Configurar BGP AS Override no Firewall Seguro

Contents

Introdução

Este documento descreve como configurar a Substituição do Sistema Autônomo (AS) BGP no Cisco Secure Firewall Threat Defense.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- BGP (Border Gateway Protocol)
- Cisco Secure Firewall Management Center (FMC)
- Defesa contra ameaças (FTD) do Cisco Secure Firewall

Componentes Utilizados

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

- Cisco Secure Firewall Management Center executando a versão 7.7.0.

- Cisco Secure Firewall Threat Defense executando a versão 7.7.0.

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

Para grandes empresas com localizações geograficamente dispersas, alcançar a alcançabilidade fim-a-fim pode ser desafiador quando vários sites usam o mesmo número de Sistema Autônomo (AS). O comportamento atual do BGP é descartar as atualizações de roteamento recebidas se o caminho de AS contiver seu próprio número de AS, para evitar loops na rede.

A versão 7.6 introduziu o suporte as-override especificamente para casos de uso relacionados à SD-WAN. No entanto, começando com a versão 7.7, o suporte as-override para eBGP está disponível para todas as implantações devido ao seu requisito de roteamento de núcleo. Isso permite que você tenha sites idênticos com o mesmo número AS.

Aplicativos e gerentes:

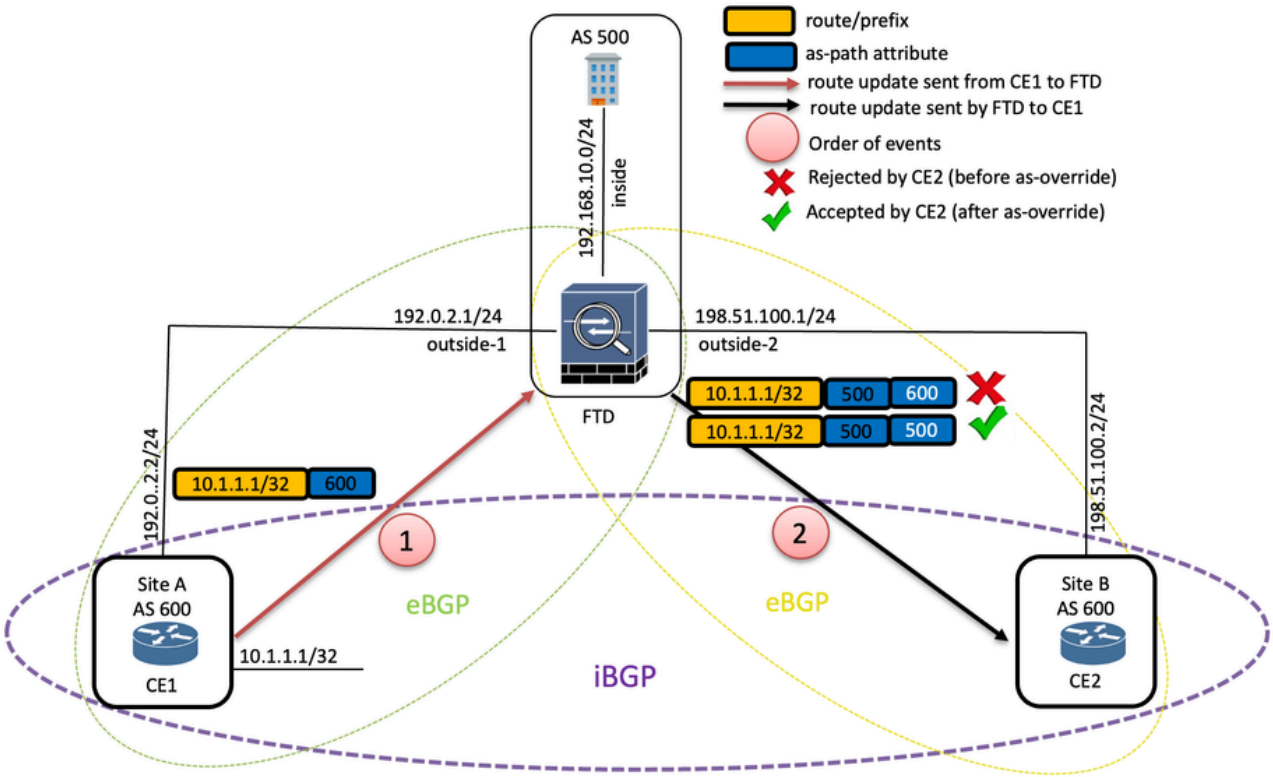
FTD	Todas as Plataformas de FTD
FMC em 7.7.0 API REST FMC	Yes Yes
Versões de suporte de FTD	Somente 7.7.0
Suporte a Snort	Snort 3
FDM em 7.7.0	Not Supported

