Entender o VRF (Virtual Router, roteador virtual) na defesa contra ameaças do firewall seguro

Contents

Introduction

Este documento descreve o **Virtual Routing and Forwarding (VRF)** no Cisco **Secure Firewall Threat Defense (FTD)**.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco **Secure Firewall Threat Defense (FTD)**Defesa contra ameaças de firewall (FTD) segura
- **Virtual Routing and Forwarding (VRF)**
- Protocolos de roteamento dinâmico (OSPF, BGP)

Licenciamento

Sem necessidade de licença específica, a licença básica é suficiente

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco **Secure Firewall Threat Defense (FTD)**, **Secure Firewall Management Center (FMC)** versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O **Virtual Routing and Forwarding (VRF)** foi adicionado na versão 6.6 do software FTD.

As vantagens que esse recurso oferece são:

- Segregação de tabelas de roteamento
- Segmentos de rede com sobreposições em espaços de endereços IP
- VRF-lite
- Suporte a várias instâncias de FXOS para casos de uso de migração de vários contextos
- BGP **Route Leak Support-v4v6** e BGPv6 **VTI Support** recursos foram adicionados ao software FTD versão 7.1.

Visão geral do recurso

Suporte a VRF

Dispositivo	Máximo de roteadores virtuais
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 virtual	30
ISA 3000	10(7.0+)

Limites de VRF por blade com modo nativo

Políticas de roteamento

Políticas	VRF global	VRF de usuário
Rota estática	✓	✓
OSPFv2	✓	✓
OSPFv3	✓	✖
RIP	✓	✖

BGPv4	✓	✓
BGPv6	✓	✓ (7.1+)
IRB (BVI)	✓	✓
EIGRP	✓	✖

Redes Sobrepostas

Políticas	Sem sobreposição	Redes Sobrepost
Roteamento e IRB	✓	✓
AVC	✓	✓
Descriptografia SSL	✓	✓
Intrusion and Malware Detection (IPS e política de arquivos)	✓	✓
VPN	✓	✓
Análise de eventos de malware (perfis de host, IoC, trajetória do arquivo)	✓	✖
Inteligência de ameaças (TID)	✓	✖

Configuração

CVP

Etapa 1. Navegue até **Devices > Device Management** e edite o FTD a ser configurado.

Etapa 2. Navegue até a guia **Routing**

Etapa 3. Clique em **Manage Virtual Routers** .

Etapa 4. Clique em **Add Virtual Router** .

Etapa 5. Na caixa Add Virtual Router (Adicionar roteador virtual), insira um nome e uma descrição para o roteador virtual.

Etapa 6. Clique em **Ok** .

Passo 7. Para adicionar interfaces, selecione a interface no **Available Interfaces** e clique em **Add** .

Etapa 8. Configure o roteamento no Roteador Virtual.

- OSPF
- RIP
- BGP
- Roteamento estático
- Multicast

FDM

Etapa 1. Navegue até **Device > Routing** .

Etapa 2.

- Se não houver roteadores virtuais criados, clique em **Add Multiple Virtual Routers** e clique em **Create First Customer Virtual Router** .
- Clique no botão **+** na parte superior da lista de roteadores virtuais para criar um novo.

Etapa 3. No **Add Virtual Router** caixa de diálogo. Digite o nome e a descrição do roteador virtual.

Etapa 4. Clique em **+** para selecionar cada interface que precisa fazer parte do roteador virtual.

Etapa 5. Clique em **Ok** .

Etapa 6. Configure o roteamento no **Virtual Router**.

- OSPF
- RIP
- BGP
- Roteamento estático
- Multicast

API REST

CVP

O CVP apoia a plena CRUD em roteadores virtuais.

