セキュアファイアウォールの脅威防御における VRF（仮想ルータ）について

内容

概要
前提条件
要件
ライセンス
使用するコンポーネント
背景説明
機能の概要
VRFサポート
ルーティングポリシー
重複ネットワーク
コンフィギュレーション
FMC
FDM
REST API
FMC
FDM
使用例
サービス プロバイダー
共有リソース
ホストとのオーバーラップネットワークは相互に通信する
BGPルート漏出
確認
トラブルシューティング
関連するリンク

概要

このドキュメントでは、 **Virtual Routing and Forwarding (VRF)** Cisco **Secure Firewall Threat Defense(FTD)の機能。**

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 『シスコ **Secure Firewall Threat Defense (FTD)**Secure Firewall Threat Defense(FTD)
- **Virtual Routing and Forwarding (VRF)**
- ダイナミックルーティングプロトコル(OSPF、BGP)

ライセンス

特定のライセンス要件はありません。基本ライセンスで十分です

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 『シスコ **Secure Firewall Threat Defense (FTD)、 Secure Firewall Management Center (FMC)** version 7.2.

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

「 **Virtual Routing and Forwarding (VRF)** この機能は、FTDソフトウェアリリース6.6で追加されました。

この機能には、次のような利点があります。

- ルーティングテーブルの分離
- IPアドレス空間に重複があるネットワークセグメント
- VRF-lite
- FXOSマルチインスタンスのサポートにより、マルチコンテキスト移行のユースケースに対応
- BGP **Route Leak Support-v4v6** およびBGPv6 **VTI Support** ftdソフトウェアリリース7.1で機能が追加されました。

機能の概要

VRFサポート

デバイス	仮想ルータの最大数
平均応答時間	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
仮想FTD	30
ISA 3000	10（7.0以上）

ネイティブモードでのブレードごとのVRF制限

ルーティングポリシー

ポリシー	グローバルVRF	ユーザVRF
スタティック ルート	✓	✓
OSPPFv2	✓	✓

OSPFv3	✓	✖
RIP	✓	✖
BGPv4	✓	✓
BGPv6	✓	✓（7.1以上）
IRB(BVI)	✓	✓
EIGRP	✓	✖

重複ネットワーク

ポリシー	重複しない 重複ネ
ルーティングとIRB	✓
AVC	✓
SSL復号化	✓
侵入およびマルウェア検出（IPSおよびファイルポリシー）	✓
VPN	✓
マルウェアイベント分析（ホストプロファイル、IoC、ファイルトラジェクトリー）	✓
脅威インテリジェンス(TID)	✓

コンフィギュレーション

FMC

ステップ 1：移動先 **Devices > Device Management** をクリックし、設定するFTDを編集します。

ステップ 2：タブに移動します **Routing**

ステップ 3：クリック **Manage Virtual Routers** .

ステップ 4：クリック **Add Virtual Router** .

ステップ 5：[Add Virtual Router]ボックスに、仮想ルータの名前と説明を入力します。

手順 6：クリック **Ok** .

手順 7：インターフェイスを追加するには、 **Available Interfaces** ボックスをクリックし、 **Add** .

ステップ 8：仮想ルータでルーティングを設定します。

- OSPF
- RIP
- BGP
- スタティックルーティング
- マルチキャスト

FDM

ステップ 1：移動先 **Device > Routing** .

ステップ 2：

- 仮想ルータが作成されていない場合は、 **Add Multiple Virtual Routers** をクリックし、 **Create First Customer Virtual Router** .
- 仮想ルータのリストの上部にある**+**ボタンをクリックして、新しい仮想ルータを作成します。

ステップ 3：内 **Add Virtual Router** ボックス。仮想ルータの名前と説明を入力します。

ステップ 4：**+**をクリックして、仮想ルータの一部にする必要がある各インターフェイスを選択します。

ステップ 5：クリック **Ok** .

