Verständnis von VRF (Virtual Router) auf der sicheren Firewall-Bedrohungsabwehr

Inhalt

Einleitung

In diesem Dokument wird die **Virtual Routing and Forwarding (VRF)** in Cisco **Secure Firewall Threat Defense (FTD)**.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco **Secure Firewall Threat Defense (FTD)**Sichere Firewall-Bedrohungsabwehr (FTD)
- **Virtual Routing and Forwarding (VRF)**
- Dynamic Routing Protocols (OSPF, BGP)

Lizenzierung

Keine spezifische Lizenzanforderung, die Basislizenz ist ausreichend

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Die Fehlermeldung **Virtual Routing and Forwarding (VRF)** wurde in der FTD-Softwareversion 6.6 hinzugefügt.

Diese Funktion bietet die folgenden Vorteile:

- Trennung von Routing-Tabellen
- Netzwerksegmente mit Überschneidungen bei IP-Adressräumen
- VRF-Lite
- FXOS Multi-Instance-Unterstützung für Anwendungsfälle der Multi-Context-Migration
- BGP **Route Leak Support-v4v6** und BGPv6 **VTI Support** Funktionen wurden in der FTD-Softwareversion 7.1 hinzugefügt.

Funktionsüberblick

VRF-Unterstützung

"Slot0:"	Maximale Anzahl virtueller Router
ASA	10-20
FirePOWER 1000	5-10 x 1010 (7,2+)
Firepower 2100	10-40
Firepower 3100	15-100
Firepower 4100	60-100
Firepower 9300	60-100
Virtuelle FTD	30
ISA 3000	10 (7,0+)

VRF-Grenzwerte pro Blade mit nativem Modus

Routingrichtlinien

Richtlinien	Globales VRF	Benutzer-VRF
Statische Route	✓	✓

OSPFv2	✓	✓
OSPFv3	✓	✖
RIP	✓	✖
BGPv4	✓	✓
BGPv6	✓	✓ (7,1+)
IRB (BVI)	✓	✓
EIGRP	✓	✖

Überlappende Netzwerke

Richtlinien	Nicht überlappend	Überlappende Netzwerke
Routing und IRB	✓	✓
AVC	✓	✓
SSL-Verschlüsselung	✓	✓
Intrusion Detection und Malware Detection (IPS und Dateirichtlinie)	✓	✓
VPN	✓	✓
Malware-Ereignisanalyse (Hostprofile, IoC, File Trajectory)	✓	✖
Threat-Intelligence (TID)	✓	✖

Konfiguration

FMC

Schritt 1: Navigieren Sie zu **Devices > Device Management** , und bearbeiten Sie die FTD, die konfiguriert werden soll.

Schritt 2: Zur Registerkarte navigieren **Routing**

Schritt 3: Klicken Sie auf **Manage Virtual Routers** .

Schritt 4: Klicken Sie auf **Add Virtual Router** .

Schritt 5: Geben Sie im Feld Virtuellen Router hinzufügen einen Namen und eine Beschreibung für den virtuellen Router ein.

Schritt 6: Klicken Sie auf **Ok** .

Schritt 7. Um Schnittstellen hinzuzufügen, wählen Sie die Schnittstelle unter **Available Interfaces** ein, und klicken Sie auf **Add** .

Schritt 8: Konfigurieren Sie das Routing im virtuellen Router.

- OSPF
- RIP
- BGP
- Statisches Routing
- Multicast

FDM

Schritt 1: Navigieren Sie zu **Device > Routing** .

Schritt 2:

- Wenn keine virtuellen Router erstellt wurden, klicken Sie auf **Add Multiple Virtual Routers** , und klicken Sie dann auf **Create First Customer Virtual Router** .
- Klicken Sie auf die Schaltfläche + oben in der Liste der virtuellen Router, um einen neuen zu erstellen.

Schritt 3: Im **Add Virtual Router** Box. Geben Sie den Namen und die Beschreibung des virtuellen Routers ein.

Schritt 4: Klicken Sie auf +, um jede Schnittstelle auszuwählen, die Teil des virtuellen Routers sein soll.

Schritt 5: Klicken Sie auf **Ok** .

Schritt 6: Konfigurieren Sie Routing im **Virtual Router**.

- OSPF
- RIP
- BGP
- Statisches Routing
- Multicast

REST-API

FMC

FMC unterstützt voll CRUD auf virtuellen Routern.

