Configurer le remplacement BGP AS dans le pare-feu sécurisé

Table des matières

Introduction

Ce document décrit comment configurer le remplacement du système autonome BGP (AS) dans Cisco Secure Firewall Threat Defense.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- BGP (Border Gateway Protocol)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Cisco Secure Firewall Management Center version 7.7.0.
- Cisco Secure Firewall Threat Defense version 7.7.0.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Pour les grandes entreprises avec des emplacements géographiquement dispersés, l'accessibilité de bout en bout peut être difficile lorsque plusieurs sites utilisent le même numéro de système autonome (AS). Le comportement BGP actuel consiste à ignorer les mises à jour de routage reçues si le chemin AS contient son propre numéro AS, afin d'éviter les boucles dans le réseau.

La version 7.6 a introduit la prise en charge de la fonction de remplacement spécifique pour les cas d'utilisation liés au SD-WAN. Cependant, à partir de la version 7.7, la prise en charge de l'as-override pour eBGP est disponible pour tous les déploiements en raison de ses exigences de routage de base. Cela vous permet d'avoir des sites identiques avec le même numéro de système autonome.

Applications et responsables :

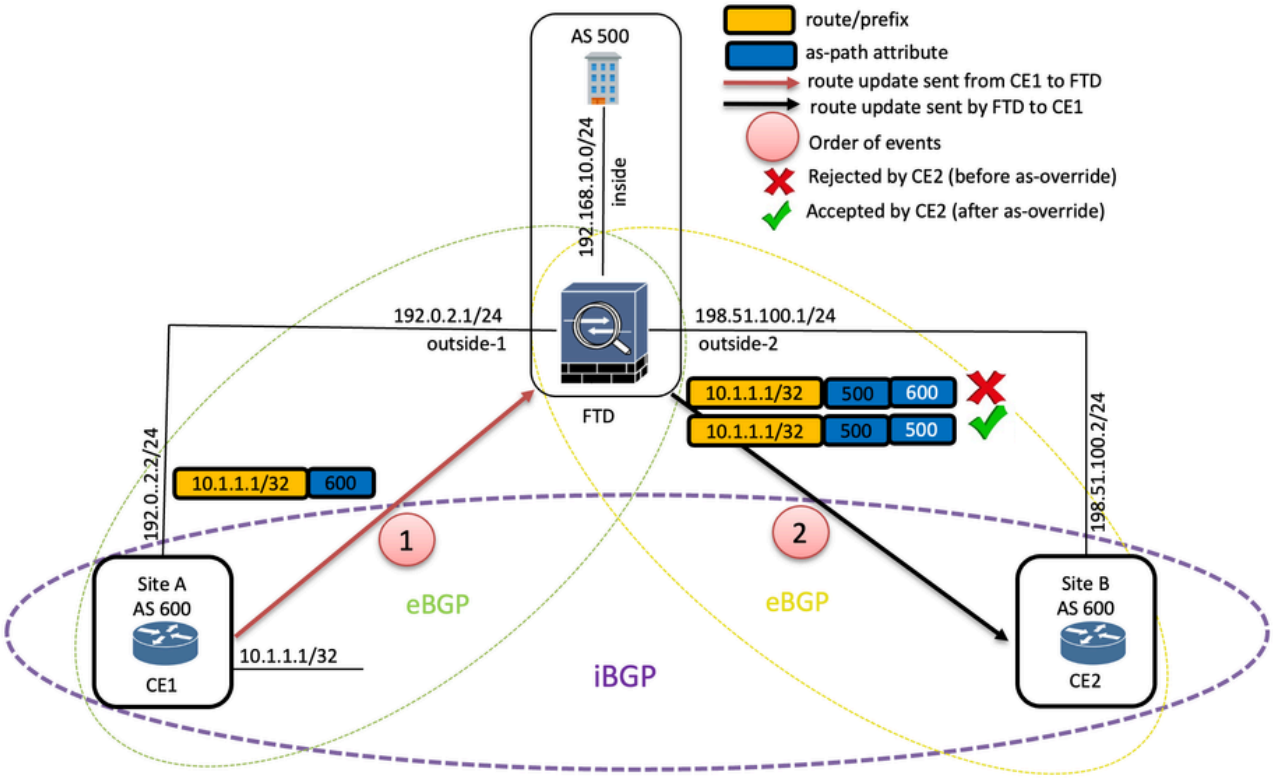
FTD	Toutes les plates-formes FTD
FMC sur 7.7.0 API REST FMC	Oui Oui
Versions de support FTD	7.7.0 uniquement
Snort Support	Snort 3
FDM sur 7.7.0	Non pris en charge