O caminho das chamadas dos roteadores virtuais está em **Devices > Routing > virtualrouters**

FDM

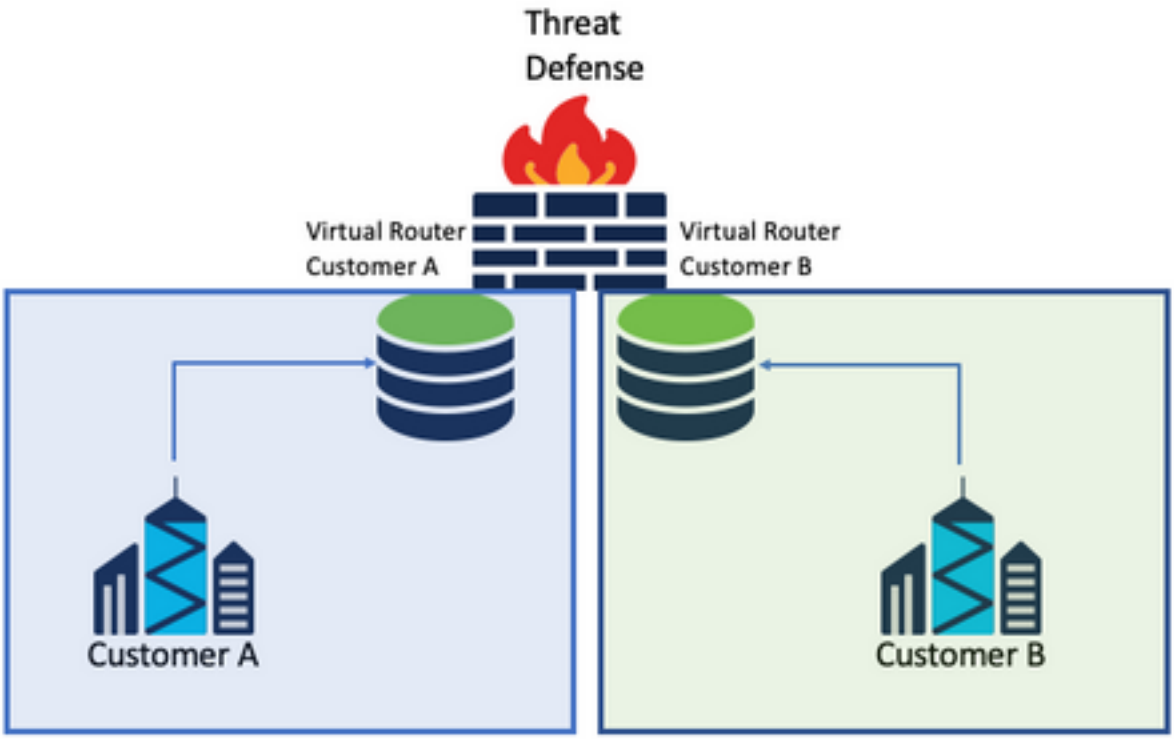
O FDM suporta operações CRUD completas em roteadores virtuais.

O caminho das chamadas dos roteadores virtuais está em **Devices > Routing > virtualrouters**

Casos de uso

Provedor de serviços

Em tabelas de roteamento separadas, duas redes não estão relacionadas entre si e não há comunicação entre elas.