Der Pfad für die Anrufe des virtuellen Routers befindet sich unter **Devices > Routing > virtualrouters**

FDM

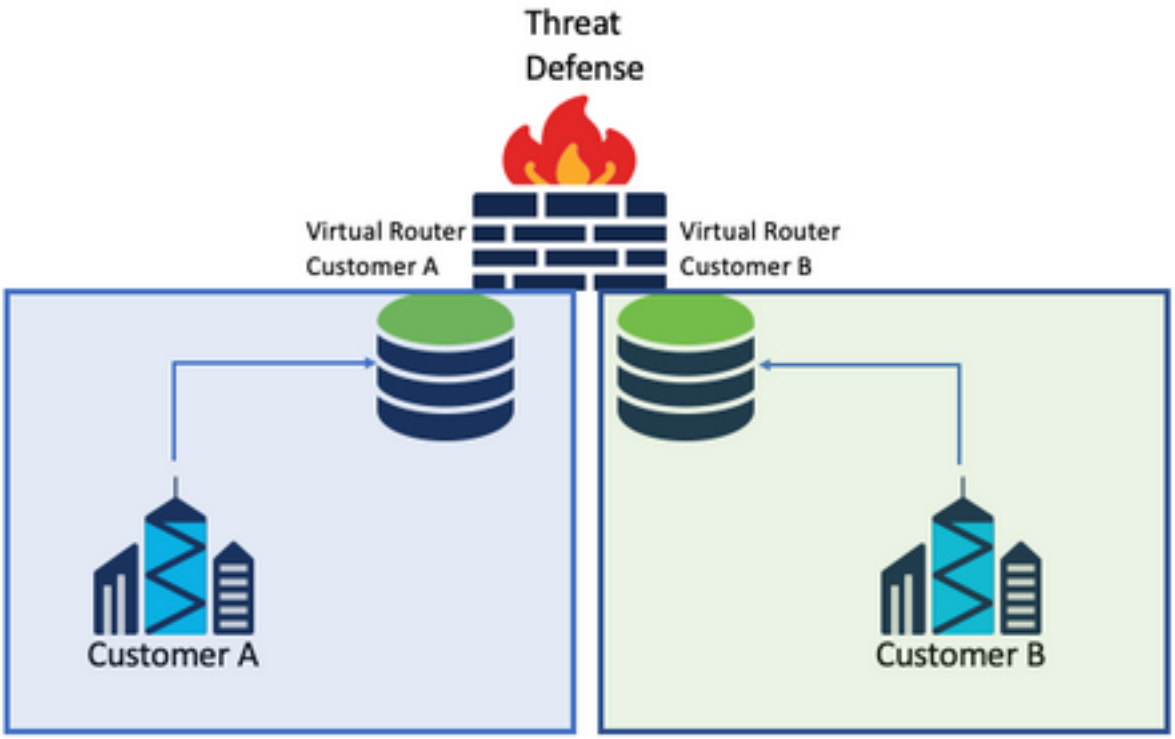
Der FDM unterstützt den vollständigen CRUD-Betrieb auf virtuellen Routern.

Der Pfad für die Anrufe des virtuellen Routers befindet sich unter **Devices > Routing > virtualrouters**

Anwendungsfälle

Service Provider

In separaten Routing-Tabellen sind zwei Netzwerke nicht miteinander verknüpft, und es findet keine Kommunikation zwischen ihnen statt.

