

# 瞭解安全防火牆威脅防禦上的VRF ( 虛擬路由器 )

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[授權](#)

[採用元件](#)

[背景資訊](#)

[功能概述](#)

[VRF支援](#)

[路由策略](#)

[重疊網路](#)

[組態](#)

[FMC](#)

[FDM](#)

[REST API](#)

[FMC](#)

[FDM](#)

[使用案例](#)

[服務提供商](#)

[共用資源](#)

[與主機相互通訊的網路重疊](#)

[BGP路由洩漏](#)

[驗證](#)

[疑難排解](#)

[相關連結](#)

## 簡介

本檔案將介紹 Virtual Routing and Forwarding (VRF) 安全防火牆威脅防禦(FTD)中的功能。

## 必要條件

## 需求

思科建議您瞭解以下主題：

- 思科 Secure Firewall Threat Defense (FTD)安全防火牆威脅防禦(FTD)
- Virtual Routing and Forwarding (VRF)
- 動態路由協定(OSPF、BGP)

## 授權

無特定許可證要求，基本許可證就足夠了

## 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科 Secure Firewall Threat Defense (FTD)中， Secure Firewall Management Center (FMC) 7.2版。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

其 Virtual Routing and Forwarding (VRF) ftd軟體版本6.6新增功能。

此功能提供的優勢包括：

- 路由表的分隔
- 在IP地址空間中有重疊的網段
- VRF-lite
- FXOS多例項支援多情景遷移使用案例
- BGP Route Leak Support-v4v6 和BGPv6 VTI Support ftd軟體版本7.1新增功能。

## 功能概述

### VRF支援

裝置	最大虛擬路由器數量
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
虛擬FTD	30
ISA 3000	10(7.0+)

使用本機模式時每個刀片的VRF限制

### 路由策略

策略	全域性VRF	使用者VRF
靜態路由	✓	✓
OSPFv2	✓	✓
OSPFv3	✓	✗
RIP	✓	✗
BGPv4	✓	✓
BGPv6	✓	✓(7.1+)

IRB(BVI)	✓	✓
EIGRP	✓	✗

## 重疊網路

策略	非重疊	重疊網路
路由和IRB	✓	✓
AVC	✓	✓
SSL解密	✓	✓
入侵和惡意軟體檢測 ( IPS和檔案策略 )	✓	✓
VPN	✓	✓
惡意軟體事件分析 ( 主機配置檔案、IoC、檔案軌跡 )	✓	✗
威脅情報(TID)	✓	✗

## 組態

### FMC

步驟1. 導航至 **Devices > Device Management** 並編輯要配置的FTD。

步驟2. 導航到頁籤 **Routing**

步驟3. 按一下 **Manage Virtual Routers** .

步驟4. 按一下 **Add Virtual Router** .

步驟5. 在新增虛擬路由器框中，輸入虛擬路由器的名稱和說明。

步驟6. 按一下 **OK** .

步驟7. 要新增介面，請在 **Available Interfaces** 框中，然後按一下 **Add** .

步驟8. 在虛擬路由器中配置路由。

- OSPF
- RIP
- BGP
- 靜態路由
- 多點傳播

### FDM

步驟1. 導航至 **Device > Routing** .

步驟2.

- 如果未建立虛擬路由器，請按一下 **Add Multiple Virtual Routers** ，然後按一下 **Create First Customer Virtual Router** .
- 按一下虛擬路由器清單頂部的+按鈕以建立新的虛擬路由器。

步驟3. 在 **Add Virtual Router** 框。輸入虛擬路由器的名稱和說明。

步驟4.按一下+以選擇需要作為虛擬路由器一部分的每個介面。

步驟5.按一下 **ok** .

步驟6.在中配置路由 **Virtual Router**.

