Configurare l'override di BGP AS in Secure Firewall

Sommario

Introduzione

Questo documento descrive come configurare l'override del sistema autonomo BGP (AS) in Cisco Secure Firewall Threat Defense.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Cisco Secure Firewall Management Center con versione 7.7.0 in esecuzione.
- Cisco Secure Firewall Threat Defense con versione 7.7.0.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Per le grandi aziende con ubicazioni geograficamente distanti, raggiungere l'estremità della rete può essere difficile quando più siti utilizzano lo stesso numero di sistema autonomo (AS). Il comportamento corrente di BGP consiste nell'ignorare gli aggiornamenti di routing ricevuti se il percorso AS contiene il proprio numero AS, per evitare loop nella rete.

La release 7.6 ha introdotto il supporto as-override specifico per i casi di utilizzo SD-WAN. Tuttavia, a partire dalla versione 7.7, il supporto as-override per eBGP è disponibile per tutte le distribuzioni a causa dei requisiti di routing di base. Ciò consente di avere siti identici con lo stesso numero AS.

Applicazioni e responsabili:

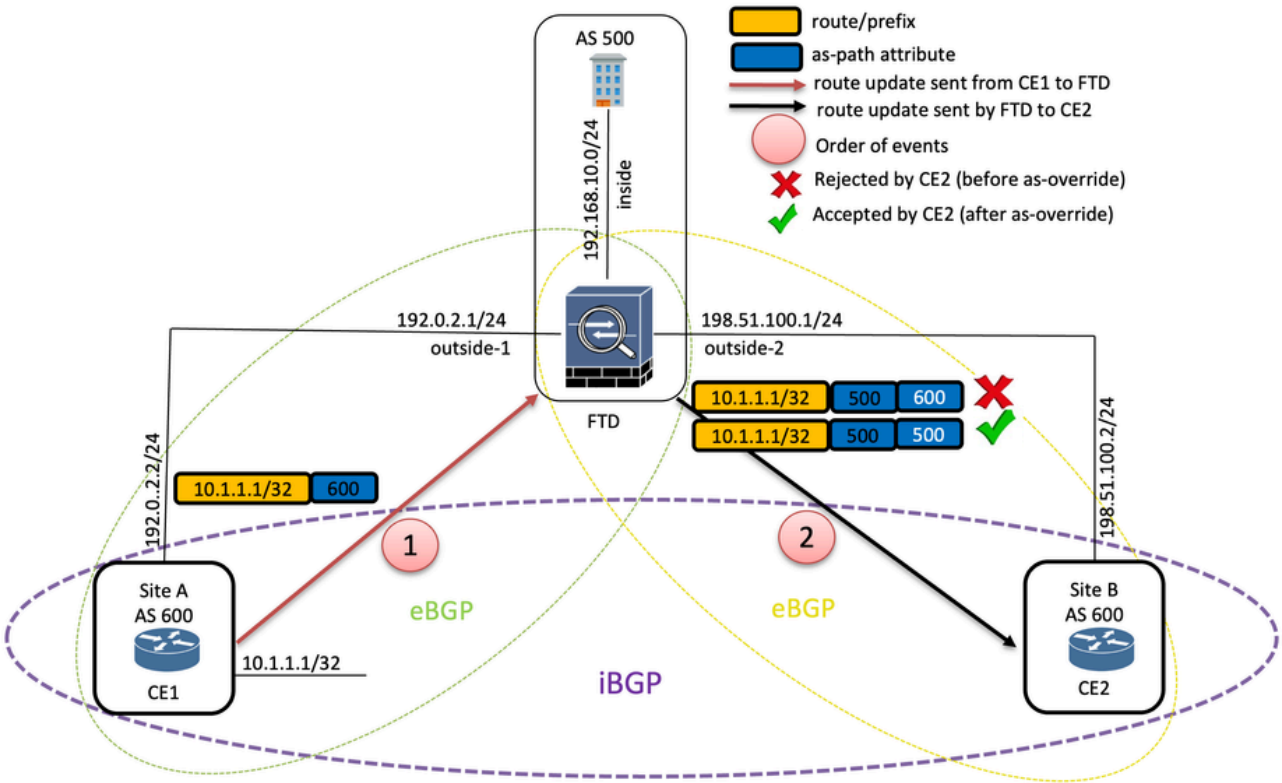
FTD	Tutte le piattaforme FTD
FMC su 7.7.0 API REST FMC	Sì Sì
Versioni del supporto FTD	Solo 7.7.0
Supporto per snort	Snort. 3
FDM su 7.7.0	Non supportata

