Configuración de BGP AS Override en Secure Firewall

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Antecedentes
- Flujo de Procesamiento de Paquetes de Invalidación de BGP AS
- Configurar
  - Diagrama de la red
  - Flujo de actualización de ruta
  - Descripción general de características
  - Pasos de configuración en FMC
- Verificación
- Troubleshoot
  - Comandos
  - Depuraciones
  - Archivos del sistema
- Información Relacionada

Introducción

Este documento describe cómo configurar la invalidación del sistema autónomo (AS) BGP en Cisco Secure Firewall Threat Defence.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- BGP (protocolo de gateway fronterizo)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defence (FTD)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Cisco Secure Firewall Management Center que ejecuta la versión 7.7.0.
- Cisco Secure Firewall Threat Defence versión 7.7.0.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Para las grandes empresas con ubicaciones geográficamente dispersas, lograr la disponibilidad de extremo a extremo puede ser un reto cuando varios sitios utilizan el mismo número de sistema autónomo (AS). El comportamiento actual de BGP es descartar las actualizaciones de routing recibidas si la ruta AS contiene el número AS propio, para evitar bucles en la red.

La versión 7.6 introdujo el soporte as-override específicamente para casos prácticos relacionados con SD-WAN. Sin embargo, a partir de la versión 7.7, el soporte as-override para eBGP está disponible para todas las implementaciones debido a su requisito de routing principal. Esto le permite tener sitios idénticos con el mismo número AS.

Aplicaciones y jefes:

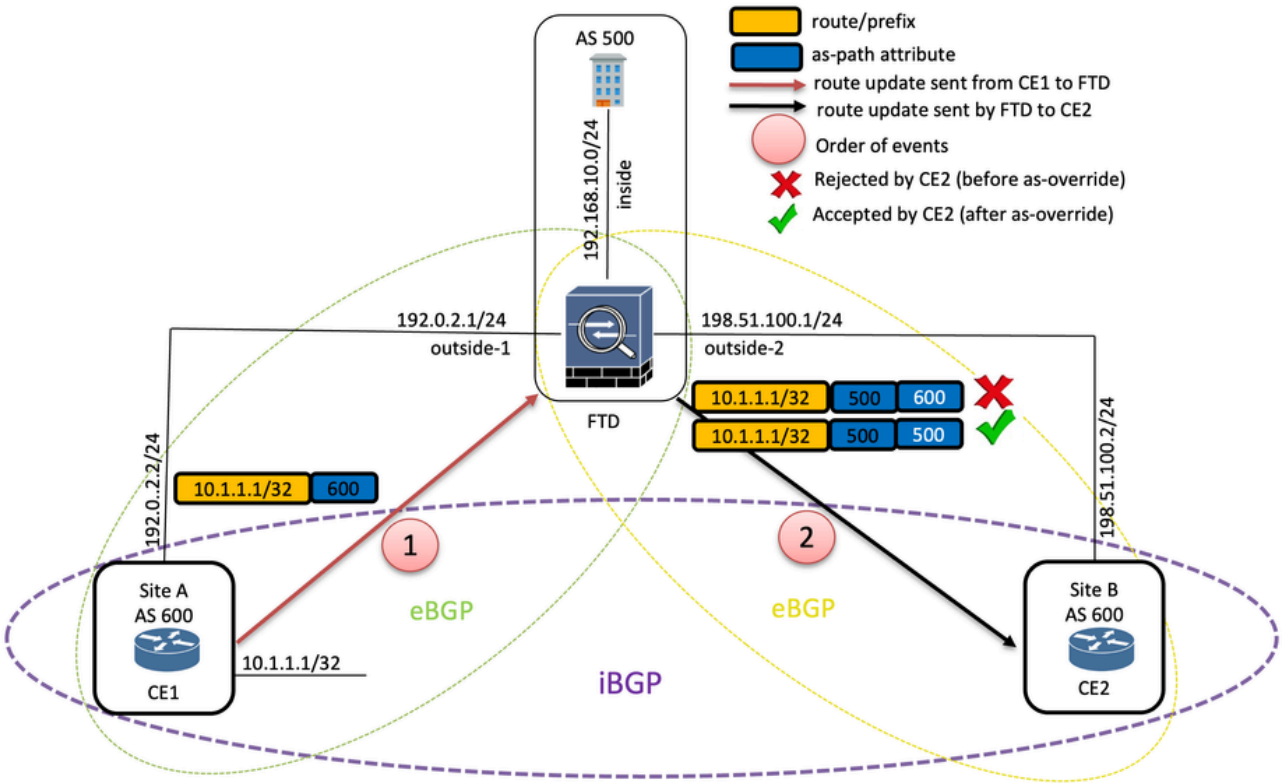
FTD	Todas las plataformas FTD
FMC en 7.7.0 API REST FMC	Yes Yes
Versiones compatibles con FTD	7.7.0 solamente
Compatibilidad con Snort	Snort 3
FDM en 7.7.0	No soportados