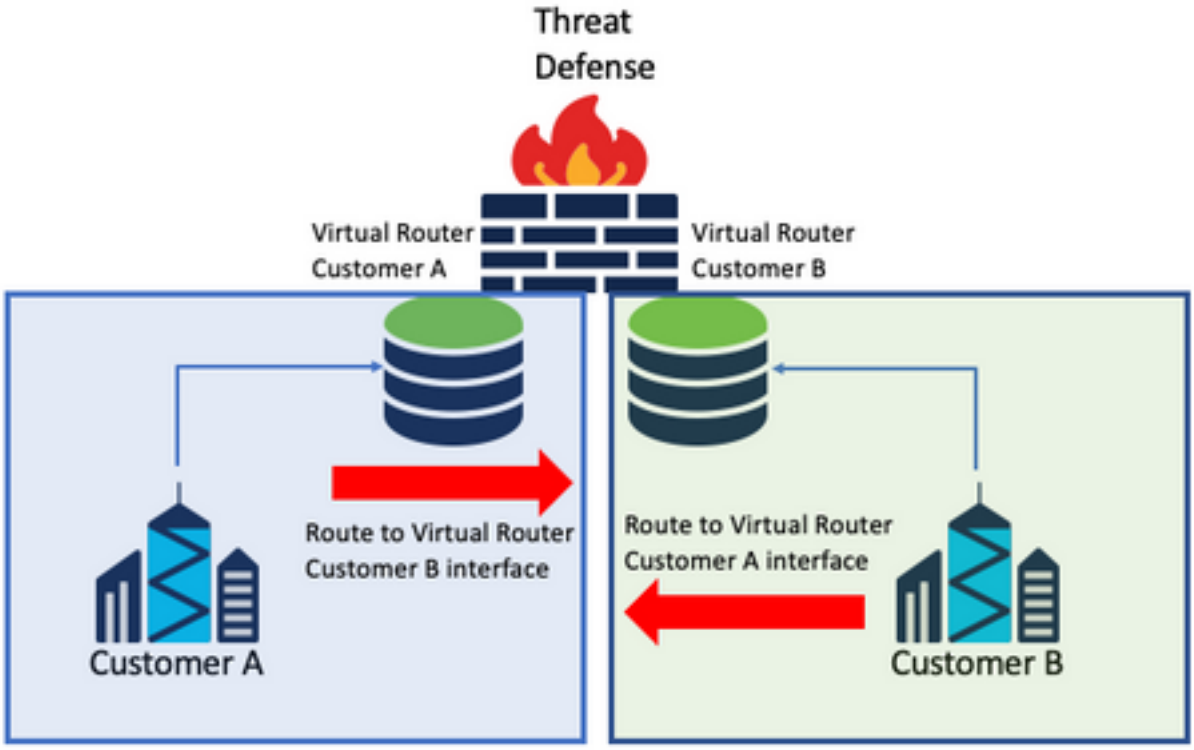


Considerações:

- Não há considerações especiais neste cenário.

Recursos compartilhados

Interconecte dois roteadores virtuais para compartilhar recursos de cada um deles e ter conectividade de **Customer A** para **Customer B** e vice-versa.



Considerações:

- Em cada roteador virtual, configure uma rota estática que aponte para a rede destino com a interface do outro roteador virtual.

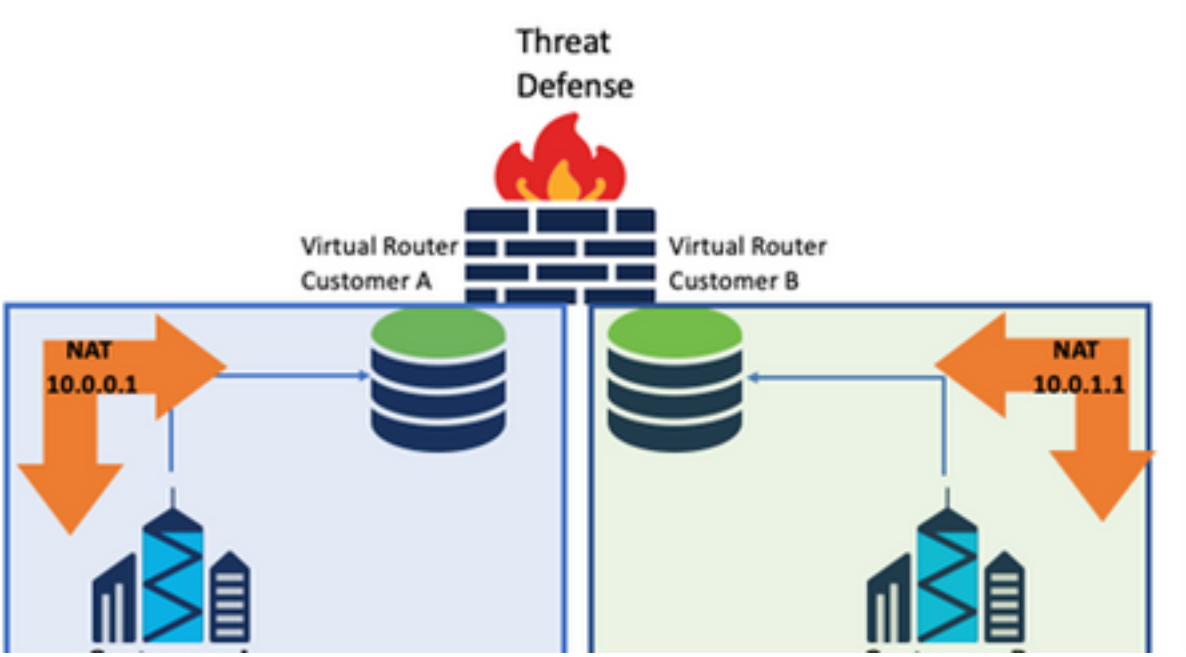
Exemplo:

No roteador virtual para **Customer A**, adicione uma rota com como destino **Customer B** sem nenhum endereço IP como gateway (não é necessário, é conhecido como **route leaking**).

