Comprendre le VRF (routeur virtuel) sur la défense pare-feu sécurisée

Table des matières

Introduction

Ce document décrit **Virtual Routing and Forwarding (VRF)** dans le module Cisco **Secure Firewall Threat Defense (FTD)**.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco **Secure Firewall Threat Defense (FTD)**Protection pare-feu contre les menaces (FTD)
- **Virtual Routing and Forwarding (VRF)**
- Protocoles de routage dynamique (OSPF, BGP)

Licences

Aucune exigence de licence spécifique, la licence de base est suffisante

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les **Virtual Routing and Forwarding (VRF)** a été ajoutée à la version 6.6 du logiciel FTD.

Les avantages de cette fonction sont les suivants :

- Séparation des tables de routage
- Segments de réseau avec des chevauchements dans les espaces d'adressage IP
- VRF-lite
- Prise en charge multiinstance FXOS pour les cas d'utilisation de migration à contextes multiples
- BGP **Route Leak Support-v4v6** et BGPv6 **VTI Support** ont été ajoutées dans la version 7.1 du logiciel FTD.

Présentation des fonctionnalités

Prise en charge VRF

Périphérique	Nombre maximal de routeurs virtuels
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
FTD virtuel	30
ISA 3000	10(7.0+)

Limites VRF par lame en mode natif

Politiques de routage

Politiques	VRF global	VRF utilisateur
Routage statique	✓	✓
OSPFv2	✓	✓

OSPFv3	✓	✖
DÉCHIRURE	✓	✖
BGPv4	✓	✓
BGPv6	✓	✓ (7,1+)
IRB (BVI)	✓	✓
EIGRP	✓	✖

Chevauchement de réseaux

Politiques	Non-chevauchement	Chevauchemen réseaux
Routage et IRB	✓	✓
AVC	✓	✓
Déchiffrement SSL	✓	✓
Détection des intrusions et des programmes malveillants (IPS et politique de fichiers)	✓	✓
VPN	✓	✓
Analyse des événements liés aux programmes malveillants (profils d'hôtes, IoC, trajectoire des fichiers)	✓	✖
Informations sur les menaces (TID)	✓	✖

Configuration

FMC

Étape 1. Naviguez jusqu'à **Devices > Device Management** et modifiez le FTD à configurer.

Étape 2. Accédez à l'onglet **Routing**

Étape 3. Cliquer **Manage Virtual Routers** .

Étape 4. Cliquer **Add Virtual Router** .

Étape 5. Dans la zone Ajouter un routeur virtuel, entrez un nom et une description pour le routeur virtuel.

Étape 6. Cliquer **Ok** .

Étape 7. Pour ajouter des interfaces, sélectionnez l'interface sous l'onglet **Available Interfaces** , puis cliquez sur **Add** .

Étape 8. Configurer le routage dans le routeur virtuel

- OSPF
- DÉCHIRURE
- BGP
- Routage statique
- Multidiffusion

FDM

Étape 1. Naviguez jusqu'à **Device > Routing** .

Étape 2.

- Si aucun routeur virtuel n'est créé, cliquez sur **Add Multiple Virtual Routers** , puis cliquez sur **Create First Customer Virtual Router** .
- Cliquez sur le bouton + en haut de la liste des routeurs virtuels pour en créer un nouveau.

Étape 3. Dans la **Add Virtual Router** , sélectionnez une option. Entrez le nom et la description du routeur virtuel.

Étape 4. Cliquez sur + pour sélectionner chaque interface qui doit faire partie du routeur virtuel.

Étape 5. Cliquer **Ok** .

Étape 6. Configurez le routage dans le **Virtual Router**.

- OSPF
- DÉCHIRURE
- BGP
- Routage statique
- Multidiffusion

API REST

FMC

Le FMC prend en charge CRUD les opérations sur les routeurs virtuels.