Fluxo de Processamento de Pacote de Substituição de BGP AS

- O BGP envia atualizações de rotas para seus peers/vizinhos através de mensagens UPDATE.
- Atributos obrigatórios conhecidos são reconhecidos por todos os peers BGP, passados a todos os peers e presentes em todas as mensagens UPDATE.
- O atributo AS-path na mensagem UPDATE contém uma lista ordenada de todos os sistemas autônomos através dos quais essa atualização passou.
- Quando a CLI as-override está habilitada, cada ocorrência do número AS de vizinhos é substituída pelo número AS local no as-path.

Configurar

Diagrama de Rede



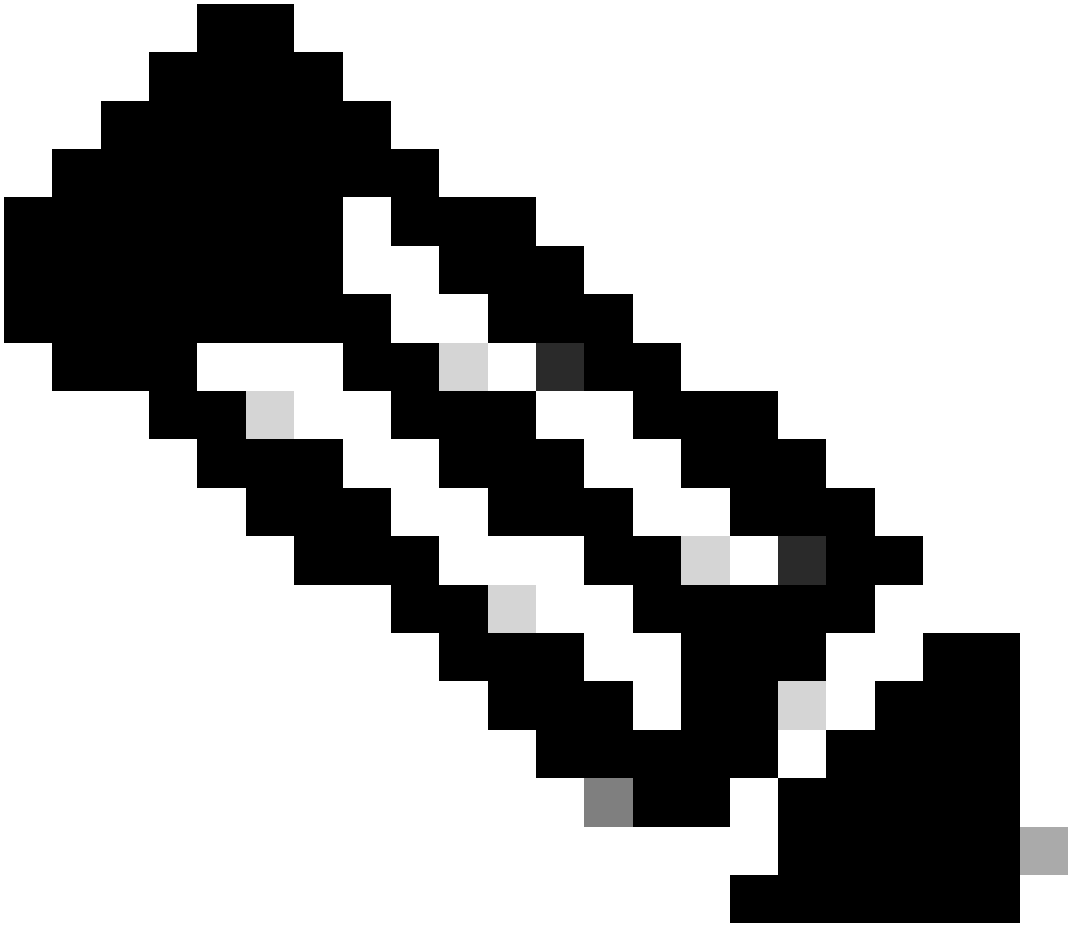
Topologia

Fluxo de atualização de rota

- O site A e o site B são dois sites idênticos que contêm dispositivos/correspondentes com o mesmo número AS.
- Nesse caso, 10.1.1.1/32 é a atualização de prefixo/rota que está sendo anunciada do CE1 do site A para o CE2 do site B via FTD.
- Antes de habilitar as-override, o FTD encaminha as atualizações de rota como estão para o CE2 do local B. Mas, o CE2 ao recebê-lo, descarta a atualização de rota como vê seu próprio número AS no as-path(600).
- Depois de ativar as-override, o FTD encaminha a atualização de rota para CE2 substituindo o número AS de CE1 no AS-path para seu próprio número AS/local (500). Agora o CE2 aceita a atualização de rota.

Visão geral do recurso

- Nova caixa de seleção no FMC para habilitar AS Override.
- O novo comando CLI neighbor <neighbor-ip-address> as-override é introduzido no BGP como parte deste recurso.



Note: O recurso BGP AS Override está disponível para configuração somente através do Centro de Gerenciamento de Firewall Seguro (FMC - Secure Firewall Management Center).