Flujo de Procesamiento de Paquetes de Invalidación de BGP AS

- BGP envía actualizaciones de ruta a sus pares/vecinos a través de mensajes UPDATE.
- Los atributos obligatorios conocidos son reconocidos por todos los peers BGP, pasados a todos los peers y presentes en todos los mensajes UPDATE.
- El atributo AS-path del mensaje UPDATE contiene una lista ordenada de todos los sistemas autónomos por los que ha pasado esta actualización.
- Cuando se habilita la CLI as-override, cada aparición del número AS de vecinos se reemplaza por el número AS local en as-path.

Configurar

Diagrama de la red



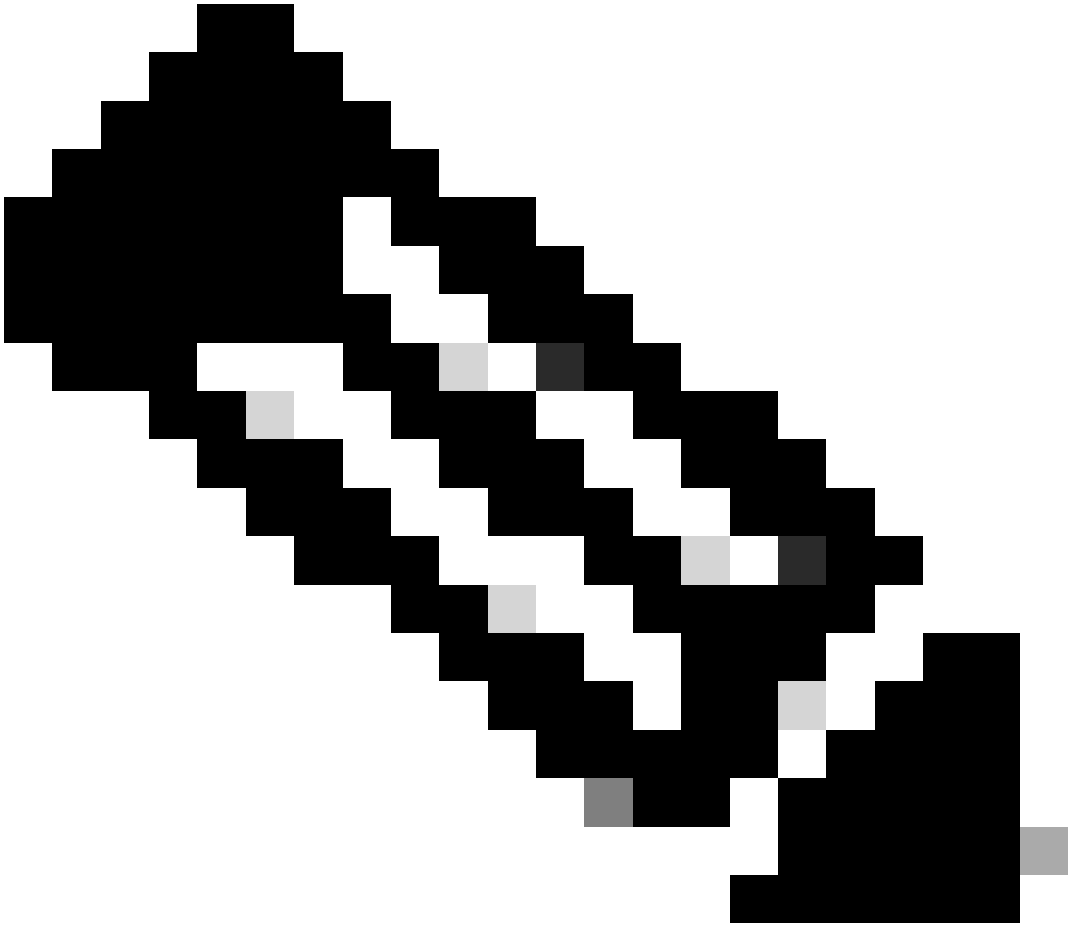
Topología

Flujo de actualización de ruta

- El sitio A y el sitio B son dos sitios idénticos que contienen dispositivos/pares con el mismo número AS.
- En este caso, 10.1.1.1/32 es la actualización de prefijo/ruta que se anuncia desde CE1 del sitio A al CE2 del sitio B a través de FTD.