Le chemin des appels des routeurs virtuels est sous **Devices > Routing > virtualrouters**

FDM

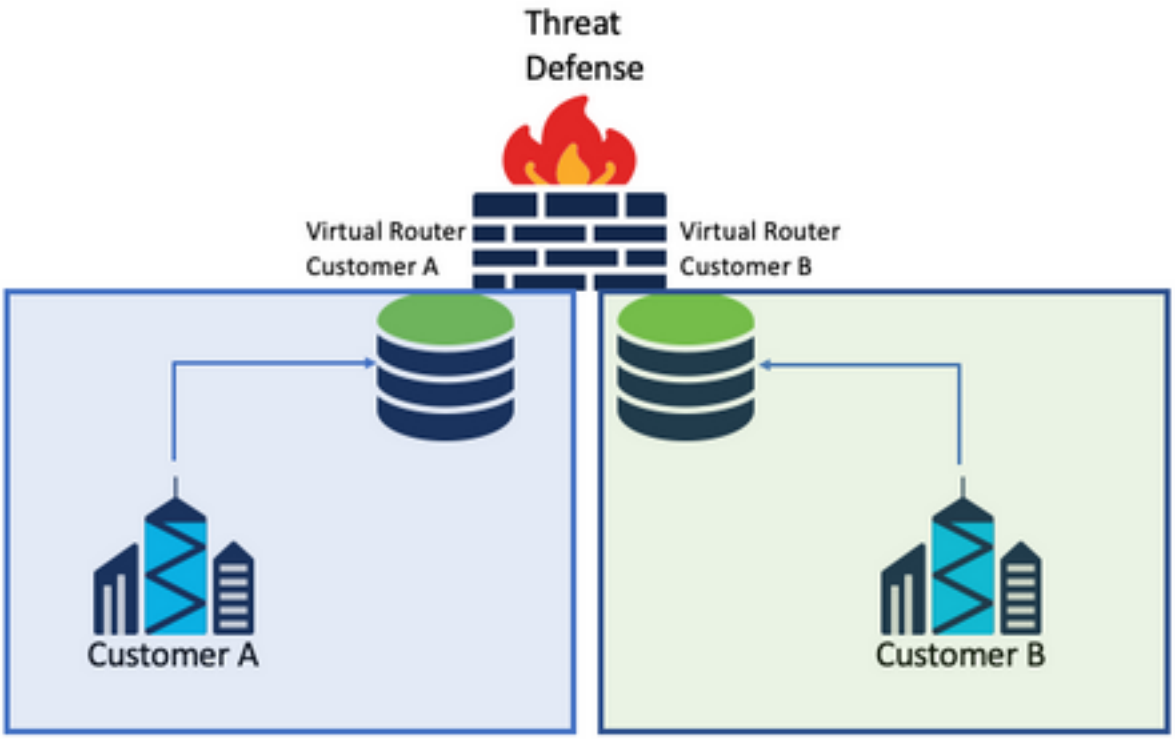
Le FDM prend en charge les opérations CRUD complètes sur les routeurs virtuels.

Le chemin des appels des routeurs virtuels est sous **Devices > Routing > virtualrouters**

Scénarios :

Fournisseur de services

Dans des tables de routage distinctes, deux réseaux ne sont pas liés et aucune communication n’existe entre eux.