手順 6：Cisco IOSソフトウェアリリース12.1以降の **Virtual Router.**

- OSPF
- RIP
- BGP
- スタティックルーティング
- マルチキャスト

REST API

FMC

FMCはフルをサポートします CRUD 仮想ルータでの動作。

仮想ルータのコールのパスは、 **Devices > Routing > virtualrouters**

FDM

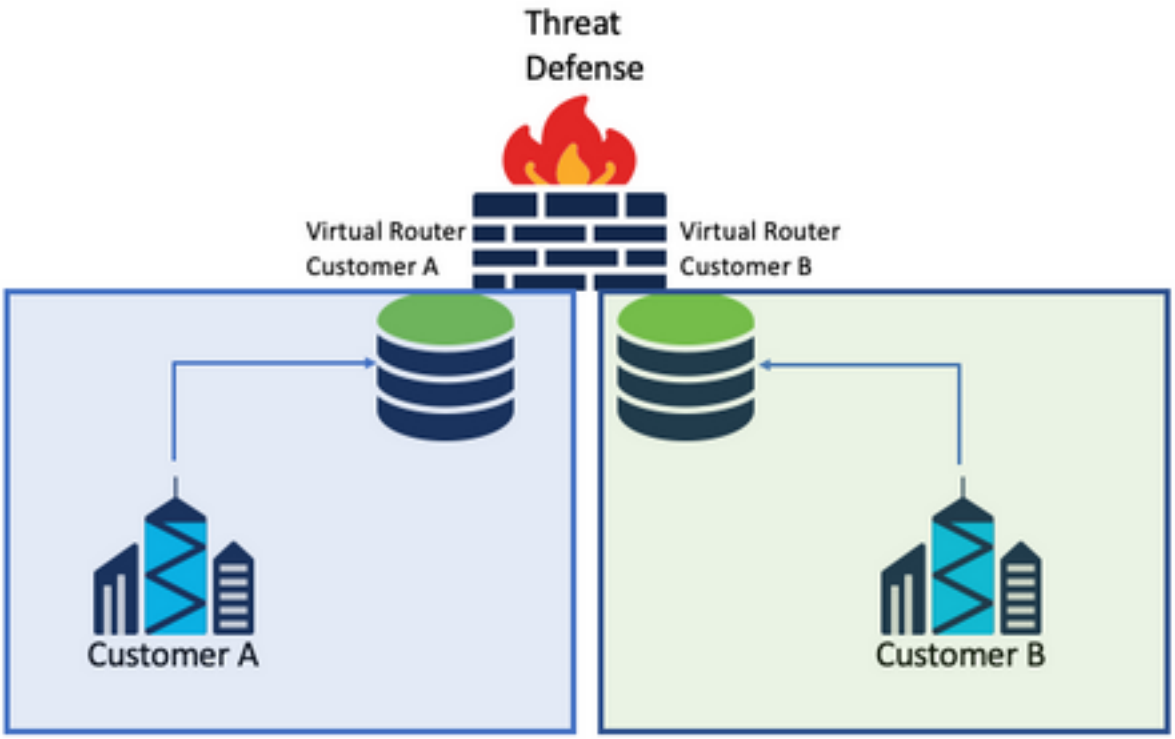
FDMは、仮想ルータ上で完全なCRUD操作をサポートします。

仮想ルータのコールのパスは、 **Devices > Routing > virtualrouters**

使用例

サービス プロバイダー

別々のルーティングテーブルでは、2つのネットワークは互いに関連しておらず、それらの間で通信が行われません。