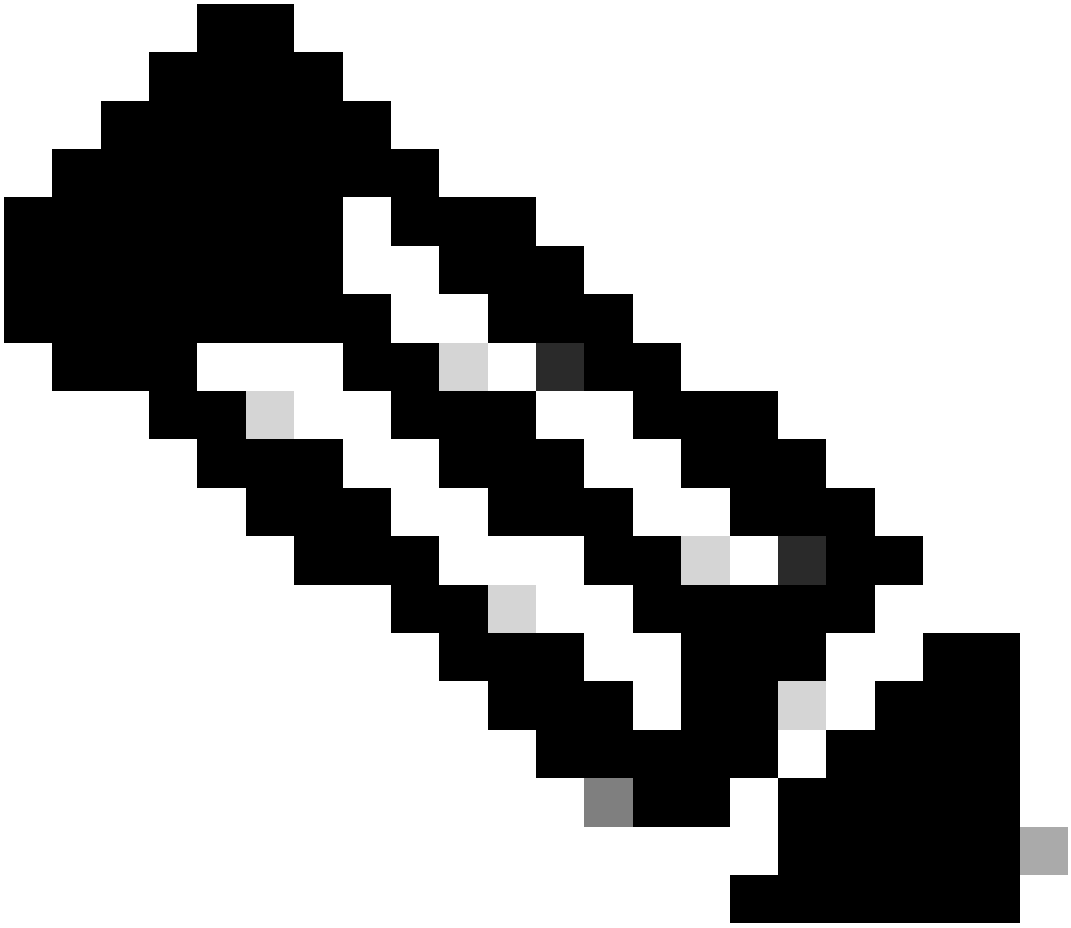
Etapas de configuração no FMC

Passo 1: Navegue até Devices > Device Management e edite o dispositivo threat defense.

Passo 2: Selecione Routing.