Flusso di elaborazione dei pacchetti di override BGP AS

- BGP invia aggiornamenti della route ai peer/router adiacenti tramite messaggi UPDATE.
- Gli attributi obbligatori noti vengono riconosciuti da tutti i peer BGP, passati a tutti i peer e presenti in tutti i messaggi UPDATE.
- L'attributo AS-path nel messaggio UPDATE contiene un elenco ordinato di tutti i sistemi autonomi attraverso i quali è stato passato l'aggiornamento.
- Quando la CLI as-override è abilitata, ogni occorrenza del numero AS adiacente viene sostituita dal numero AS locale nel percorso as.

Configurazione

Esempio di rete



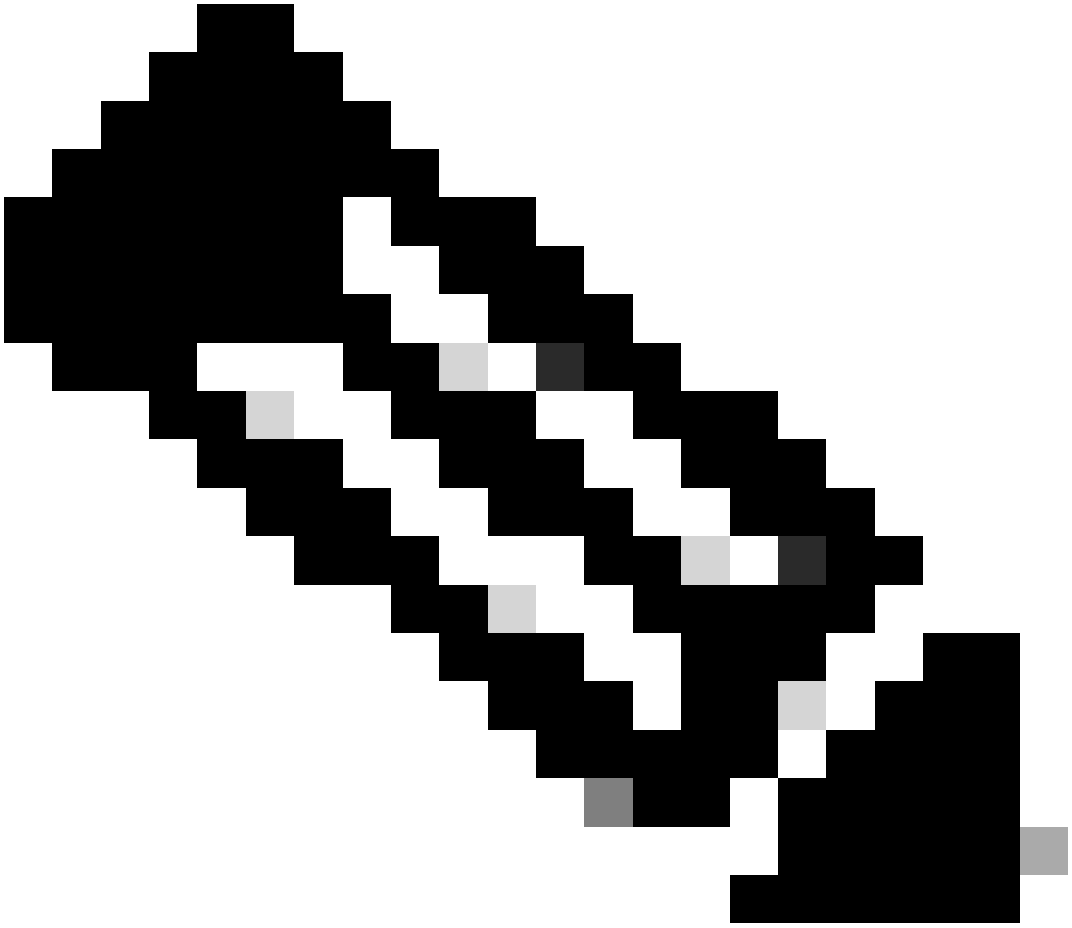
Topologia

Flusso di aggiornamento ciclo di lavorazione

- Il Sito A e il Sito B sono due siti identici contenenti dispositivi/peer con lo stesso numero di AS.
- In questo caso, 10.1.1.1/32 è l'aggiornamento di prefisso/percorso pubblicizzato da CE1 del sito A a CE2 del sito B tramite FTD.