- Antes de habilitar as-override, el FTD reenvía las actualizaciones de ruta tal como están al CE2 del sitio B. Pero, CE2 al recibirlo, descarta la actualización de ruta ya que ve su propio número AS en as-path(600).
- Después de habilitar as-override, el FTD reenvía la actualización de la ruta a CE2 reemplazando el número de AS de CE1 en la ruta as a su propio número AS local (500). Ahora CE2 acepta la actualización de la ruta.

Descripción general de características

- Nueva casilla de verificación en FMC para activar la sustitución de AS.
- El nuevo comando CLI neighbor <neighbor-ip-address> as-override se introduce en BGP como parte de esta función.



Nota: La función BGP AS Override (Anulación de AS BGP) sólo está disponible para la configuración a través de Secure Firewall Management Center (FMC).

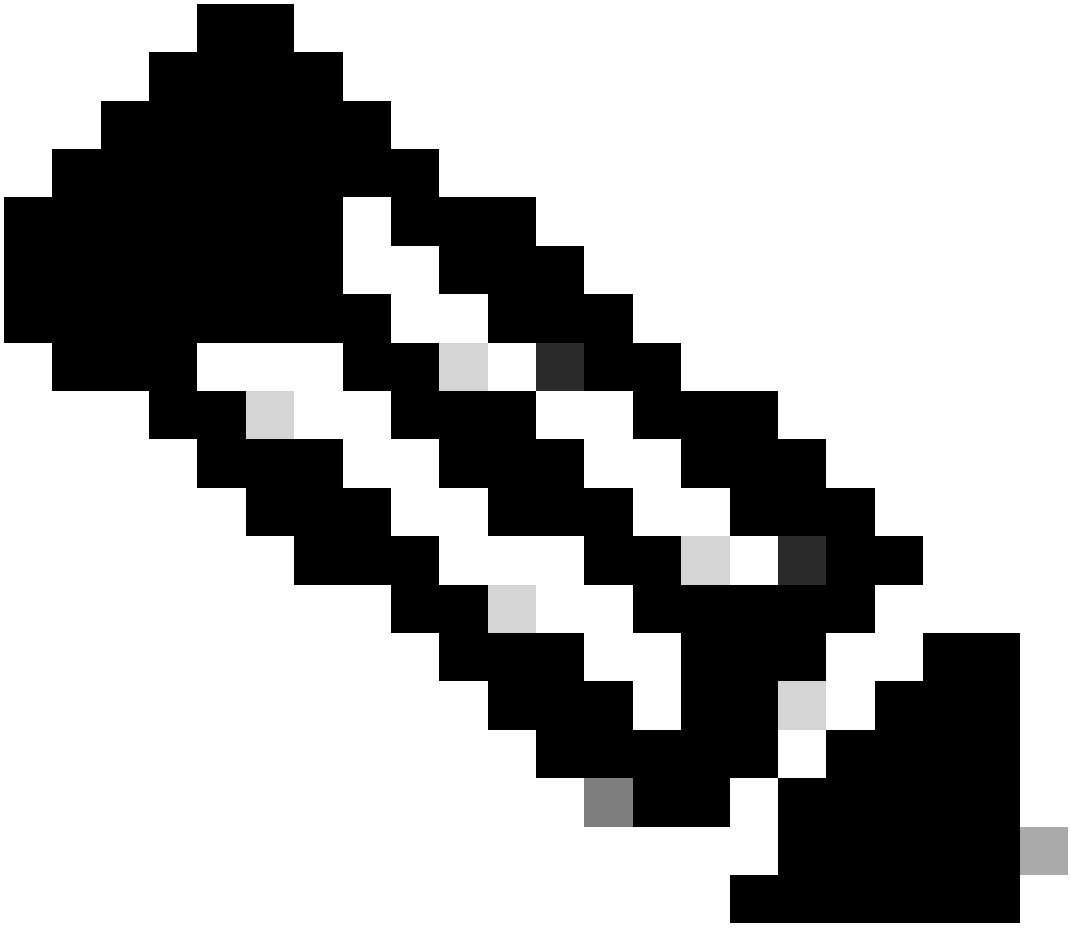
Pasos de configuración en FMC

Paso 1: Navegue hasta Devices > Device Management, y edite el dispositivo de defensa contra amenazas.