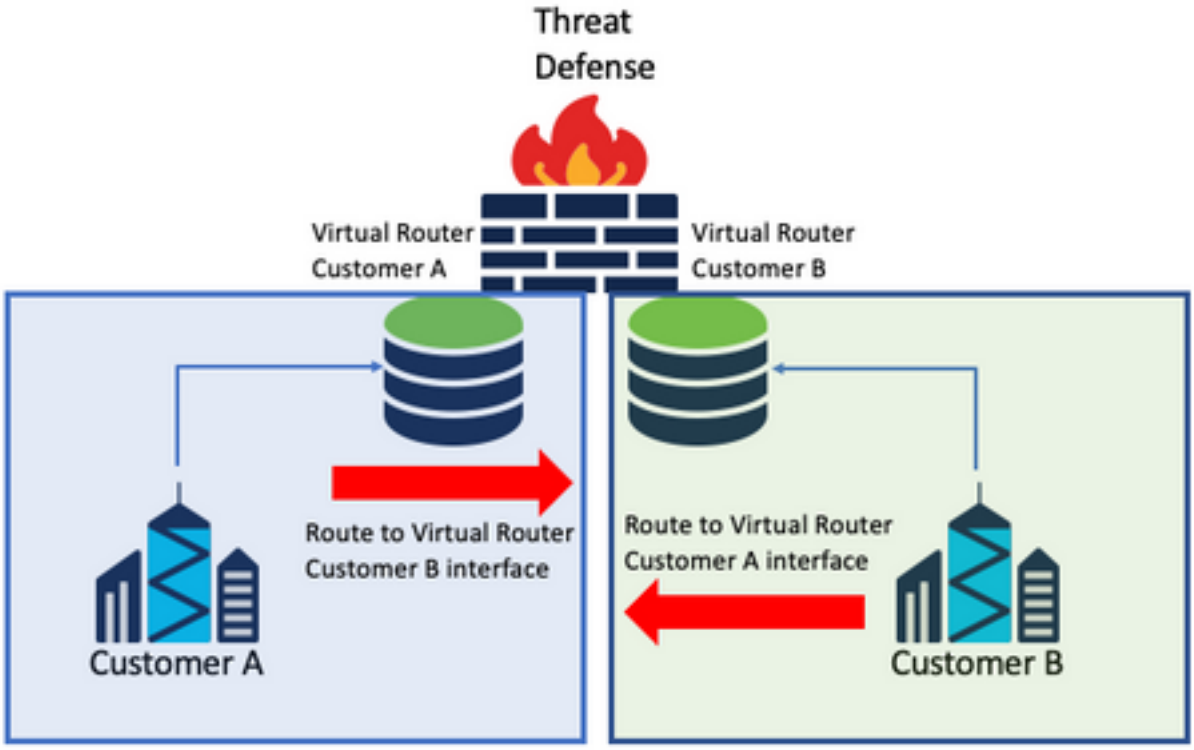


考慮事項:

- このシナリオでは、特別な考慮事項はありません。

共有リソース

2台の仮想ルータを相互接続して、各ルータからのリソースを共有し、 **Customer A** から **Customer B** その逆も同様です



考慮事項:

- 各仮想ルータで、他の仮想ルータのインターフェイスを使用して宛先ネットワークを指すスタティックルートを設定します。

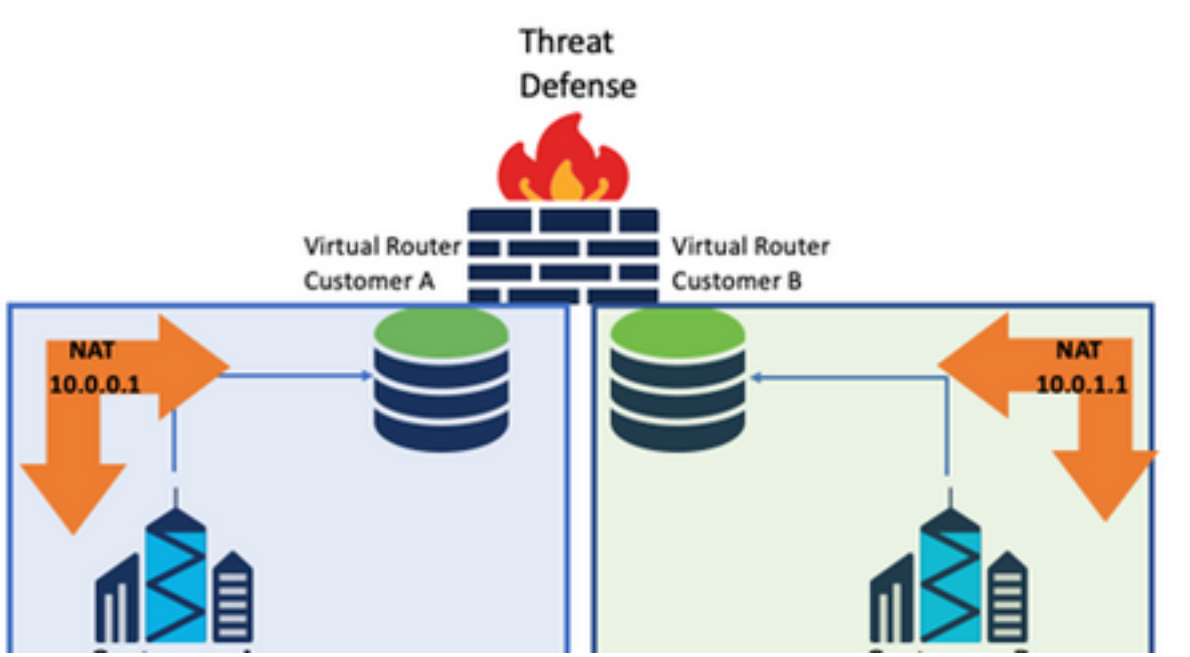
例：

仮想ルータ内で **Customer A**を使用してルートを宛先として追加し、 **Customer B** IPアドレスを持たないインターフェイスをゲートウェイとして使用します(これは不要で、 **route leaking** ）。

同じプロセスを繰り返す **Customer B**.