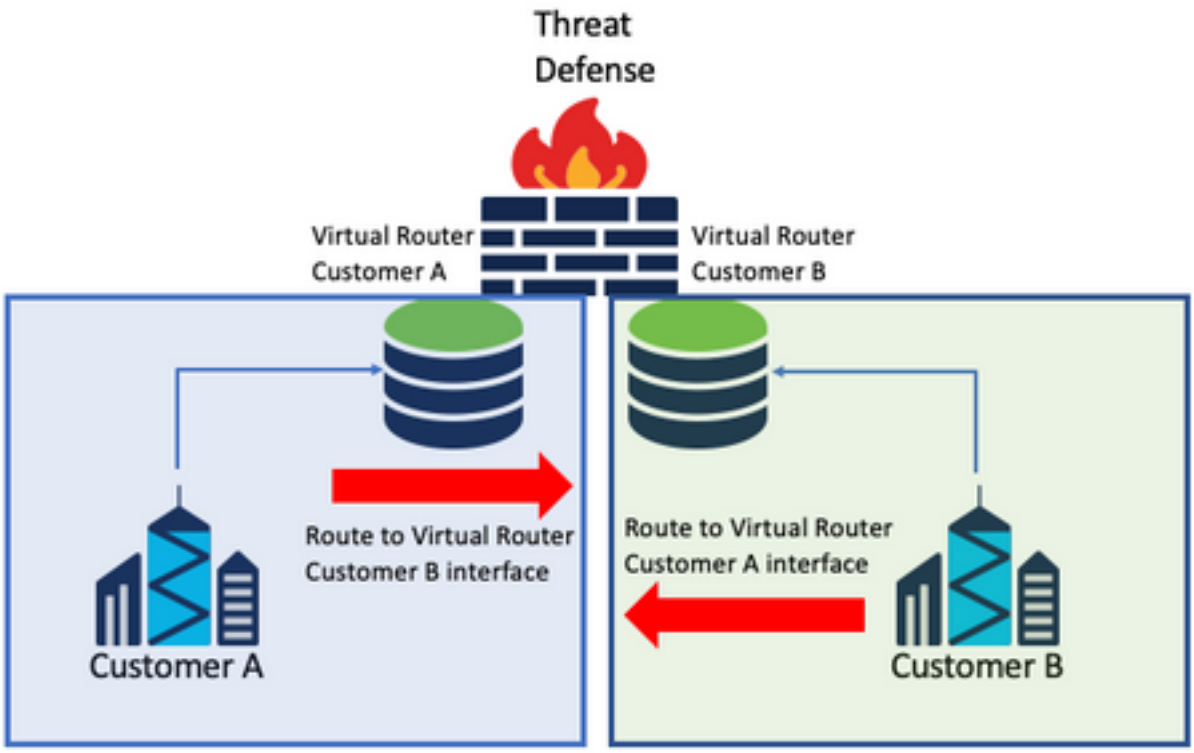


Überlegungen:

- In diesem Szenario gibt es keine besonderen Überlegungen.

Freigegebene Ressourcen

Verbinden Sie zwei virtuelle Router, um Ressourcen von jedem dieser Router freizugeben und Verbindungen von **Customer A** zu **Customer B** und umgekehrt.



Überlegungen:

- Konfigurieren Sie auf jedem virtuellen Router eine statische Route, die mit der Schnittstelle des anderen virtuellen Routers auf das Zielnetzwerk verweist.

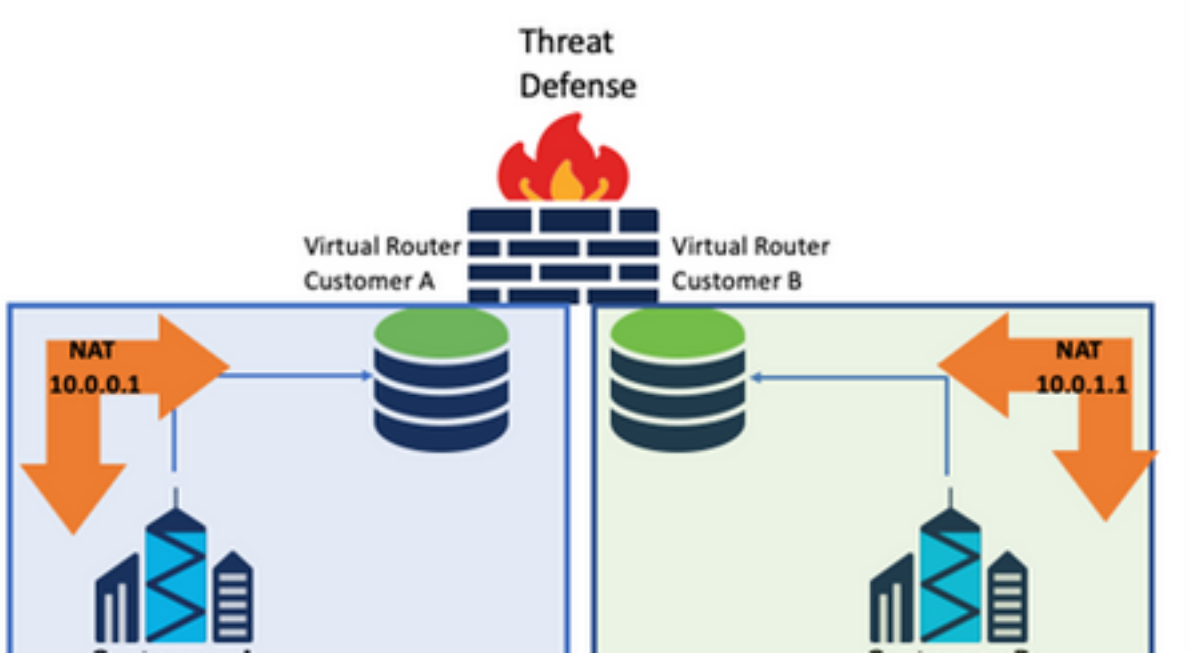
Beispiel:

Im virtuellen Router für **Customer A**, eine Route mit als Ziel der **Customer B** Schnittstelle ohne jegliche IP-Adresse als Gateway (wird nicht benötigt, wird als **route leaking**).