Flux de traitement des paquets BGP AS Override

- BGP envoie des mises à jour de route à ses homologues/voisins via des messages UPDATE.
- Les attributs obligatoires bien connus sont reconnus par tous les homologues BGP, transmis à tous les homologues et présents dans tous les messages UPDATE.
- L'attribut AS-path du message UPDATE contient une liste ordonnée de tous les systèmes autonomes par lesquels cette mise à jour a été transmise.
- Lorsque l'interface de ligne de commande as-override est activée, chaque occurrence du numéro de système autonome voisin est remplacée par le numéro de système autonome local dans l'as-path.

Configurer

Diagramme du réseau



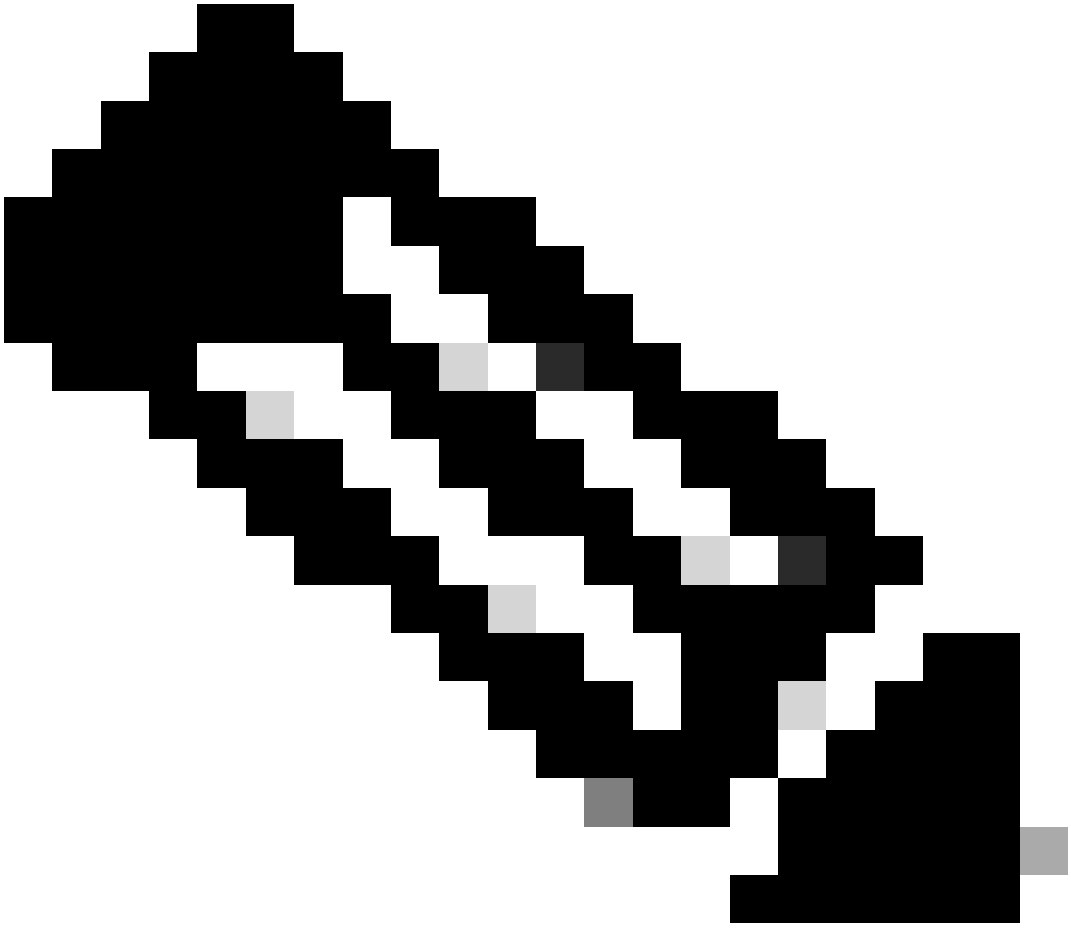
Topologie

Flux de mise à jour de route

- Le site A et le site B sont deux sites identiques contenant des périphériques/homologues avec le même numéro de système autonome.
- Dans ce cas, 10.1.1.1/32 est la mise à jour de préfixe/route qui est annoncée de CE1 du site A à CE2 du site B via FTD.