- OSPF
- RIP
- BGP
- 靜態路由
- 多點傳播

## REST API

### FMC

FMC支援全功能 **CRUD** 虛擬路由器上的操作。

虛擬路由器呼叫的路徑位於 **Devices > Routing > virtualrouters**

### FDM

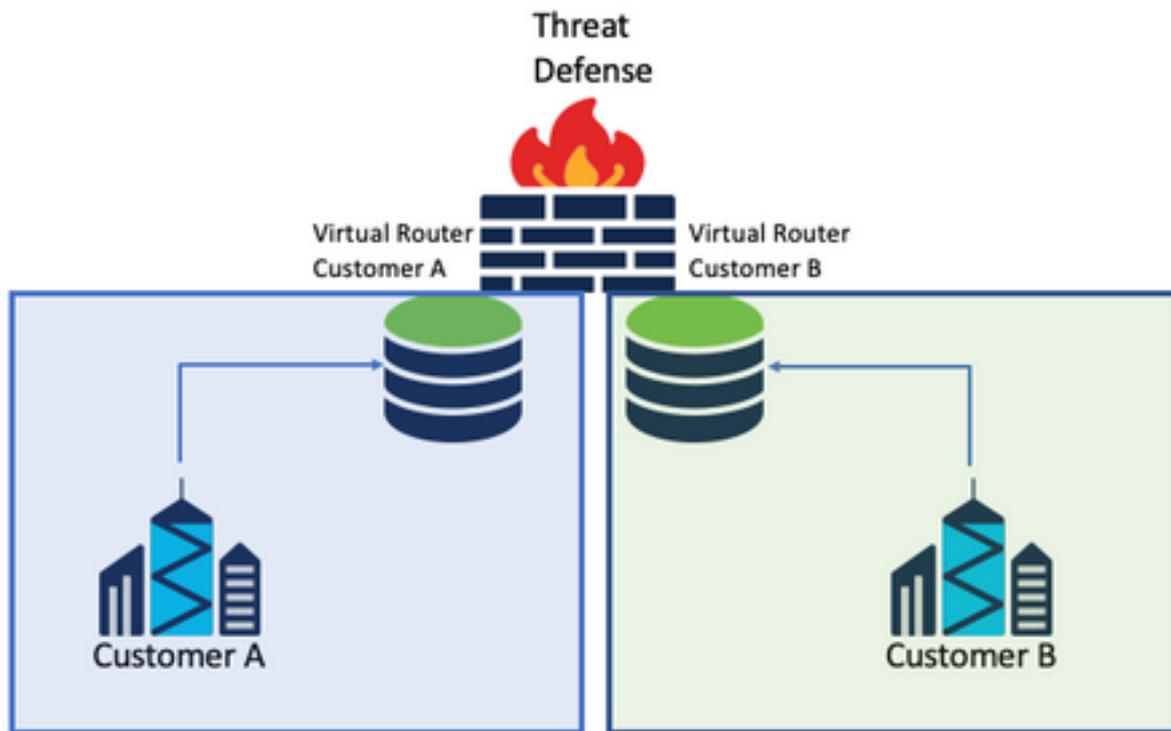
FDM支援虛擬路由器上的完整**CRUD**操作。

虛擬路由器呼叫的路徑位於 **Devices > Routing > virtualrouters**

## 使用案例

### 服務提供商

在單獨的路由表中，兩個網路彼此不相關，並且它們之間沒有通訊。