Passo 3: (Para um dispositivo com reconhecimento de roteador virtual) Em Configurações gerais, clique em BGP.

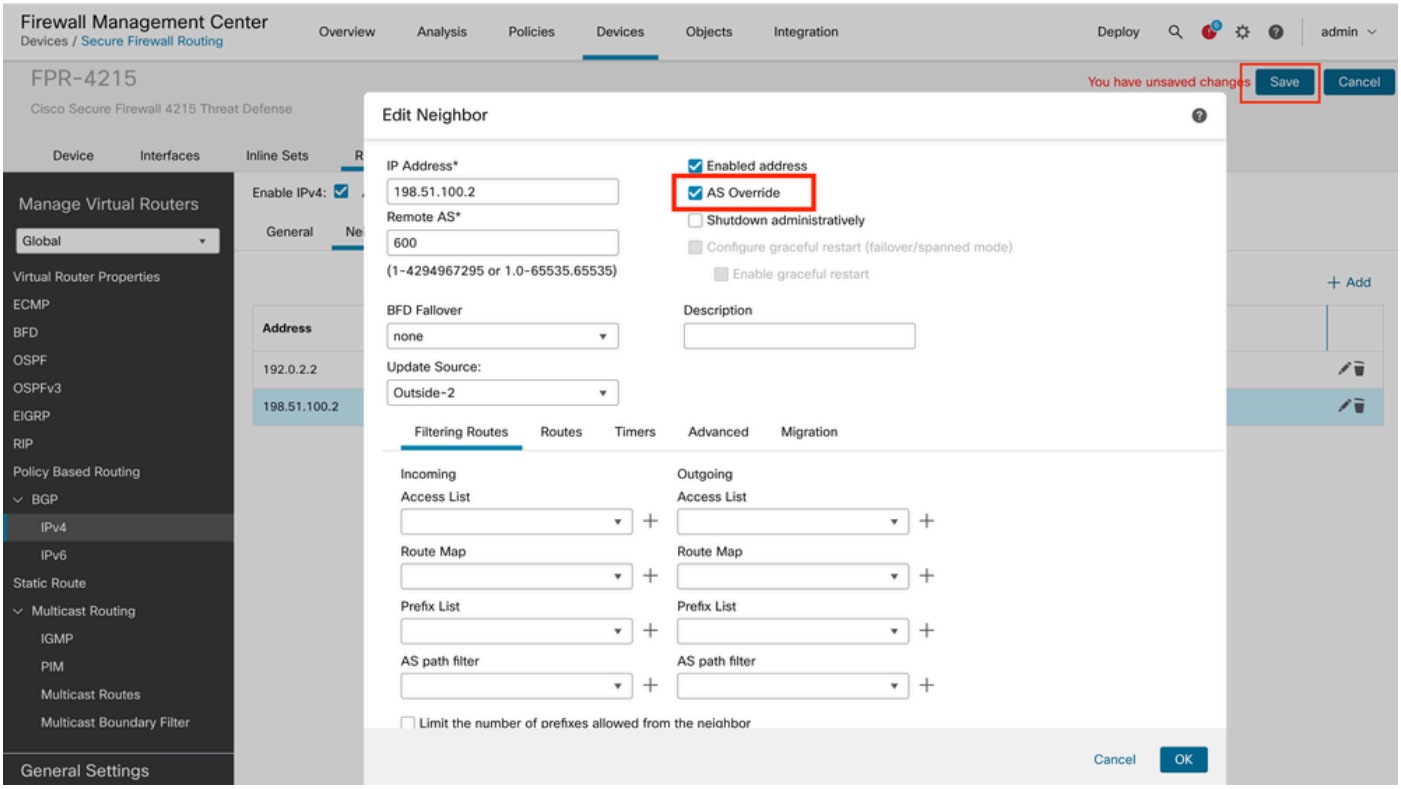
Passo 4: Marque a caixa de seleção Enable BGP para habilitar o processo de roteamento BGP.