- Avant d'activer as-override, le FTD transfère les mises à jour de route telles qu'elles sont à CE2 du site B. Mais, CE2 à la réception, rejette la mise à jour de route car il voit son propre numéro AS dans l'as-path(600).
- Après l'activation de as-override, le FTD transfère la mise à jour de route à CE2 en remplaçant le numéro AS de CE1 dans le chemin as vers son propre numéro AS local (500). CE2 accepte maintenant la mise à jour de la route.

Présentation des fonctionnalités

- Nouvelle case à cocher dans FMC pour activer le remplacement AS.
- La nouvelle commande CLI neighbor <neighbor-ip-address> as-overrides est introduite dans BGP dans le cadre de cette fonctionnalité.



Remarque : La fonctionnalité de remplacement du système autonome BGP est disponible pour la configuration via le Centre de gestion du pare-feu sécurisé (FMC) uniquement.

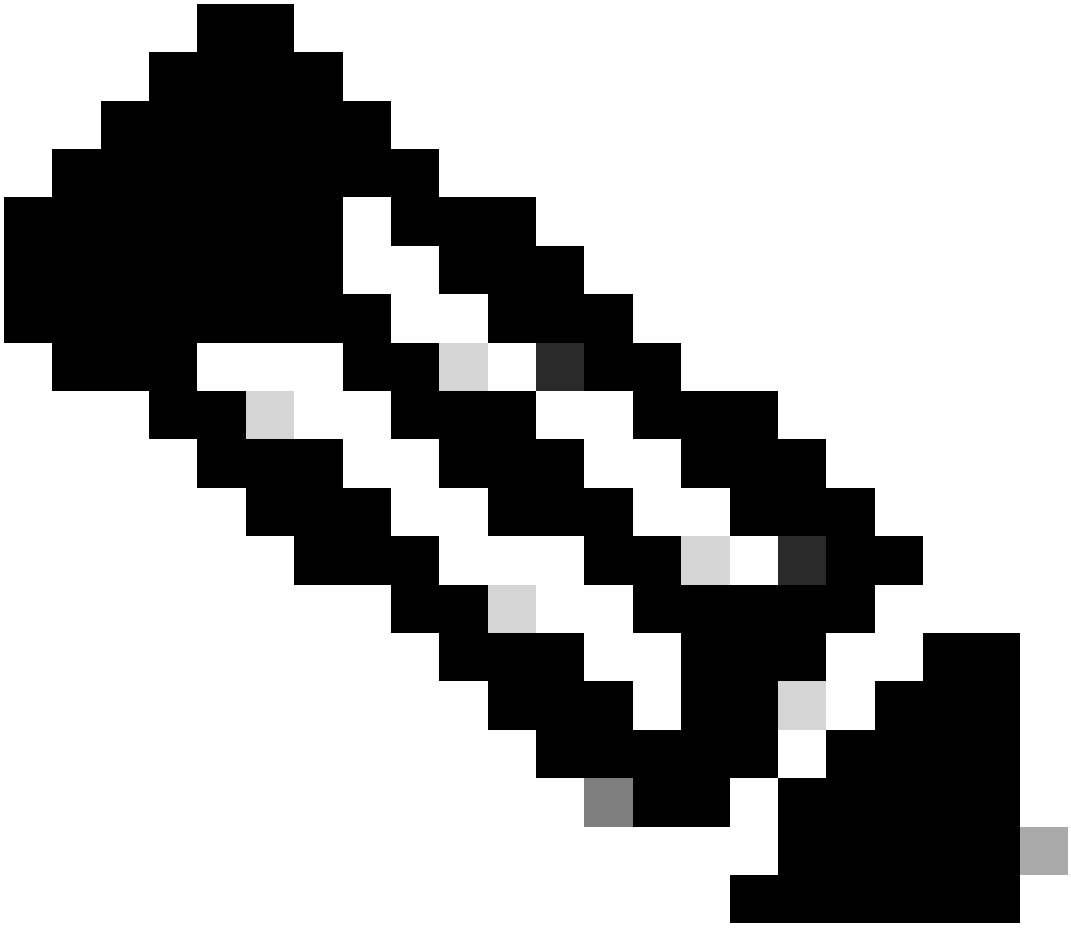
Étapes de configuration sur FMC

Étape 1 : Accédez à Devices > Device Management, et modifiez le périphérique de défense contre les menaces.