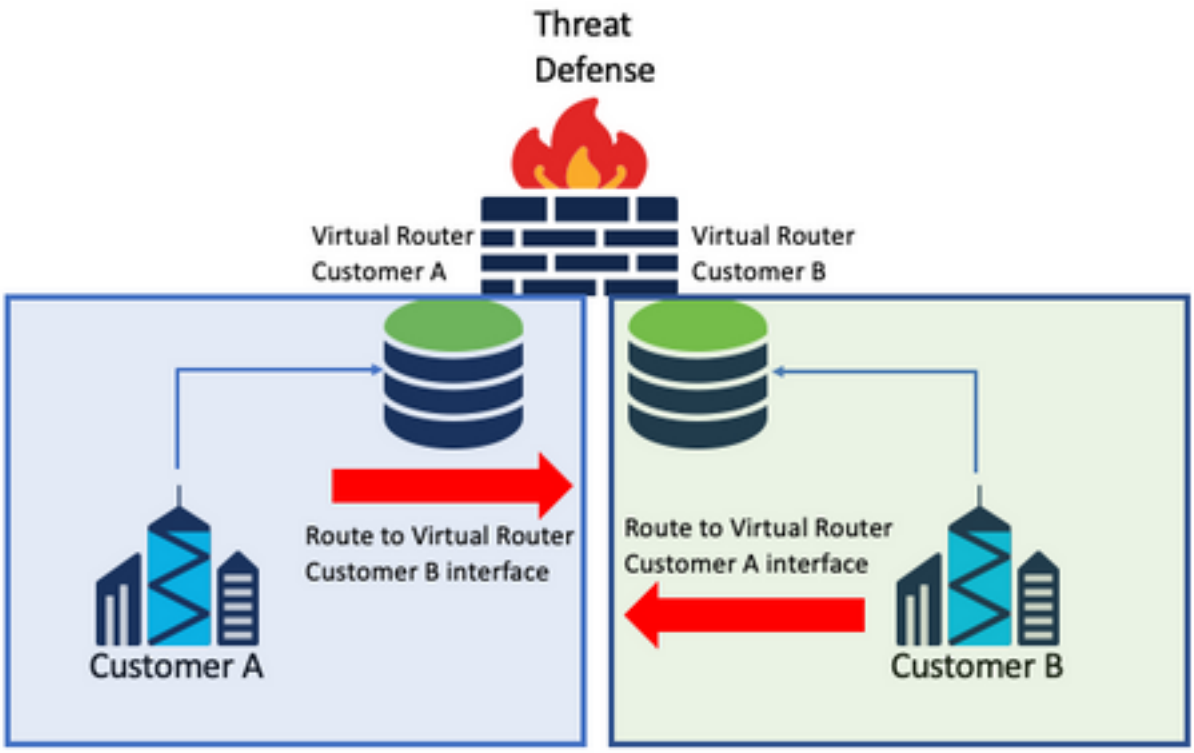


Considérations:

- Il n'y a pas de considérations spéciales dans ce scénario.

Ressources partagées

Interconnectez deux routeurs virtuels pour partager les ressources de chacun d'eux et bénéficier d'une connectivité à partir de **Customer A** par **Customer B** et vice versa.



Considérations:

- Dans chaque routeur virtuel, configurez une route statique qui pointe vers le réseau de destination avec l'interface de l'autre routeur virtuel.

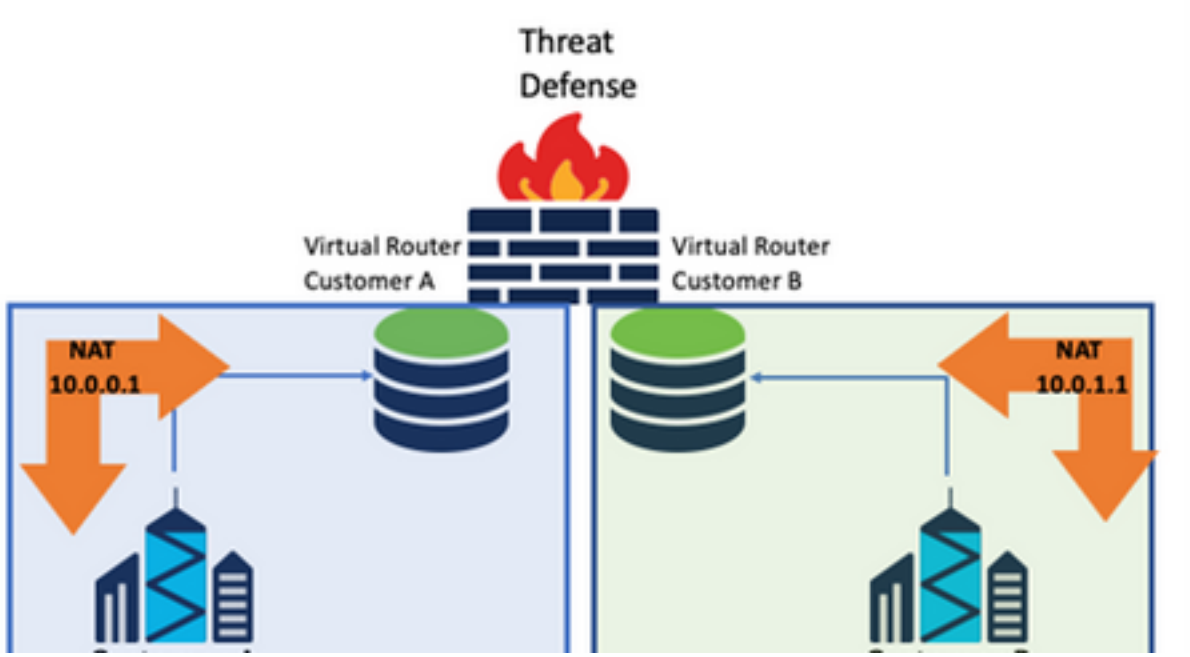
Exemple :

Dans le routeur virtuel pour **Customer A**, ajoutez une route avec comme destination le **Customer B** sans adresse IP en tant que passerelle (ce n'est pas nécessaire, c'est ce que l'on appelle **route leaking** .