Repita o mesmo processo para **Customer B**.

Rede sobreposta com hosts que se comunicam entre si

Há 2 roteadores virtuais com os mesmos endereços de rede e com intercâmbio de tráfego entre eles.



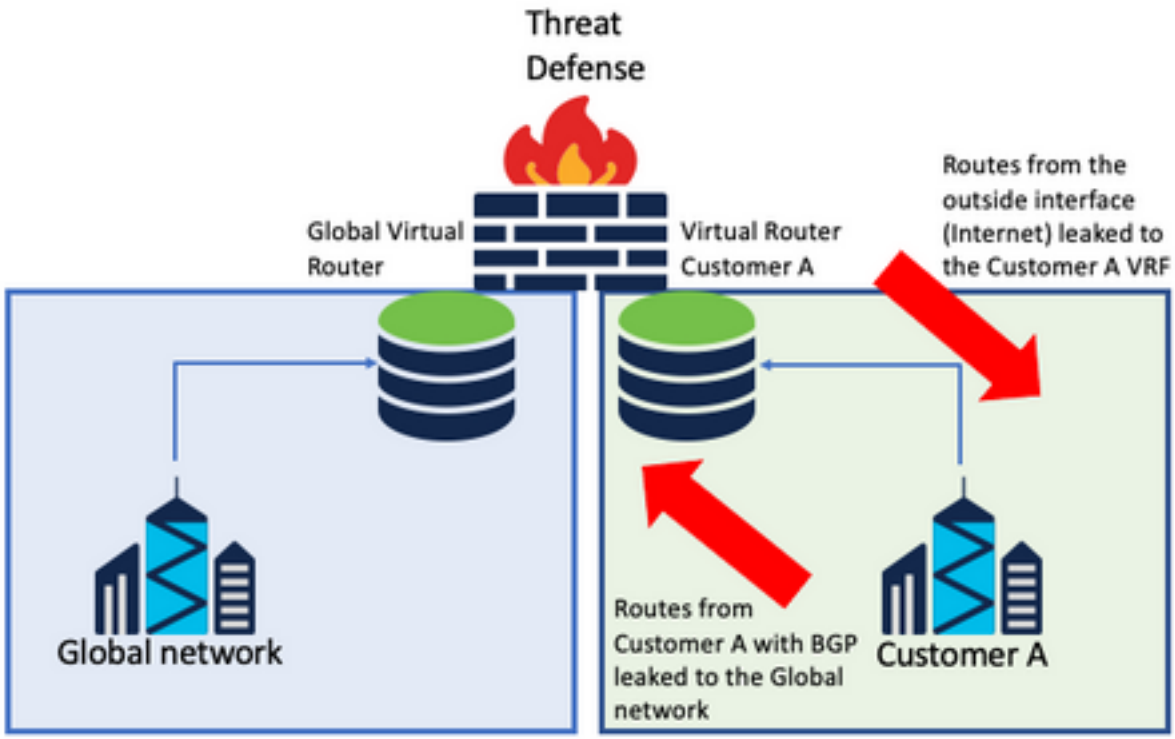
Considerações:

Para ter comunicação entre as duas redes, configure duas vezes o NAT para substituir o endereço IP de origem e colocar um endereço IP falso.

vazamento de rota BGP

Há um roteador virtual definido pelo usuário e as rotas desse roteador virtual precisam vazar para o roteador virtual global.

A interface externa roteia da interface global para vazamento no roteador virtual definido pelo usuário.



Considerações:

- Certifique-se de que a versão do FTD seja 7.1+.
- Use as opções **Importar/Exportar** no **BGP > IPv4** menu.
- Use o mapa de rotas para distribuição.

Verificação

A maneira de verificar se o roteador virtual foi criado é por meio dos comandos:

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

Troubleshooting

Os comandos necessários para coletar e diagnosticar informações sobre VRF são:

Todos os VRFs

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

VRF global

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

VRF definido pelo usuário

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

Links relacionados

Guia de configuração de dispositivos do Cisco Secure Firewall Management Center, 7.2 - Roteadores virtuais Cisco Secure Firewall Management Center - Cisco

Guia de configuração do gerenciador de dispositivos do Cisco Secure Firewall, versão 7.2 - Roteadores virtuais Cisco Secure Firewall Threat Defense - Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.