Étape 2 : Sélectionnez Routage.

Étape 3 : (Pour un périphérique compatible routeur virtuel) Sous General Settings, cliquez sur BGP.

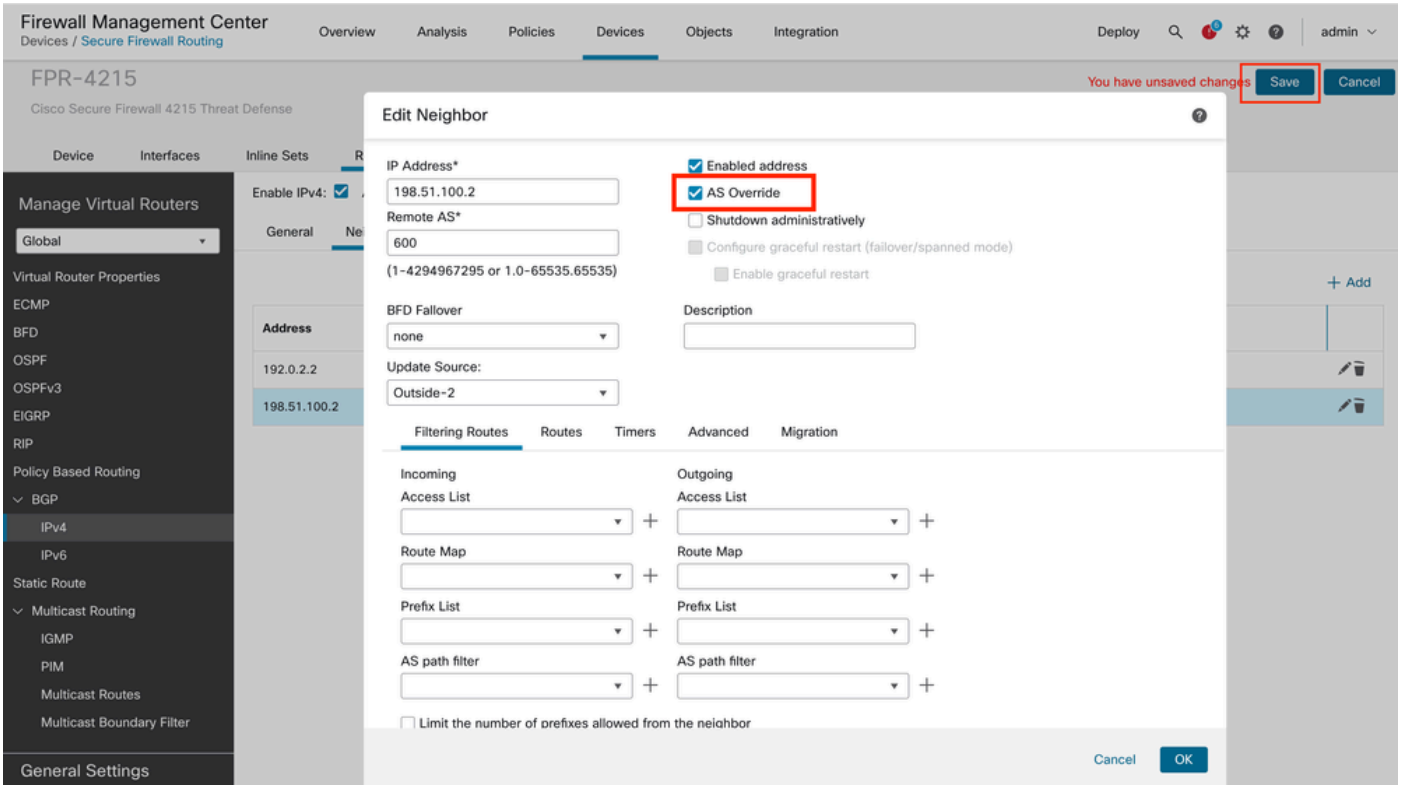
Étape 4 : Cochez la case Enable BGP pour activer le processus de routage BGP.



Remarque : Pour configurer le routage BGP, vous pouvez vous référer au Guide de configuration des périphériques Cisco Secure Firewall Management Center, 7.7

Voisin IPv4 BGP

- Activez le remplacement AS pour le voisin 198.51.100.2.
- Cliquez sur Enregistrer et déployer.



