

Configurar o multipath de BGP na defesa contra ameaças do firewall seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama](#)

[Configuração de BGP](#)

[Configuração de multipath de BGP](#)

[Verificar](#)

[Troubleshooting](#)

[Perguntas e respostas](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar o Border Gateway Protocol (BGP) Multipath no Cisco Secure Firewall Threat Defense.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de BGP no Cisco Secure Firewall Threat Defense (FTD)
- BGP geral
- Cisco Secure Firewall Management Center (FMC)

Componentes Utilizados

As informações neste documento são baseadas nesta versão de software e hardware:

- Cisco FTD versão 7.6
- Cisco FMC versão 7.6

Ressalva: As redes e os endereços IP mencionados neste documento não estão associados a nenhum usuário, grupo ou organização individual. Essa configuração foi criada exclusivamente

para uso em um ambiente de laboratório.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento descreve como configurar o compartilhamento de carga de vários caminhos BGP no Firepower Threat Defense quando uma rota para o mesmo destino for recebida de diferentes roteadores no mesmo AS (por exemplo, o mesmo ISP).

O BGP Multipath permite a instalação na tabela de roteamento IP de vários caminhos BGP de mesmo custo para o mesmo prefixo de destino. O tráfego para o prefixo de destino é compartilhado em todos os caminhos instalados.

Esses caminhos são adicionados à tabela de roteamento juntamente com o melhor caminho para fins de compartilhamento de carga. O BGP Multipath não influencia o processo de seleção do melhor caminho. Por exemplo, um FTD ainda seleciona um caminho como o melhor com base no algoritmo e anuncia esse melhor caminho para seus peers BGP.

Para se qualificar como candidatos a vários caminhos, os caminhos para o mesmo destino devem corresponder ao melhor caminho nestas características:

- Peso
- Preferência local
- Comprimento AS-PATH
- Código de origem
- Discriminador de saída múltipla (MED - Multi Exit Discriminator)

Um dos seguintes:

- AS ou sub-AS vizinho (antes da adição de multipath de BGP)
- AS-PATH (após adição de multipath de BGP)

Determinados recursos de multipath de BGP impõem requisitos adicionais aos candidatos de multipath:

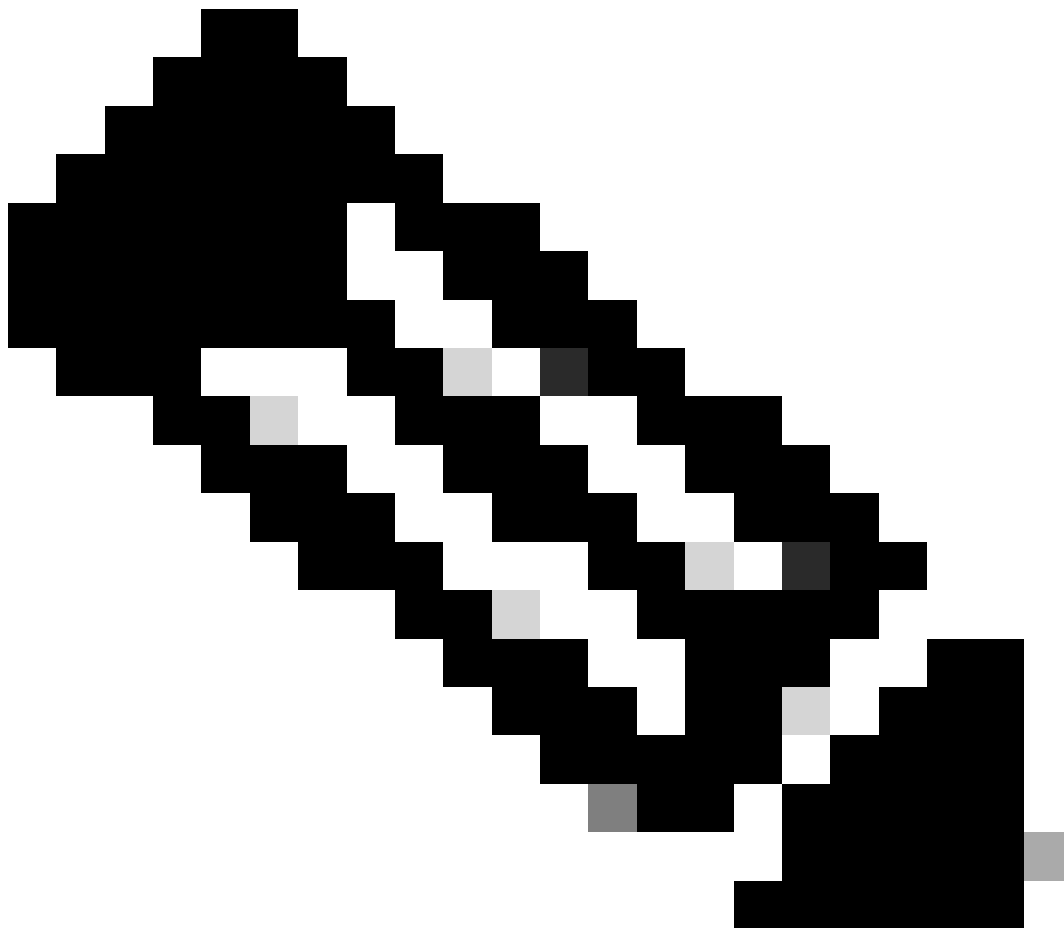
- O caminho deve se originar de um vizinho externo ou externo à confederação (eBGP).
- A métrica IGP para o próximo salto BGP deve corresponder à métrica IGP do melhor caminho.

Para candidatos de multipath de BGP interno (iBGP), estes requisitos adicionais se aplicam:

- O caminho deve ser aprendido com um vizinho interno (iBGP).
- A métrica IGP para o próximo salto de BGP deve corresponder à métrica IGP dos melhores caminhos, a menos que o roteador esteja definido para multicaminho iBGP de custo

desigual.

O BGP insere até n os caminhos recebidos mais recentemente de candidatos de vários caminhos na tabela de roteamento IP, onde n é o número de rotas a serem instaladas na tabela de roteamento, conforme especificado quando você configura o BGP Multipath. O intervalo de valores para n é de 1 a 8 para FTD. O valor padrão, quando multipath está desabilitado, é 1.



Note: O seguinte-salto-auto equivalente é executado no melhor caminho que está selecionado entre multipath de eBGP antes que esteja enviado aos peers internos.

