セキュアファイアウォールでのBGP ASオーバーライドの設定

内容

はじめに

このドキュメントでは、Cisco Secure Firewall Threat DefenseでBGP自律システム(AS)オーバーライドを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- BGP（ボーダーゲートウェイプロトコル）
- Cisco Secure Firewall Management Center(FMC)
- Cisco Secure Firewall Threat Defense(FTD)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン7.7.0を実行しているCisco Secure Firewall Management Center。
- バージョン7.7.0が稼働しているCisco Secure Firewall Threat Defense

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

地理的に分散した拠点を持つ大企業では、複数のサイトが同じ自律システム(AS)番号を使用する場合、エンドツーエンドの到達可能性を実現するのは困難です。 現在のBGPの動作では、ASパスに自身のAS番号が含まれている場合に受信したルーティングアップデートを廃棄し、ネットワーク内のループを回避します。

7.6リリースでは、特にSD-WAN関連のユースケースに対して、as-overrideサポートが導入されました。ただし、7.7リリース以降では、コアルーティング要件により、eBGPのas-overrideサポートはすべての導入で使用できます。これにより、同じAS番号を持つ同一のサイトを持つことができます。

アプリケーションとマネージャ：

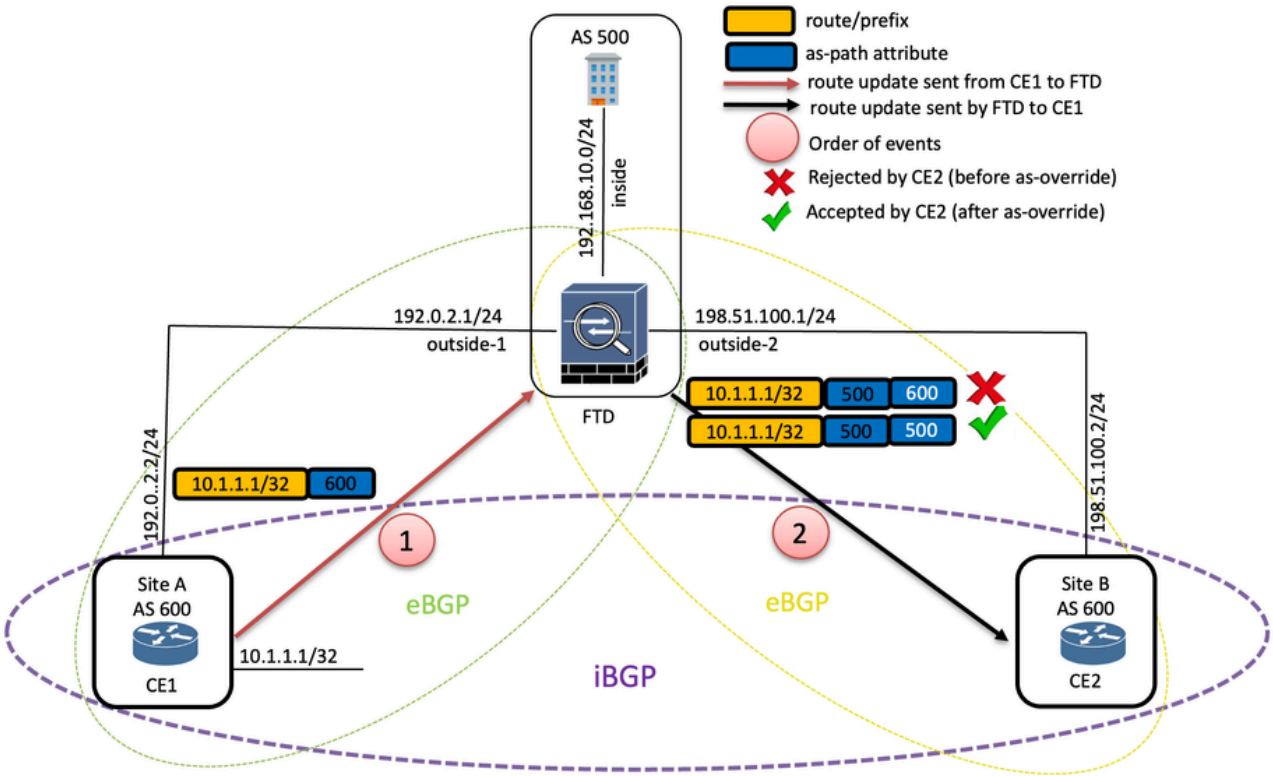
FTD	すべてのFTDプラットフォーム
7.7.0上のFMC FMC REST API	Yes Yes
FTDサポートバージョン	7.7.0のみ
Snortのサポート	Snort 3
7.7.0上のFDM	非サポート