Activer le remplacement AS

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Fin 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
```

Extrémité des récepteurs :

<#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
```

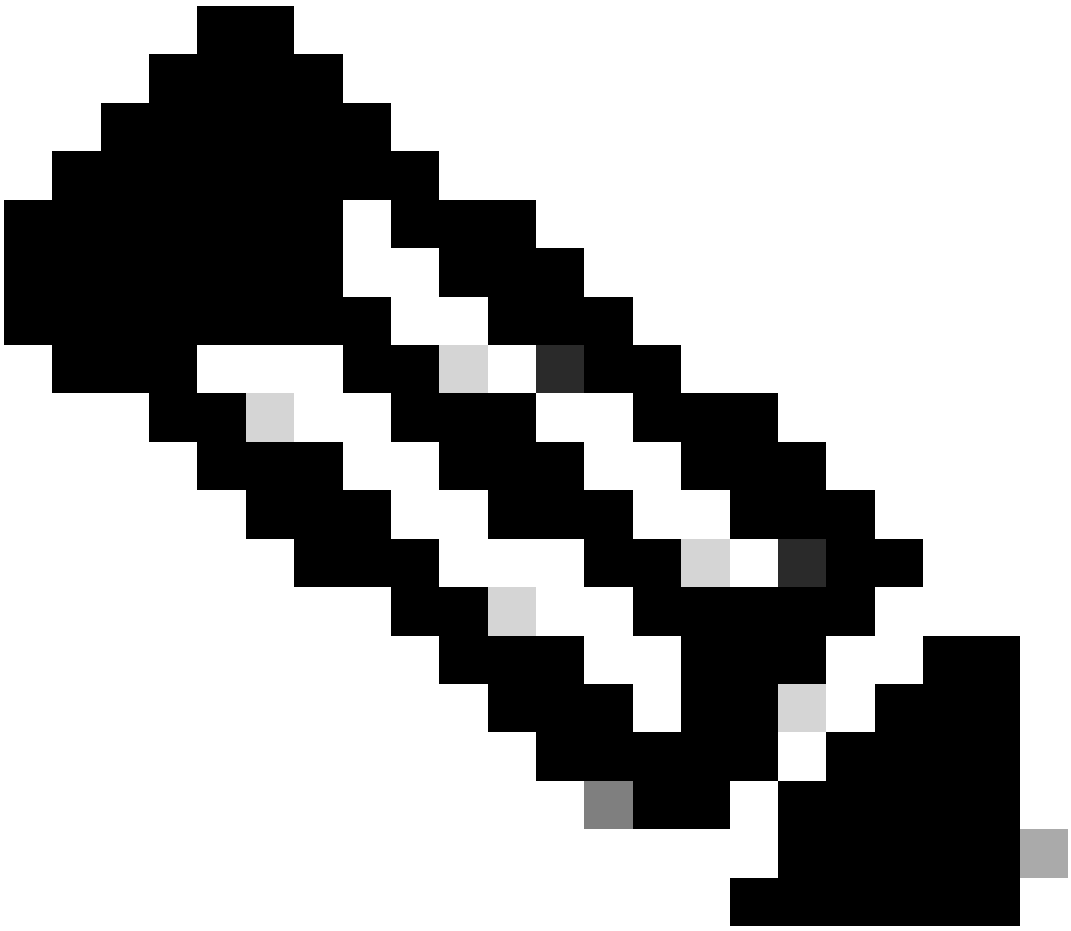
Dépannage

Commandes

- show run router bgp all doit avoir AS-override CLI activé dans FTD.
- show bgp <ipv4/ipv6> unicast neighbors on FTD doit spécifier ce texte indiquant que la commande as-override est activée -> Remplace le système autonome voisin par mon système autonome avant d'envoyer les mises à jour.
- show bgp <ipv4/ipv6> unicast à l'extrémité du récepteur doit avoir les informations de chemin modifiées.

Déboguages

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



Remarque : Il n'y a aucune modification dans les débogages avant et après l'activation de as-override.

Fichiers système

Ce fichier journal contient des informations relatives au déploiement de la fonction 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
```

Informations connexes

[Assistance technique de Cisco et téléchargements]

[Guide de configuration des périphériques Cisco Secure Firewall Management Center, 7.7]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.