Répétez le même processus pour **Customer B**.

Chevauchement du réseau avec les hôtes communiquant entre eux

Il existe deux routeurs virtuels avec les mêmes adresses réseau et un échange de trafic entre eux.



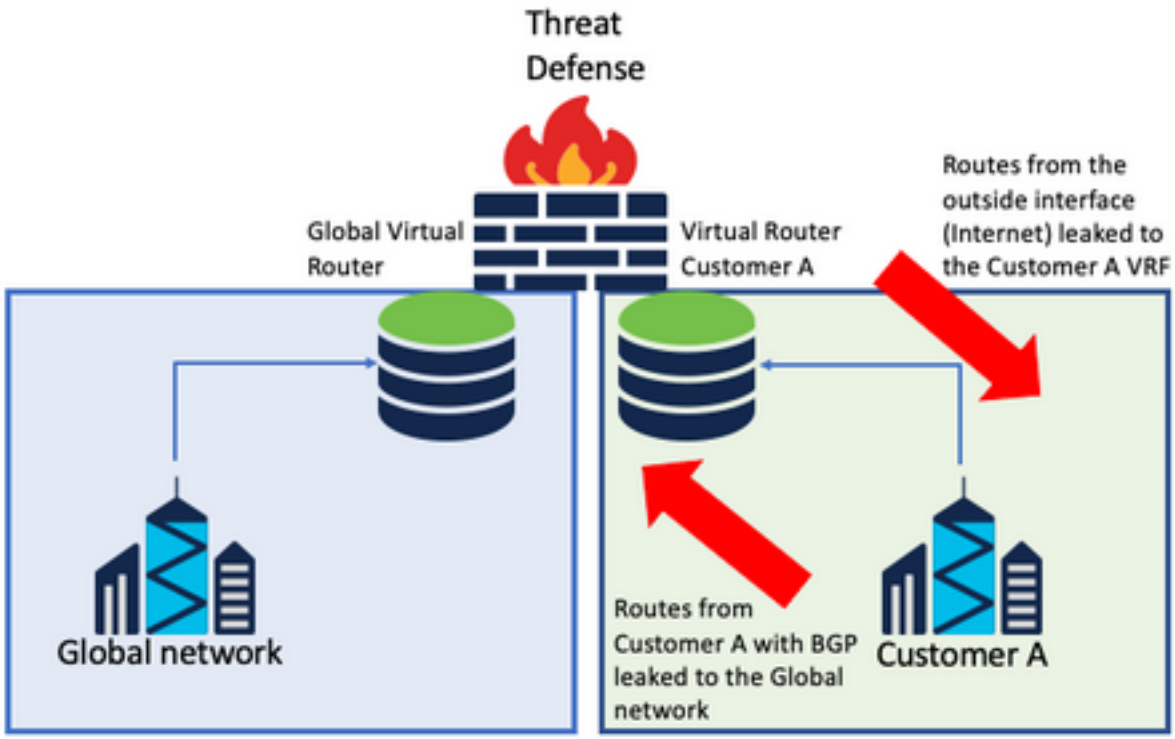
Considérations:

Afin d'avoir une communication entre les 2 réseaux, configurez une NAT deux fois pour remplacer l'adresse IP source et mettre une fausse adresse IP.

Fuite de route BGP

Il existe un routeur virtuel défini par l'utilisateur et les routes de ce routeur virtuel doivent être transmises au routeur virtuel global.

L'interface externe achemine l'interface globale vers le routeur virtuel défini par l'utilisateur.



Considérations:

- Assurez-vous que la version FTD est 7.1+.
- Utilisez les options **Importer/Exporter** de la **BGP > IPv4** s'affiche.
- Utilisez route-map pour la distribution.

Vérification

Pour vérifier que le routeur virtuel a été créé, utilisez les commandes suivantes :

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

Dépannage

Les commandes nécessaires pour collecter et diagnostiquer des informations sur le VRF sont les suivantes :

Tous les VRF

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

VRF global

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

VRF défini par l'utilisateur

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

Liens connexes

Cisco Secure Firewall Management Center Device Configuration Guide, 7.2 - Routeurs virtuels
Cisco Secure Firewall Management Center - Cisco

Guide de configuration de Cisco Secure Firewall Device Manager, version 7.2 - Routeurs virtuels
Cisco Secure Firewall Threat Defense - Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.