Wiederholen Sie den gleichen Vorgang für **Customer B**.

Überlappendes Netzwerk mit Hosts kommunizieren miteinander

Es gibt zwei virtuelle Router mit denselben Netzwerkadressen und einem Datenaustausch zwischen diesen.



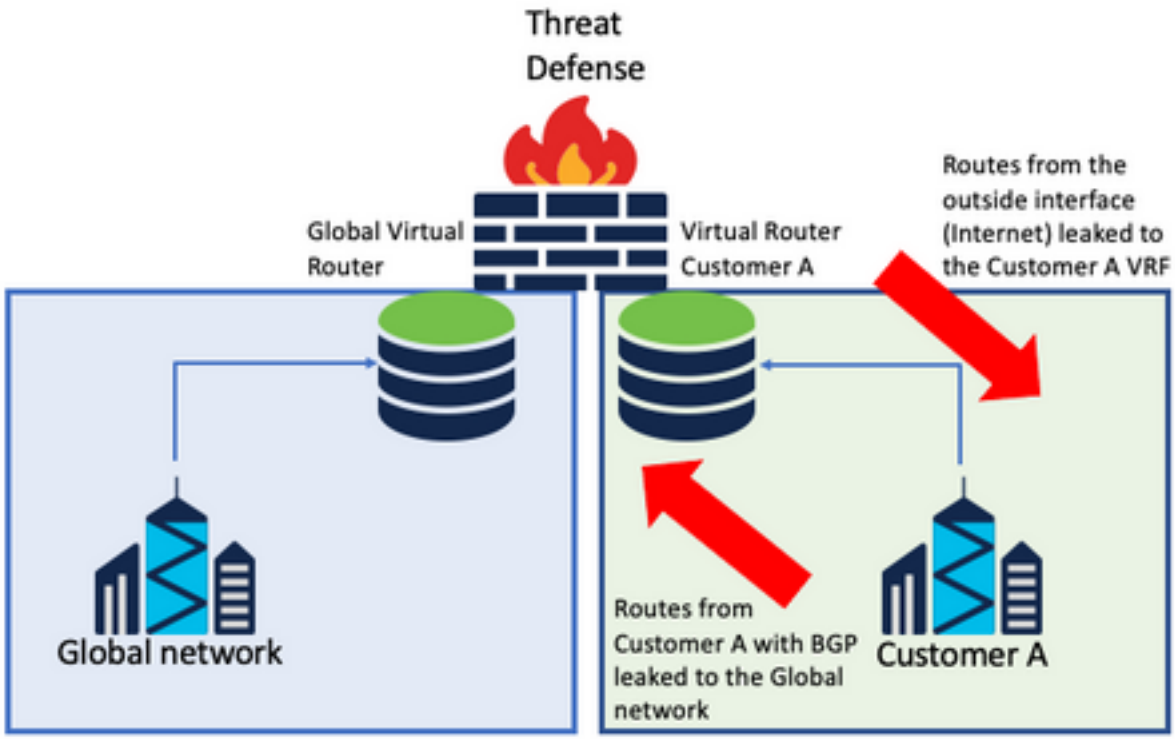
Überlegungen:

Um eine Kommunikation zwischen den beiden Netzwerken zu ermöglichen, konfigurieren Sie eine zweimal vorhandene NAT, um die Quell-IP-Adresse außer Kraft zu setzen, und legen Sie eine gefälschte IP-Adresse fest.

BGP-Route Leaking

Es gibt einen benutzerdefinierten virtuellen Router, dessen Routen an den globalen virtuellen Router geleitet werden müssen.

Die externe Schnittstelle leitet von der globalen Schnittstelle, die an den benutzerdefinierten virtuellen Router weitergeleitet werden soll, weiter.



Überlegungen:

- Vergewissern Sie sich, dass die FTD-Version 7.1+ ist.
- Verwenden Sie die Optionen **Importieren/Exportieren** im **BGP > IPv4** Menü.
- Verwenden Sie route-map zur Verteilung.

Verifizierung

Mit den folgenden Befehlen können Sie überprüfen, ob der virtuelle Router erstellt wurde:

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

Fehlerbehebung

Die Befehle zum Erfassen und Diagnostizieren von VRF-Informationen sind wie folgt:

Alle VRFs

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

Globales VRF

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

Benutzerdefiniertes VRF

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

Verwandte Links

Cisco Secure Firewall Management Center - Gerätekonfigurationsanleitung, 7.2 - Virtuelle Router Cisco Secure Firewall Management Center - Cisco

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.