Paso 2: Seleccione Routing.

Paso 3: (Para un dispositivo con detección de router virtual) En General Settings, haga clic en BGP.

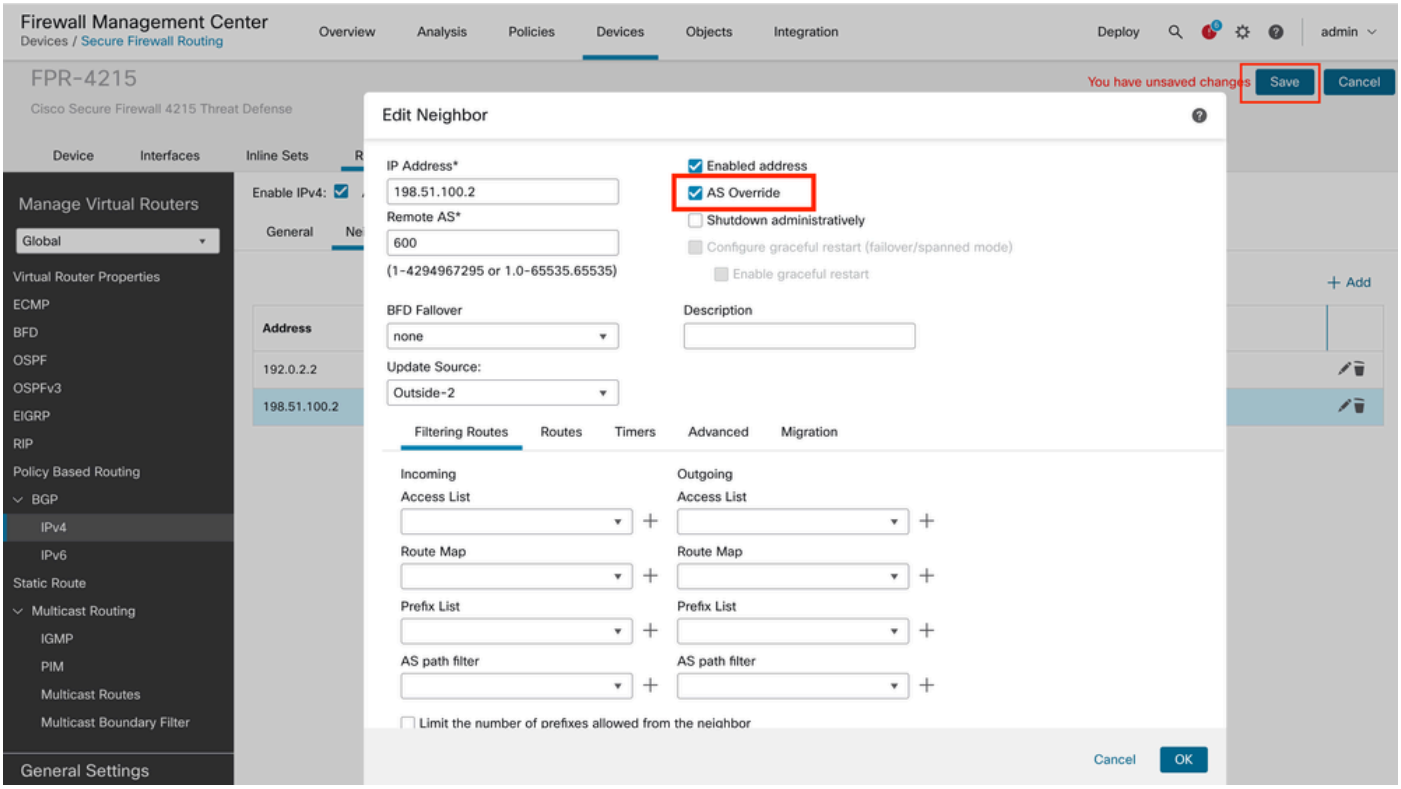
Paso 4: Marque la casilla de verificación Enable BGP para habilitar el proceso de ruteo BGP.



