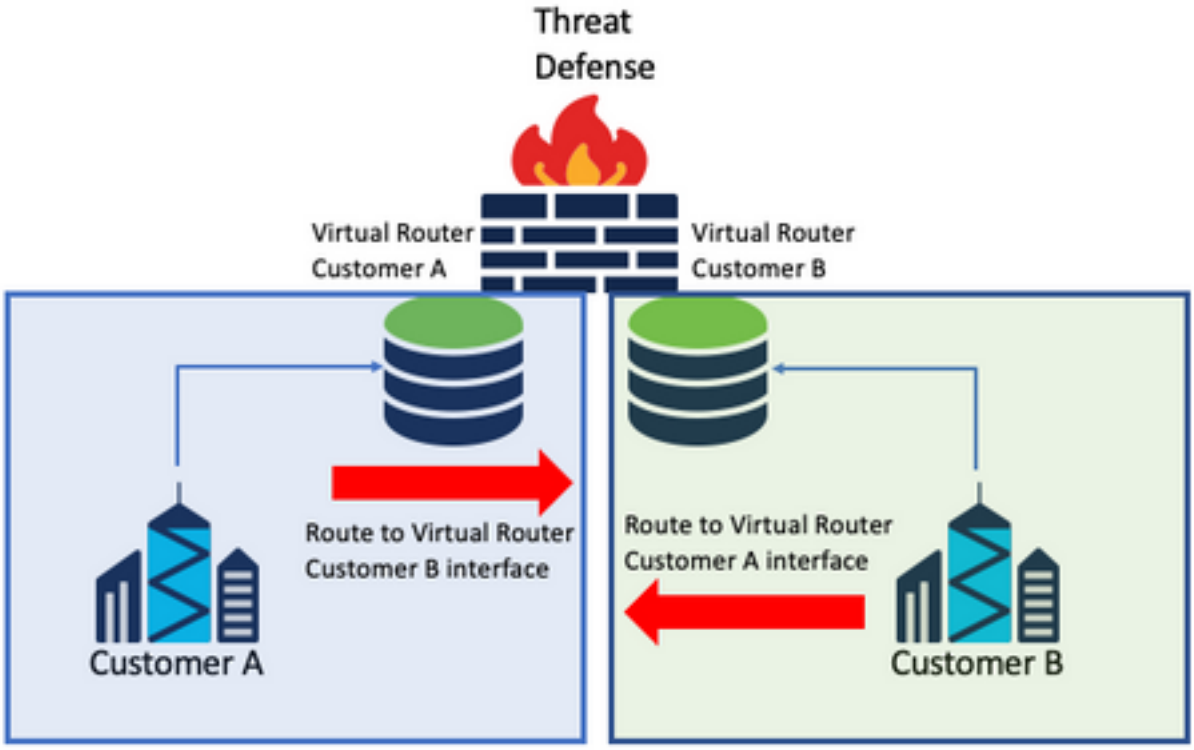


考虑事项:

- 此场景中没有特殊注意事项。

共享资源

互联两个虚拟路由器，以共享来自每个虚拟路由器的资源，并连接来自 **Customer A** 到 **Customer B** 反之亦然。



考虑事项:

- 在每台虚拟路由器中，配置一条静态路由，通过另一台虚拟路由器的接口指向目标网络。

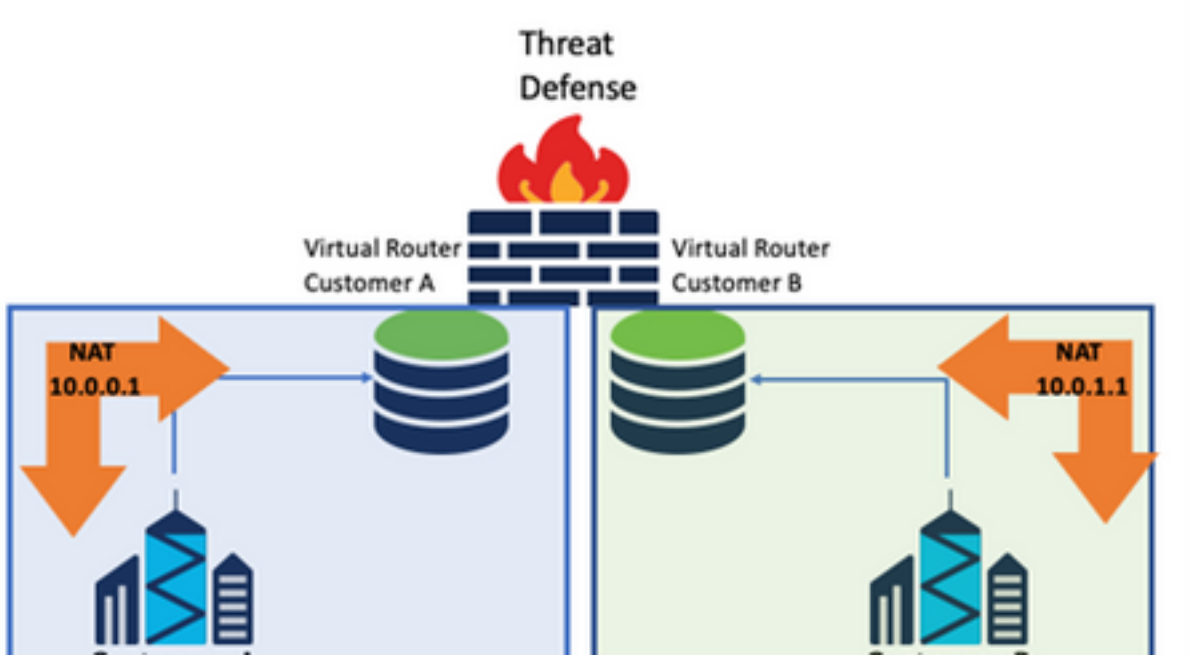
示例：

在虚拟路由器中 **Customer A**，添加一条路由，并将该路由作为目的 **Customer B** 没有任何IP地址作为网关的接口(不需要，这称为 **route leaking** 影响。

对重复相同的过程 **Customer B**.

重叠网络，使主机相互通信

有2台虚拟路由器具有相同的网络地址，并且它们之间可以交换流量。



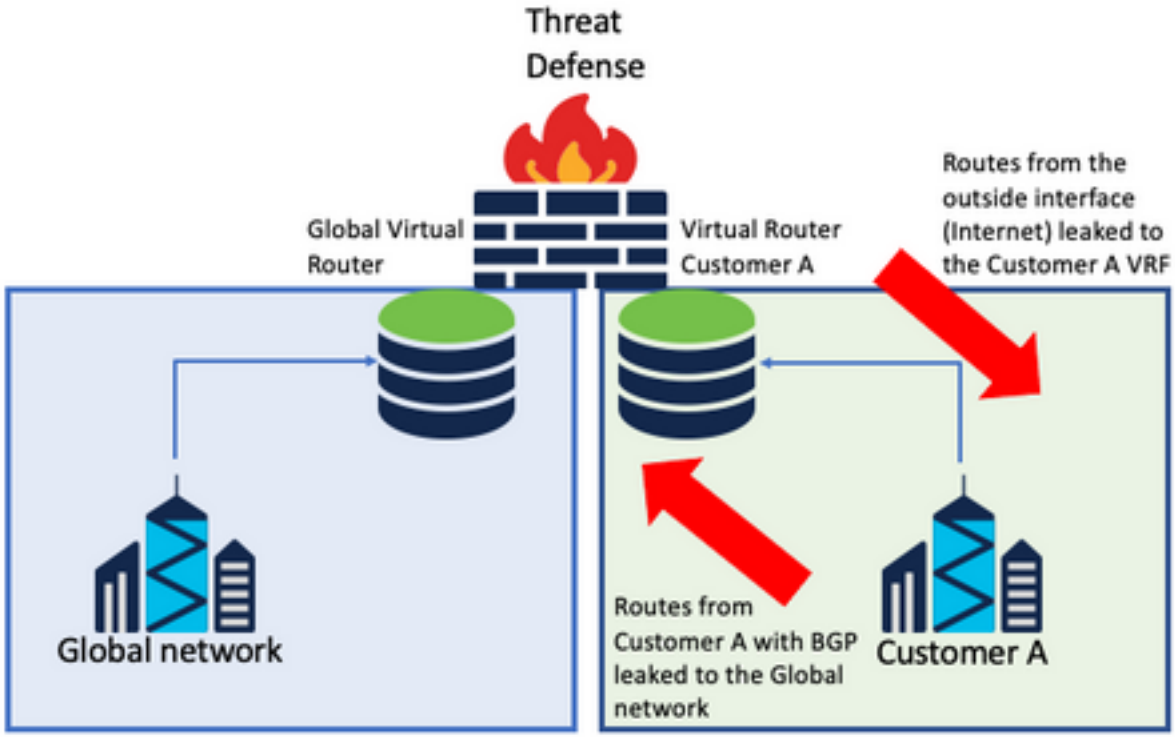
考虑事项:

为了在两个网络之间进行通信，请配置两次NAT以覆盖源IP地址并放置一个虚假IP地址。

BGP路由泄漏

有一个用户定义的虚拟路由器，来自该虚拟路由器的路由需要泄漏到全局虚拟路由器。

外部接口从全局接口路由泄漏到用户定义的虚拟路由器中。



考虑事项:

- 确保FTD版本为7.1+。
- 使用Import/Export选项 **BGP > IPv4** 菜单.
- 使用route-map进行分发。

确认

验证虚拟路由器是否创建的方法是使用以下命令：

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

故障排除

收集和诊断有关VRF的信息所需的命令包括：

所有VRF

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

全球VRF

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

用户定义的VRF

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

相关链接

[思科安全防火墙管理中心设备配置指南，7.2 — 虚拟路由器思科安全防火墙管理中心 — 思科]

[思科安全防火墙设备管理器配置指南，版本7.2 — 虚拟路由器思科安全防火墙威胁防御 — 思科]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。