BGP ASオーバーライドパケット処理フロー

- BGPはUPDATEメッセージを介してピア/ネイバーにルートアップデートを送信します。
- 既知の必須属性は、すべてのBGPピアで認識され、すべてのピアに渡され、すべてのUPDATEメッセージに含まれます。
- UPDATEメッセージのAS-path属性には、このアップデートが通過したすべての自律システムの順序付きリストが含まれます。
- as-override CLIが有効な場合、ネイバーAS番号の各オカレンスはas-path内の口ーカルAS番号に置き換えられます。

設定

ネットワーク図



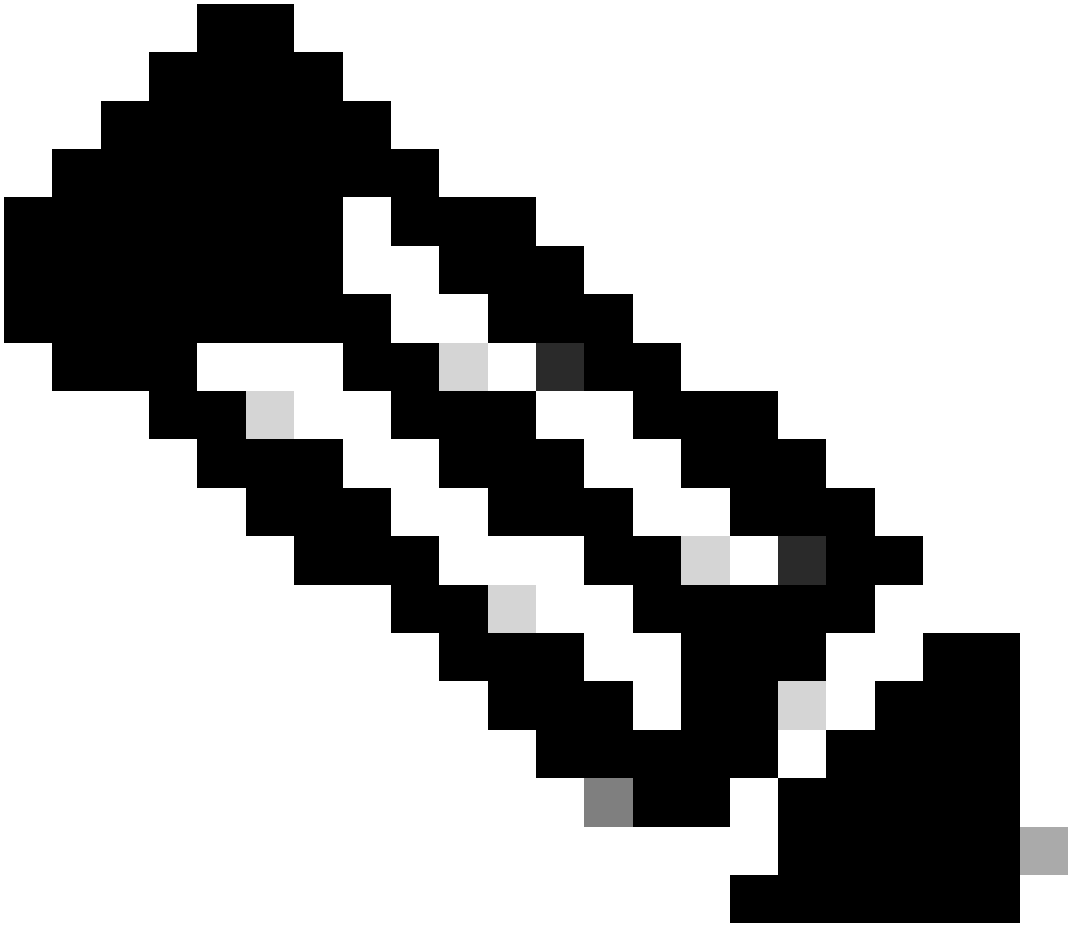
トポロジ

ルート更新フロー

- サイトAとサイトBは、同じAS番号を持つデバイス/ピアを含む2つの同一のサイトです。
- この場合、10.1.1.1/32は、FTDを介してサイトAのCE1からサイトBのCE2にアドバタイズされているプレフィックス/ルートアップデートです。
- as-overrideを有効にする前に、FTDはサイトBのCE2へのルートアップデートをそのまま転送します。ただし、CE2は、これを受信すると、as-path(600)に自身のAS番号が含まれていることを確認して、ルートアップデートを廃棄します。
- as-overrideを有効にした後、FTDは、as-path内のAS番号CE1を自身またはローカルのAS番号(500)に置き換えることによって、ルート更新をCE2に転送します。 ここで、CE2はルートの更新を受け入れます。