Note: Para configurar o roteamento BGP, você pode consultar o Guia de Configuração de Dispositivo do Cisco Secure Firewall Management Center, 7.7

Vizinho BGP IPv4

- Ative AS Override para o vizinho 198.51.100.2.
- Clique em salvar e implantar.



Habilitar Substituição de AS

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Fim do FTD:

<#root>

FTD# show running-config router bgp all

router bgp 500

 bgp log-neighbor-changes
 address-family ipv4 unicast

(Same applicable for IPv6 as well)

   neighbor 192.0.2.2 remote-as 600
   neighbor 192.0.2.2 update-source Outside-1
   neighbor 192.0.2.2 activate
   neighbor 198.51.100.2 remote-as 600
   neighbor 198.51.100.2 update-source Outside-2
   neighbor 198.51.100.2 activate

   neighbor 198.51.100.2 as-override

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

FTD# show bgp ipv4 unicast neighbors 198.51.100.2

```
BGP neighbor is 198.51.100.2,  vrf single_vf,  remote AS 600, external link
 BGP version 4, remote router ID 198.51.100.2
 BGP state = Established, up for 01:13:02
 Last read 00:00:07, last write 00:00:54, hold time is 180, keepalive interval is 60 seconds
 Neighbor sessions:
  1 active, is not multisession capable (disabled)
 Neighbor capabilities:
   Route refresh: advertised and received(new)
   Four-octets ASN Capability: advertised and received
   Address family IPv4 Unicast: advertised and received
   Multisession Capability:
Message statistics:
 InQ depth is 0
 OutQ depth is 0

.


.
For address family: IPv4 Unicast
 Session: 198.51.100.2
 BGP table version 4, neighbor version 4/0
 Output queue size : 0
 Index 5
 5 update-group member
```

Overrides the neighbor AS with my AS before sending updates

```
.
.


Transport(tcp) path-mtu-discovery is disabled
Graceful-Restart is disabled
```

FTD# show bgp ipv4 unicast neighbors 198.51.100.2 advertised-routes

```
BGP table version is 4, local router ID is 198.51.100.1
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
*> 10.1.1.1/32     192.0.2.2           0               0  600 i
Total number of prefixes 1
```

Fim dos receptores:

<#root>

```
As-path for 10.1.1.1/32 prefix/route has been modified from 600 to 500 by FTD (where as-override is enab

Cisco_C1127#show bgp ipv4 unicast


BGP table version is 10, local router ID is 198.51.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>   10.1.1.1/32      198.51.100.1                           0

500 500

 i


Cisco_C1127#show bgp ipv4 unicast 10.1.1.1


BGP routing table entry for 10.1.1.1/32, version 10
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1

  500 500


    198.51.100.1 from 198.51.100.1 (198.51.100.1)
    Origin IGP, localpref 100, valid, external, best
    rx pathid: 0, tx pathid: 0x0
    Updated on Apr 6 2025 17:02:24 UTC
```