- Prima di abilitare la sostituzione automatica, l'FTD inoltra gli aggiornamenti del ciclo di lavorazione come avviene per CE2 del sito B. Tuttavia, CE2, al momento della ricezione, scarta l'aggiornamento del ciclo di lavorazione quando vede il proprio numero AS nel percorso AS (600).
- Dopo aver abilitato as-override, l'FTD inoltra l'aggiornamento del percorso a CE2 sostituendo il numero AS di CE1 nel percorso AS con il proprio numero AS/locale (500). Ora CE2 accetta l'aggiornamento del percorso.

Panoramica delle funzionalità

- Nuova casella di controllo in FMC per abilitare la sostituzione di AS.
- Il nuovo comando CLI neighbors <indirizzo-ip-router> as-override è stato introdotto in BGP come parte di questa funzionalità.



Nota: La funzionalità BGP AS Override è disponibile per la configurazione solo tramite il centro di gestione del firewall protetto (FMC).

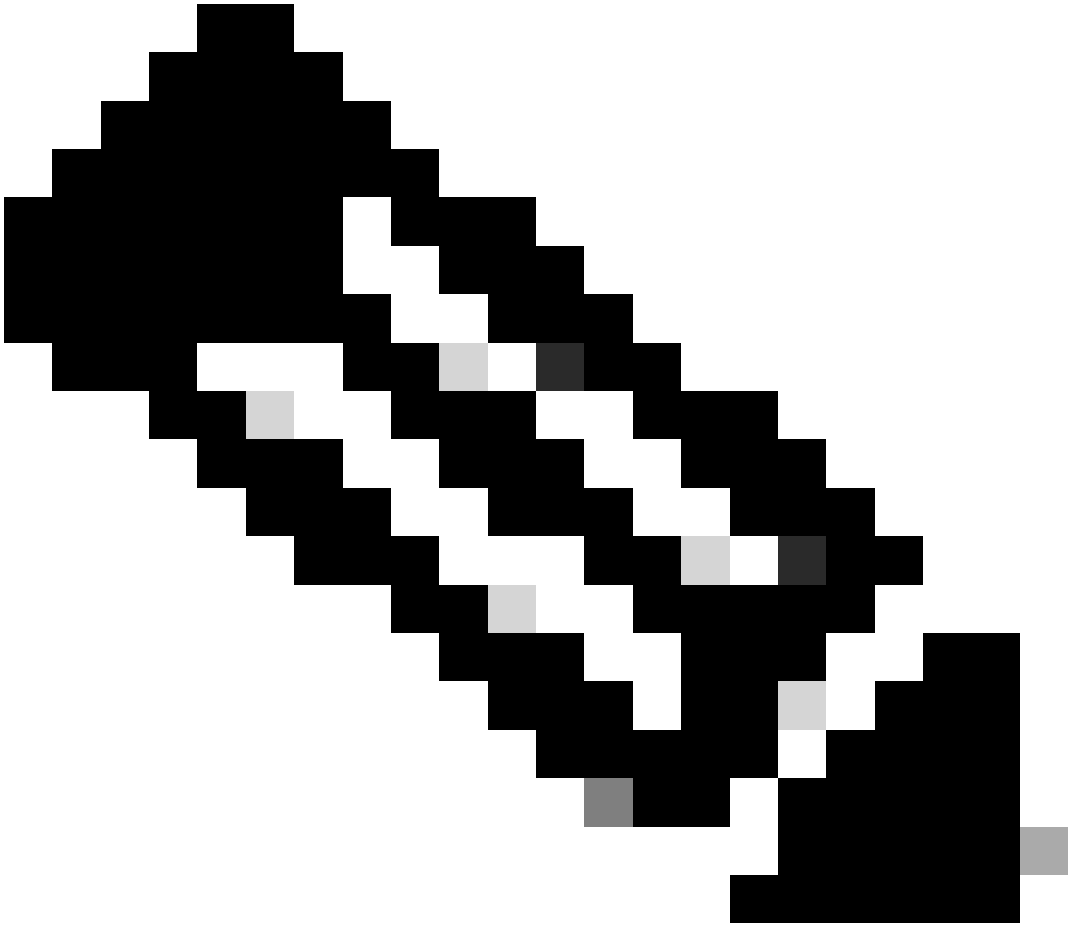
Procedura di configurazione in FMC

Passaggio 1: Passare a Dispositivi > Gestione dispositivi e modificare il dispositivo di difesa dalle minacce.