Nota: Para configurar el ruteo BGP, puede consultar la Guía de Configuración de Dispositivos de Cisco Secure Firewall Management Center, 7.7

Vecino BGP IPv4

- Habilite AS Override para el vecino 198.51.100.2.
- Haga clic en guardar e implementar.



Activar anulación de AS

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Final de 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
```

Fin de 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
```

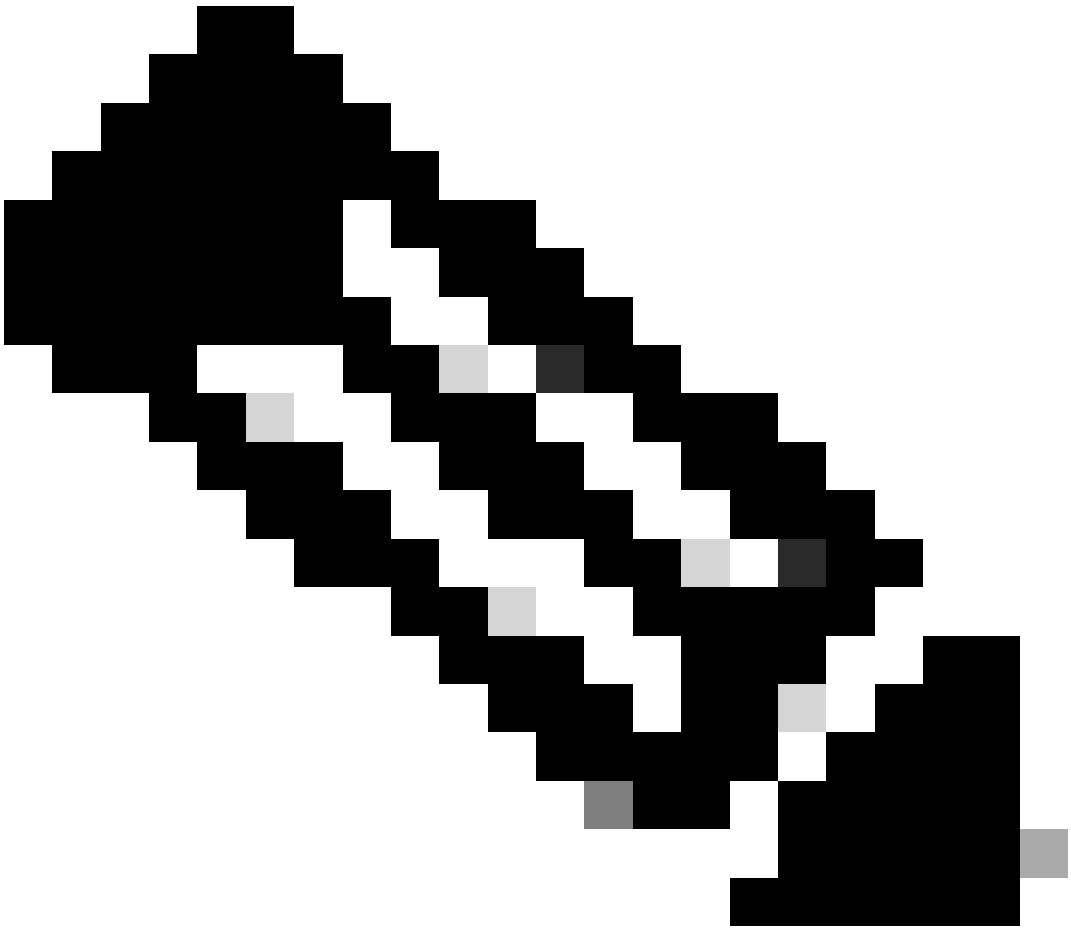
Troubleshoot

Comandos

- show run router bgp all debe tener AS-override CLI habilitado en FTD.
- show bgp <ipv4/ipv6> unicast neighbors on FTD debe especificar este texto que indica que as-override está habilitado -> Reemplaza el AS vecino con mi AS antes de enviar actualizaciones.
- show bgp <ipv4/ipv6> unicast en el extremo del receptor debe tener la información de trayectoria cambiada.

Depuraciones

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



Nota: No hay cambios en las depuraciones antes y después de la habilitación de as-override.

Archivos del sistema

Este archivo de registro contiene información relacionada con la implementación de la función as-override de 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
```

Información Relacionada

Soporte técnico y descargas de Cisco

Guía de configuración de dispositivos de Cisco Secure Firewall Management Center, 7.7

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).