Configurar

Diagrama

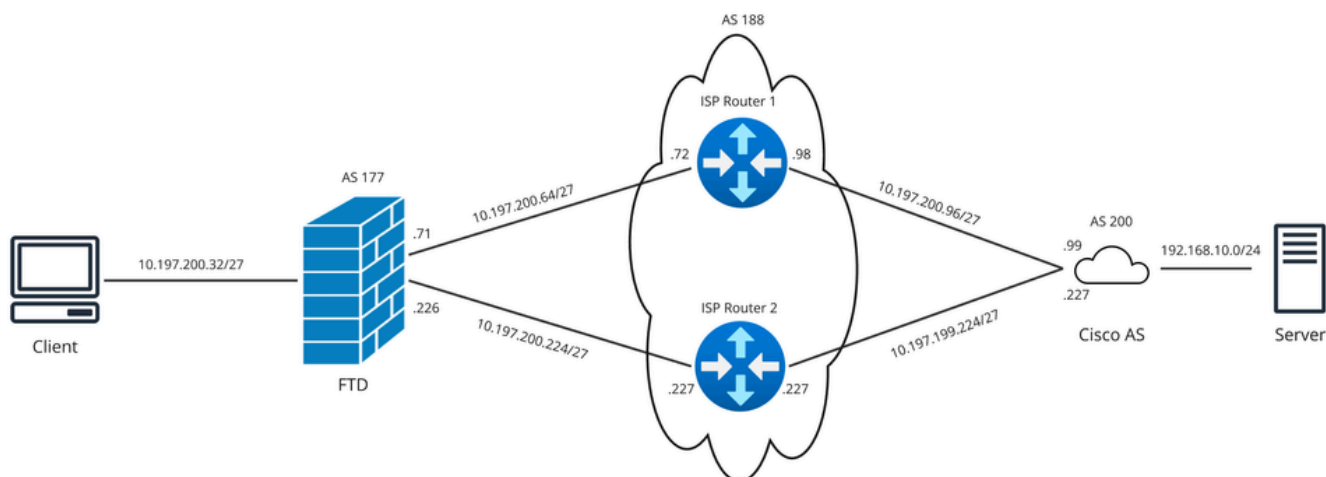
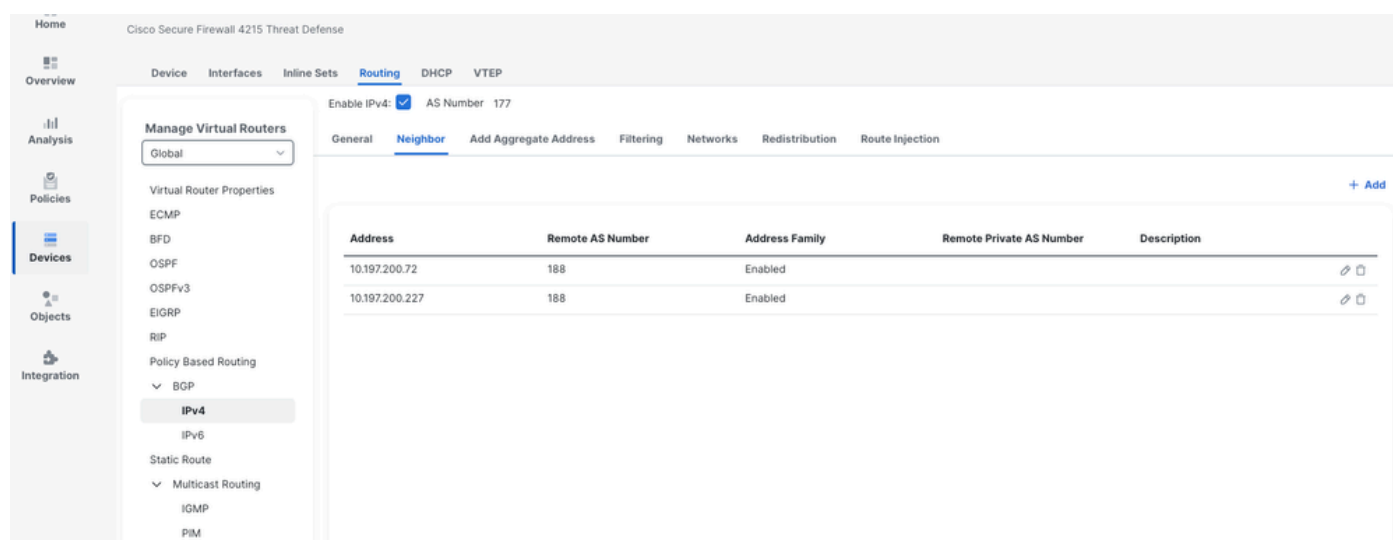


Diagrama de Rede

Configuração de BGP

Navegue até Devices > Device management > Edit Device > Routing > BGP > IPv4 para configurar o BGP depois de habilitá-lo.