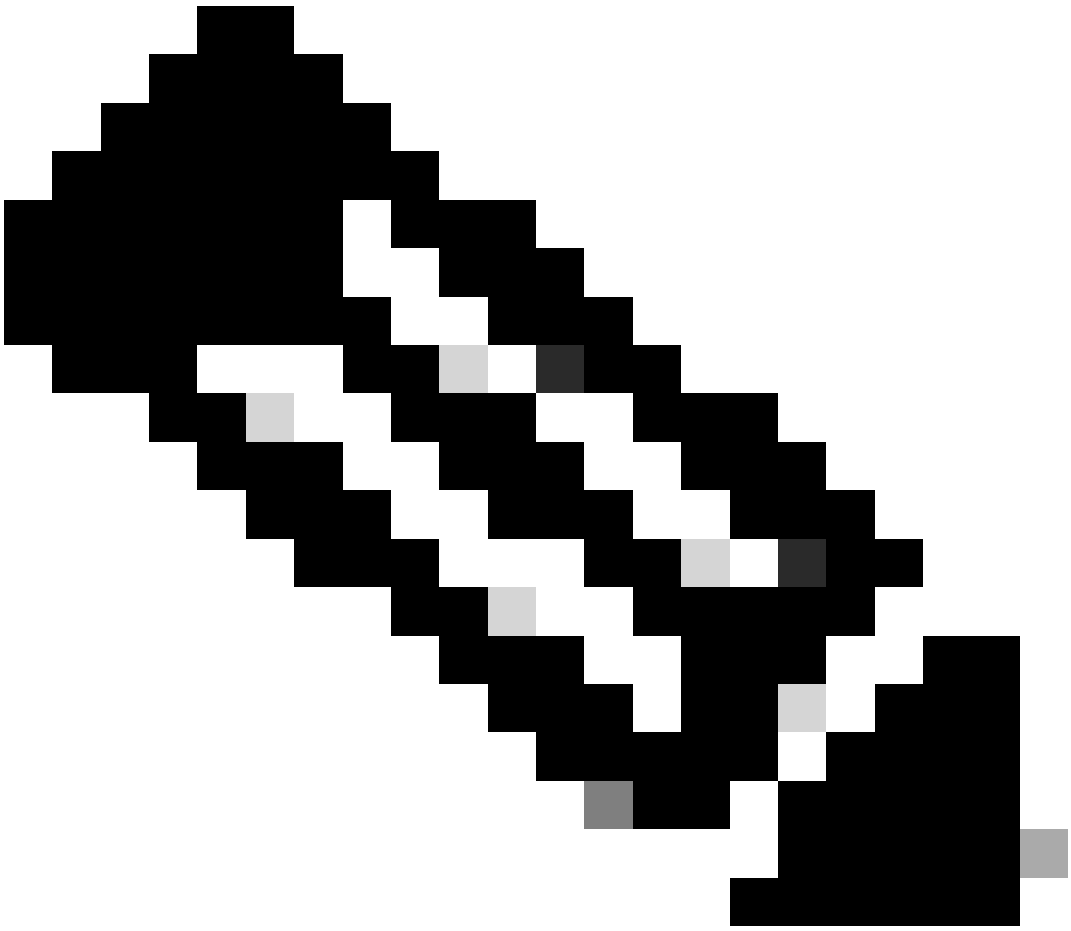
Troubleshooting

Comandos

- show run router bgp all deve ter o CLI AS-override habilitado no FTD.
- show bgp <ipv4/ipv6> unicast neighbors no FTD devem especificar esse texto indicando que as-override está habilitado -> Substitui o AS vizinho pelo meu AS antes de enviar atualizações.
- show bgp <ipv4/ipv6> unicast na extremidade do receptor deve ter as informações de caminho alteradas.

Debugs

```
debug ip bgp updates
debug ip bgp ipv6 unicast updates
debug ip bgp all updates
```



Note: Não há alterações nas depurações antes e depois da habilitação de as-override.

Arquivos de sistema

Este ficheiro de registro contém informações relativas à implementação do recurso as-override do FMC.

/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log

<#root>

```
router bgp 500
address-family ipv4 unicast
```

neighbor 198.51.100.2 as-override

```
exit-address-family
```

Informações Relacionadas

Suporte técnico e downloads da Cisco

Guia de configuração de dispositivos do Cisco Secure Firewall Management Center, 7.7

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.