ホストとのオーバーラップネットワークは相互に通信する

同じネットワークアドレスを持ち、それらの間でトラフィックが交換される2つの仮想ルータがあります。



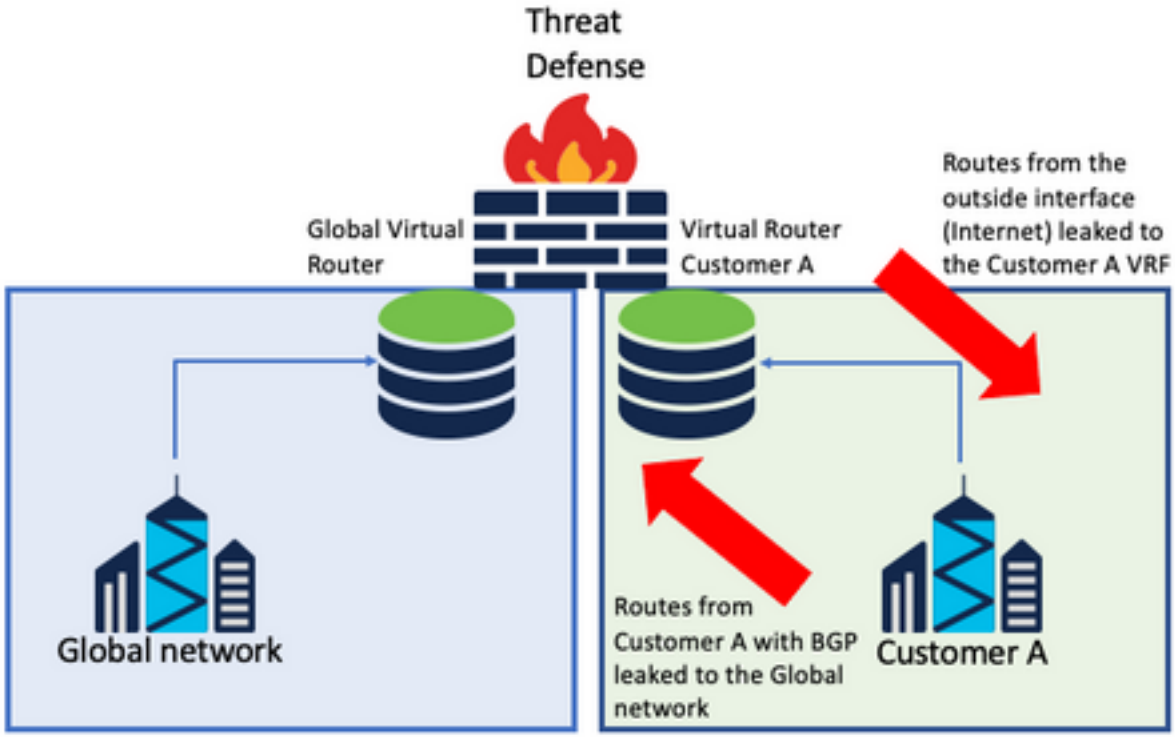
考慮事項:

2つのネットワーク間で通信するには、送信元IPアドレスを上書きするように2回のNATを設定し、偽のIPアドレスを設定します。

BGPルート漏出

ユーザ定義仮想ルータが1つあり、その仮想ルータからのルートをグローバル仮想ルータにリークする必要があります。

外部インターフェイスは、グローバルインターフェイスからユーザ定義仮想ルータに漏出するルートを作成します。



考慮事項:

- FTDのバージョンが7.1以降であることを確認します。
- Import/Exportオプションは、 **BGP > IPv4** を選択をします。
- 配布にはルートマップを使用します。

確認

仮想ルータが作成されたことを確認するには、次のコマンドを使用します。

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

トラブルシューティング

VRFに関する情報の収集と診断に必要なコマンドは次のとおりです。

すべてのVRF

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

グローバルVRF

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

ユーザ定義のVRF

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

関連するリンク

Cisco Secure Firewall Management Centerデバイス設定ガイド、7.2 – 仮想ルータCisco Secure Firewall Management Center – シスコ

Cisco Secure Firewall Device Managerコンフィギュレーションガイド、バージョン7.2 – 仮想ルータCisco Secure Firewall Threat Defense – シスコ

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。