Configuração de BGP

Configuração BGP de LINA:

```
router bgp 177
  bgp log-neighbor-changes
  bgp router-id 1.1.x.x
  bgp router-id vrf auto-assign
  address-family ipv4 unicast
    neighbor 10.197.200.72 remote-as 188
    neighbor 10.197.200.72 transport path-mtu-discovery disable
    neighbor 10.197.200.72 activate
    neighbor 10.197.200.227 remote-as 188
    neighbor 10.197.200.227 transport path-mtu-discovery disable
    neighbor 10.197.200.227 activate
  no auto-summary
```

```
no synchronization
exit-address-family
!
```

Dois vizinhos BGP do mesmo AS:

```
ftd1# show bgp summary
BGP router identifier 1.1.x.x, local AS number 177
BGP table version is 9, main routing table version 9
2 network entries using 400 bytes of memory
4 path entries using 320 bytes of memory
1/1 BGP path/bestpath attribute entries using 208 bytes of memory
1 BGP AS-PATH entries using 40 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 968 total bytes of memory
BGP activity 4/2 prefixes, 10/6 paths, scan interval 60 secs
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.197.200.72	4	188	67	66	9	0	0	01:10:15	1
10.197.200.227	4	188	60	60	9	0	0	01:00:56	1

Observe que há duas rotas válidas recebidas para a mesma rede destino, uma de cada vizinho.

```
ftd1# show bgp 192.168.10.0 255.255.255.0
BGP routing table entry for 192.168.10.0/24, version 9
Paths: (2 available, best #2, table default)
  Advertised to update-groups: 3
  188 200
    10.197.200.227 from 10.197.200.227 (3.3.x.x)
      Origin incomplete, localpref 100, valid, external
  188 200
    10.197.200.72 from 10.197.200.72 (2.2.x.x)
      Origin incomplete, localpref 100, valid, external, best
```

Você pode ver que o melhor caminho selecionado e instalado na tabela de roteamento é aquele recebido do vizinho 10.197.200.72.

```
ftd1# show route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF
Gateway of last resort is not set
```

B 192.168.10.0 255.255.255.0 [20/0] via 10.197.200.72, 00:01:55

Configuração de multipath de BGP

Configure o multipath de BGP em Devices > Device management > Edit Device > Routing > BGP > IPv4 > Edit Forward Packets Over Multiple Paths.

The screenshot shows the Cisco Secure Firewall 4215 Threat Defense configuration interface. The left sidebar contains navigation options: Overview, Analysis, Policies, Devices, Objects, and Integration. The main panel is titled 'Cisco Secure Firewall 4215 Threat Defense' and has tabs for Device, Interfaces, Inline Sets, Routing, DHCP, and VTEP. The 'Routing' tab is selected, and the 'General' sub-tab is active. The 'Enable IPv4' checkbox is checked, and the 'AS Number' is set to 177. The 'Forward Packets Over Multiple Paths' section is highlighted with a red box, showing the 'Number of Paths' set to 1 and the 'IBGP number of paths' set to 1.

Setting	Value
Learned Route Map	
Administrative Route Distances	
External	20
Internal	200
Local	200
Routes and Synchronization	
Generate default routes	No
Summarize subnet routes into network level routes	No
Advertise inactive routes	Yes
Synchronize between BGP and IGP systems	No
Redistribute IBGP into IGP	No
(Use filtering to limit the number of prefixes that are redistributed)	
Forward Packets Over Multiple Paths	
Number of Paths	1
IBGP number of paths	1

Multipath de BGP no FMC

The screenshot shows the Cisco Secure Firewall 4215 Threat Defense configuration interface. The left sidebar contains navigation options: Overview, Analysis, Policies, Devices, Objects, and Integration. The main panel is titled 'Cisco Secure Firewall 4215 Threat Defense' and has tabs for Device, Interfaces, Inline Sets, Routing, DHCP, and VTEP. The 'Routing' tab is selected, and the 'General' sub-tab is active. The 'Enable IPv4' checkbox is checked, and the 'AS Number' is set to 177. The 'Forward Packets Over Multiple Paths' section is highlighted with a red box, showing the 'Number of Paths' set to 1 and the 'IBGP number of paths' set to 1. A dialog box titled 'Edit Forward packets Over Multiple Paths' is open, showing the 'Number of Paths' field set to 2 and the 'IBGP Number of Paths' field set to 1. The dialog box has 'Cancel' and 'OK' buttons.

Setting	Value
Learned Route Map	
Administrative Route D	
External	
Internal	
Local	
Routes and Synchroniz	
Generate default routes	No
Summarize subnet routes into network level routes	No
Advertise inactive routes	Yes
Synchronize between BGP and IGP systems	No
Redistribute IBGP into IGP	No
(Use filtering to limit the number of prefixes that are redistributed)	
Forward Packets Over Multiple Paths	
Number of Paths	1
IBGP number of paths	1

Multipath de BGP no FMC

Salve as alterações e Implante.

Verificar

Configuração de BGP de LINA após ativar multipath:

<#root>