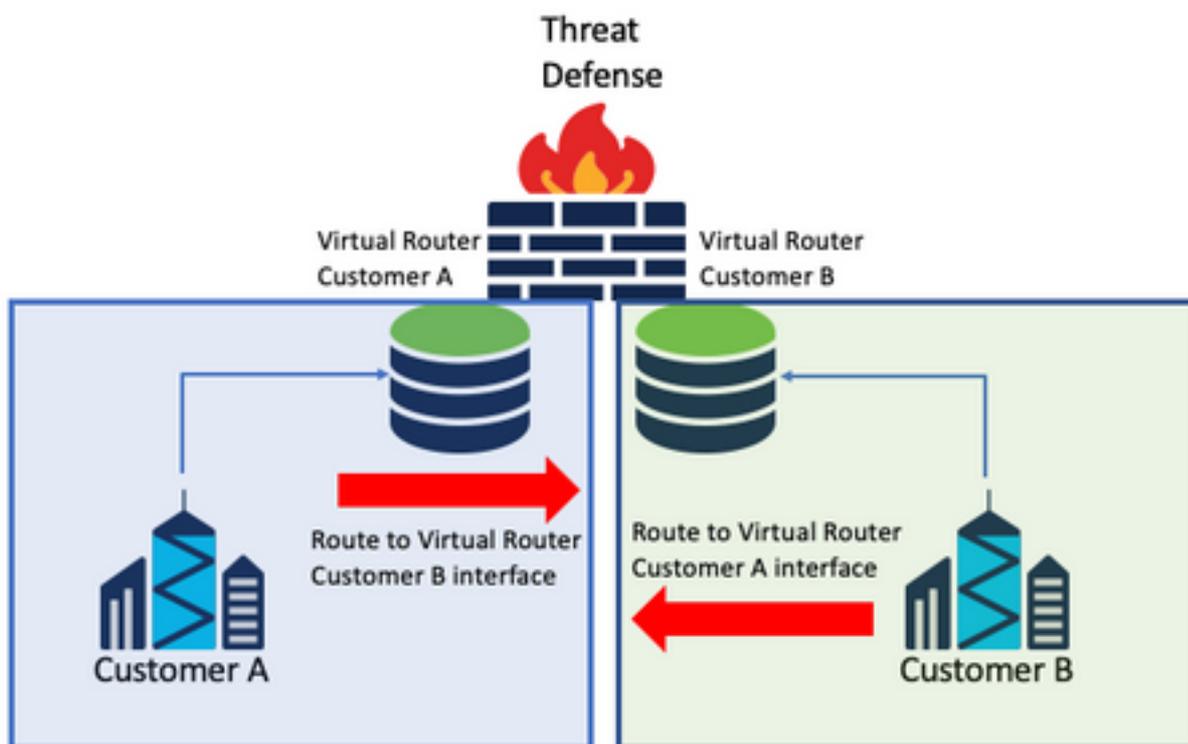


**注意事項：**

- 在此情況中沒有特殊注意事項。

**共用資源**

將兩台虛擬路由器互連，以共用每台虛擬路由器的資源，並從 Customer A 成長至 Customer B 反之。



**注意事項：**

- 在每台虛擬路由器中，配置一條靜態路由，該路由通過另一台虛擬路由器的介面指向目標網路。

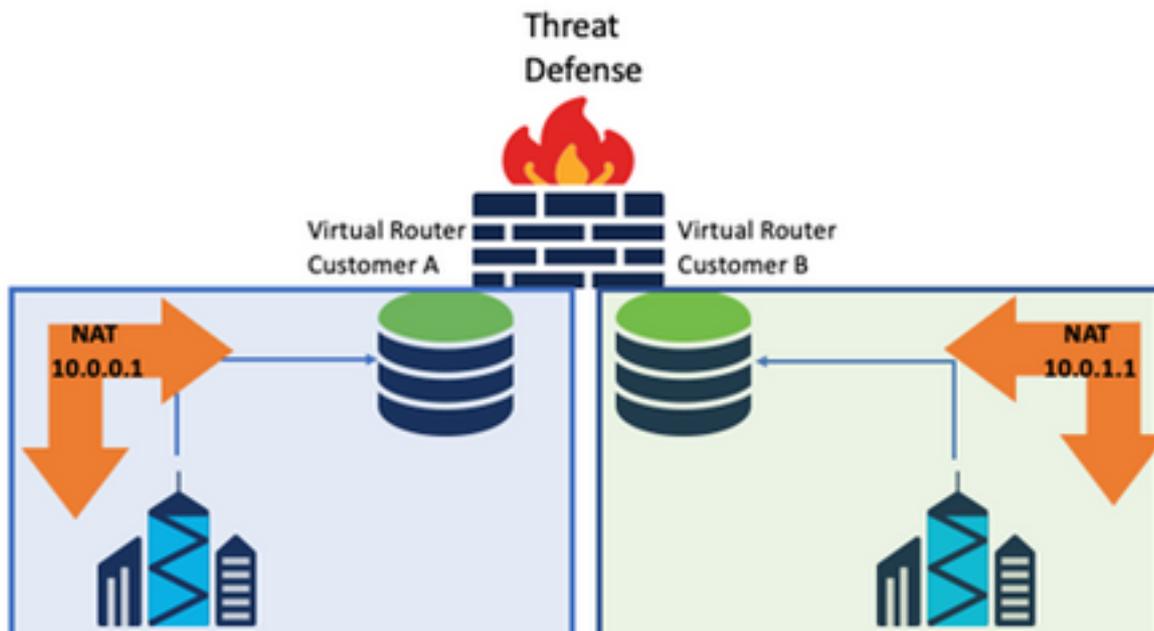
範例：

在虛擬路由器中 Customer A，新增一條作為目的地的路由 Customer B 沒有任何IP地址作為網關的介面 (不需要，這稱為 route leaking )。

對重複相同的過程 Customer B.