Passaggio 2: Selezionare Ciclo.

Passaggio 3: (Per un dispositivo compatibile con router virtuali) In Impostazioni generali, fare clic su BGP.

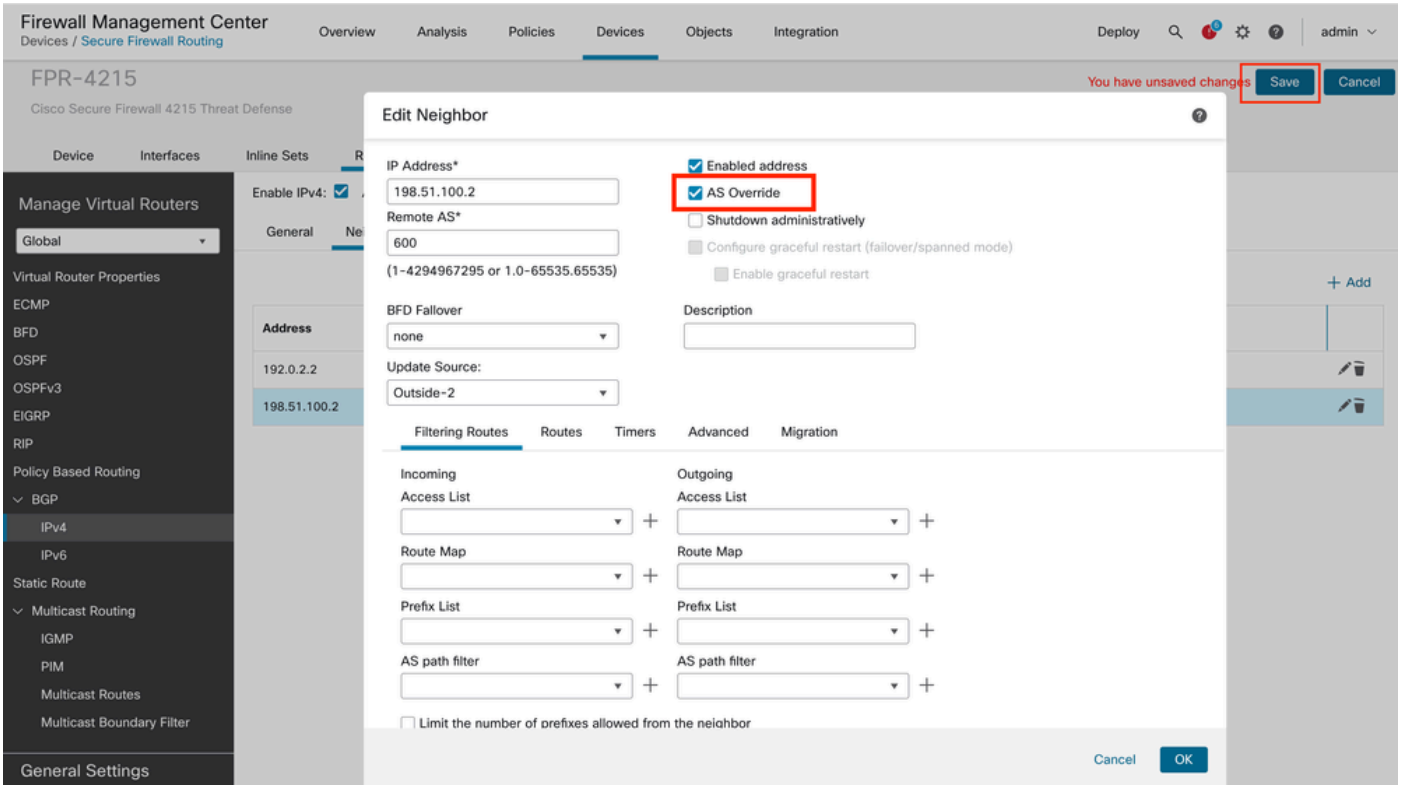
Passaggio 4: Selezionare la casella di controllo Enable BGP per abilitare il processo di routing BGP.