```
ftd1# sh run router
router bgp 177
bgp log-neighbor-changes
bgp router-id 1.1.x.x
bgp router-id vrf auto-assign
address-family ipv4 unicast
neighbor 10.197.200.72 remote-as 188
neighbor 10.197.200.72 transport path-mtu-discovery disable
neighbor 10.197.200.72 activate
neighbor 10.197.200.227 remote-as 188
neighbor 10.197.200.227 transport path-mtu-discovery disable
neighbor 10.197.200.227 activate
```

maximum-paths 2

```
no auto-summary
no synchronization
exit-address-family
```

Observe o m antes de uma das rotas que indicam multipath

<#root>

```
ftd1# show bgp
```

```
BGP table version is 11, local router ID is 1.1.x.x
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Network Next Hop Metric LocPrf Weight Path
```

```
*m 192.168.10.0 10.197.200.227 0 188 200 ?
```

```
*> 10.197.200.72 0 188 200 ?
```

```
ftd1# show bgp 192.168.10.0 255.255.255.0
BGP routing table entry for 192.168.10.0/24, version 11
Paths: (2 available, best #2, table default)
Multipath: eBGP
Advertised to update-groups: 3
188 200
10.197.200.227 from 10.197.200.227 (3.3.x.x)
Origin incomplete, localpref 100, valid, external,
```

multipath

```
188 200
10.197.200.72 from 10.197.200.72 (2.2.x.x)
Origin incomplete, localpref 100, valid, external,
```

multipath

, best

Observe que, agora, há duas rotas para o mesmo destino instaladas na tabela de roteamento depois de ativar o multipath de BGP.

<#root>

```
ftd1# show route bgp
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, + - replicated route

SI - Static InterVRF

Gateway of last resort is not set

```
B 192.168.10.0 255.255.255.0 [20/0] via 10.197.200.227, 00:01:17
```

```
[20/0] via 10.197.200.72, 00:01:17
```

Troubleshooting

1. Verificar a Configuração do BGP:

Use o comando `show bgp` para verificar a tabela BGP e garantir que vários caminhos sejam marcados como `multipath`.

Confirme se `Number of Paths` está configurado para permitir vários caminhos.

2. Verificar Atributos do Caminho:

Assegure-se de que os caminhos tenham atributos BGP iguais necessários para `multipath`; como peso, preferência local, Comprimento do caminho AS e assim por diante.

3. Verificação de Compartilhamento de Carga:

Use o comando `show route` para verificar se os caminhos estão sendo usados para o compartilhamento de carga. A saída deve mostrar vários caminhos para o mesmo destino.

Perguntas e respostas

1.O comando `bgp bestpath as-path multipath-relax` é suportado no FTD através da configuração Flex para compartilhamento de carga?

Não, já existe uma melhoria para que isso seja suportado no FTD/ASA. ID de bug da Cisco [CSCvw16654](#)

Informações Relacionadas

[Identificar e Solucionar Problemas Comuns do BGP](#)

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.