## 與主機相互通訊的網路重疊

有兩台網路地址相同的虛擬路由器，它們之間交換流量。



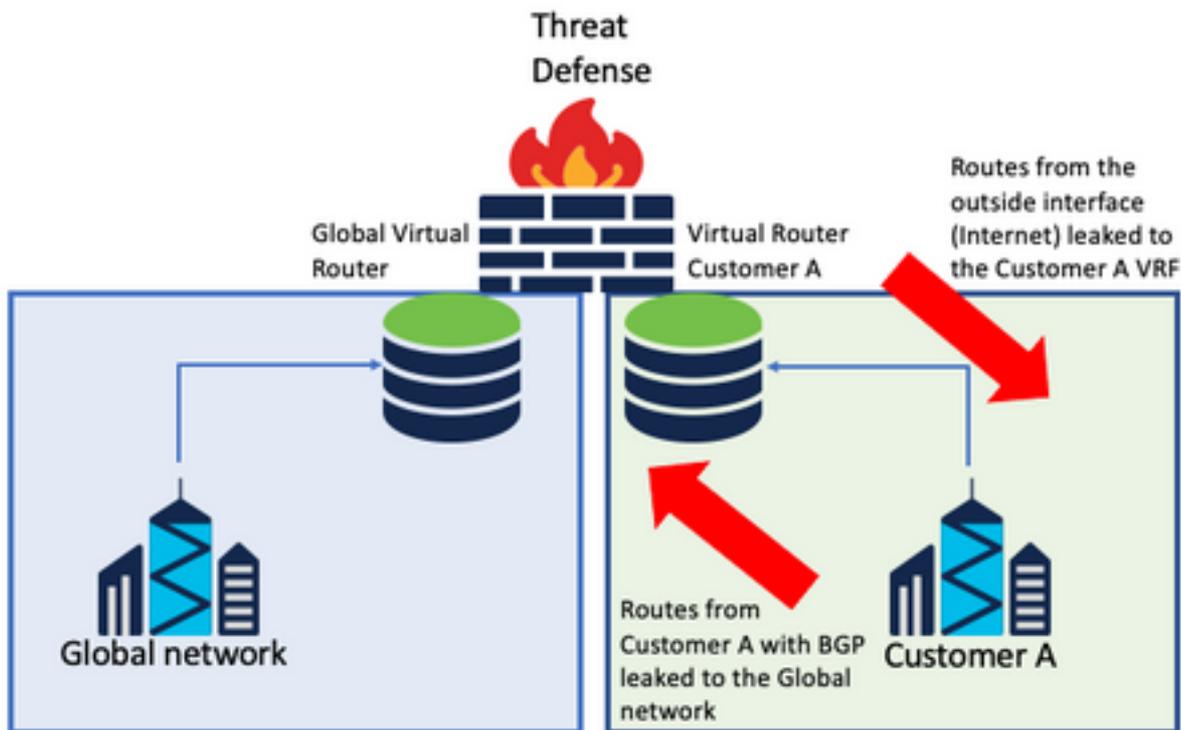
注意事項：

為了在兩個網路之間進行通訊，請配置兩次NAT以覆蓋源IP地址並放置一個假的IP地址。

## BGP路由洩漏

有一個使用者定義虛擬路由器，來自該虛擬路由器的路由需要洩漏到全域性虛擬路由器。

外部介面將從全域性介面路由洩漏到使用者定義的虛擬路由器中。



### 注意事項：

- 請確定FTD的版本是7.1+。
- 使用Import/Export選項 BGP > IPv4 選單。
- 使用route-map進行分發。

## 驗證

驗證虛擬路由器是否建立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)):
```

```
...
```

## 疑難排解

收集和診斷有關VRF的資訊所需的命令包括：

### 所有VRF

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

### 全域性VRF

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

### 使用者定義的VRF

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

## 相關連結

[思科安全防火牆管理中心裝置配置指南7.2 — 虛擬路由器思科安全防火牆管理中心 — 思科](#)

[思科安全防火牆裝置管理器配置指南7.2版 — 虛擬路由器思科安全防火牆威脅防禦 — 思科](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。