Nota: Per configurare il routing BGP, fare riferimento alla Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center, 7.7

Router adiacente BGP IPv4

- Abilitare l'override AS per la risorsa adiacente 198.51.100.2.
- Fare clic su Salva e distribuisci.



Abilita sostituzione AS

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Fine 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
```

Fine ricevitore:

<#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
```

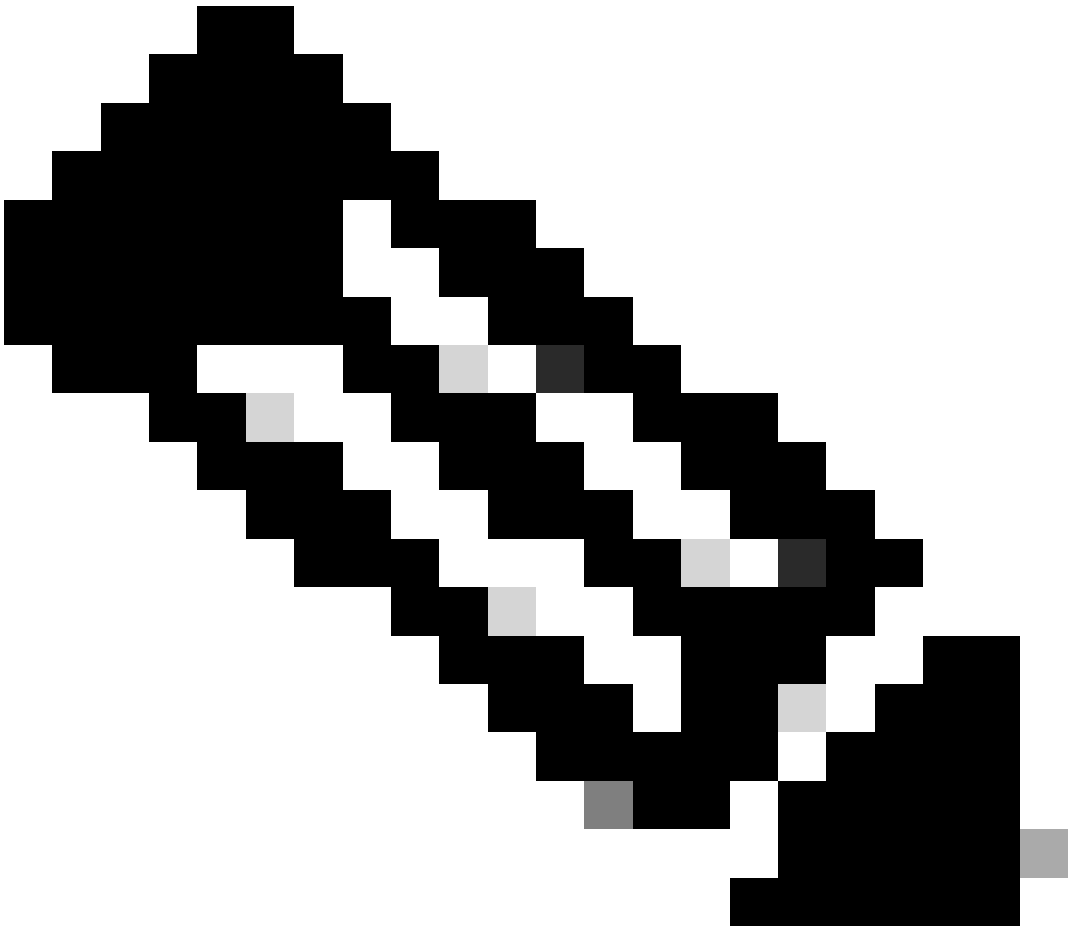
Risoluzione dei problemi

Comandi

- show run router bgp all deve avere AS-override CLI abilitato in FTD.
- show bgp <ipv4/ipv6> unicast neighbors su FTD deve specificare questo testo per indicare che è abilitata la sostituzione automatica -> Esegue l'override dell'AS adiacente con l'AS prima di inviare gli aggiornamenti.
- le informazioni sul percorso show bgp <ipv4/ipv6> unicast sull'estremità del ricevitore devono essere modificate.

Debug

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



Nota: Non vi sono modifiche nei debug prima e dopo l'abilitazione della sostituzione automatica.

File di sistema

Questo file di log contiene informazioni relative alla distribuzione della funzionalità di sostituzione automatica da 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
```

Informazioni correlate

Supporto tecnico Cisco e download

Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center, 7.7

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).