機能の概要

- AS Overrideを有効にするためのFMCの新しいチェックボックス。
- 新しいCLIコマンドneighbor <neighbor-ip-address> as-overrideisは、この機能の一部としてBGPに導入されました。



注:BGP ASオーバーライド機能は、Secure Firewall Management Center(FMC)経由でのみ設定できます。

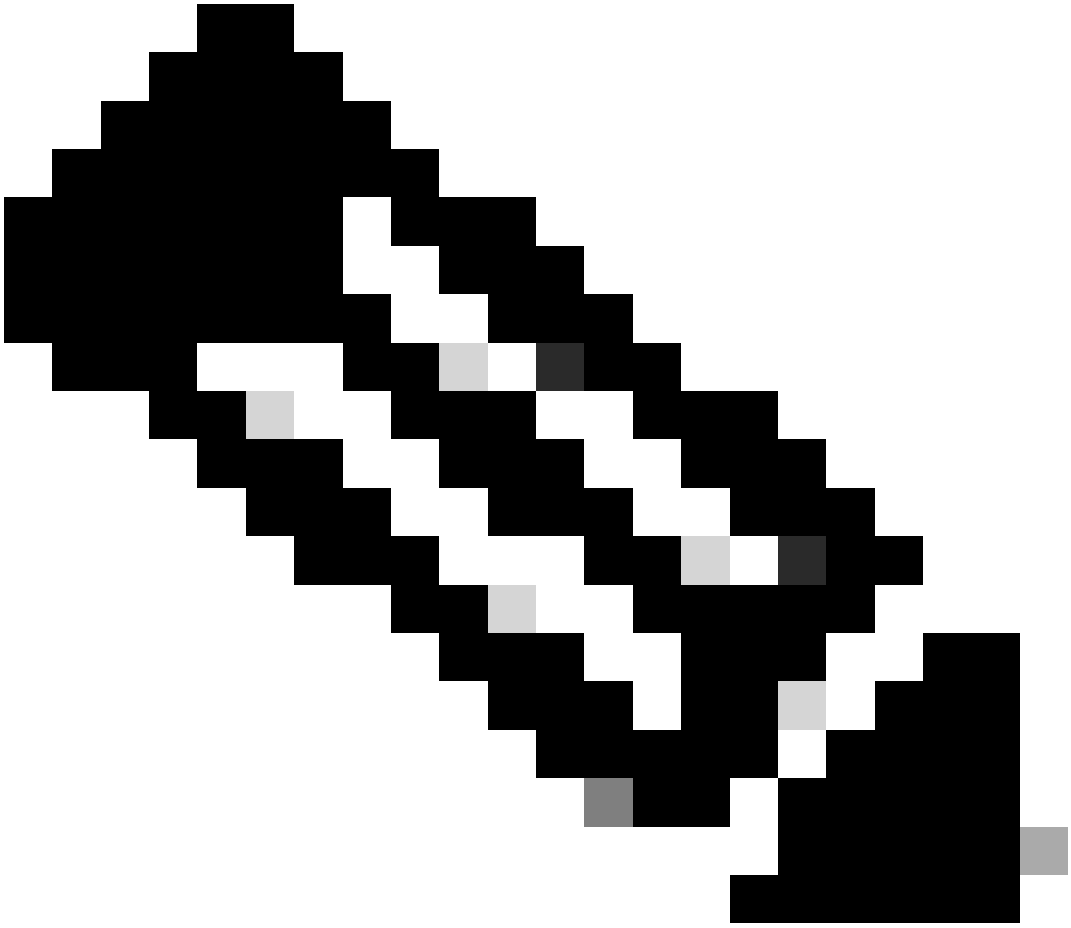
FMCでの設定手順

ステップ1:Devices > Device Managementの順に移動し、脅威対策デバイスを編集します。

ステップ2:Routingを選択します。

ステップ3:（仮想ルータ対応デバイスの場合）:General Settingsの下で、BGPをクリックします。

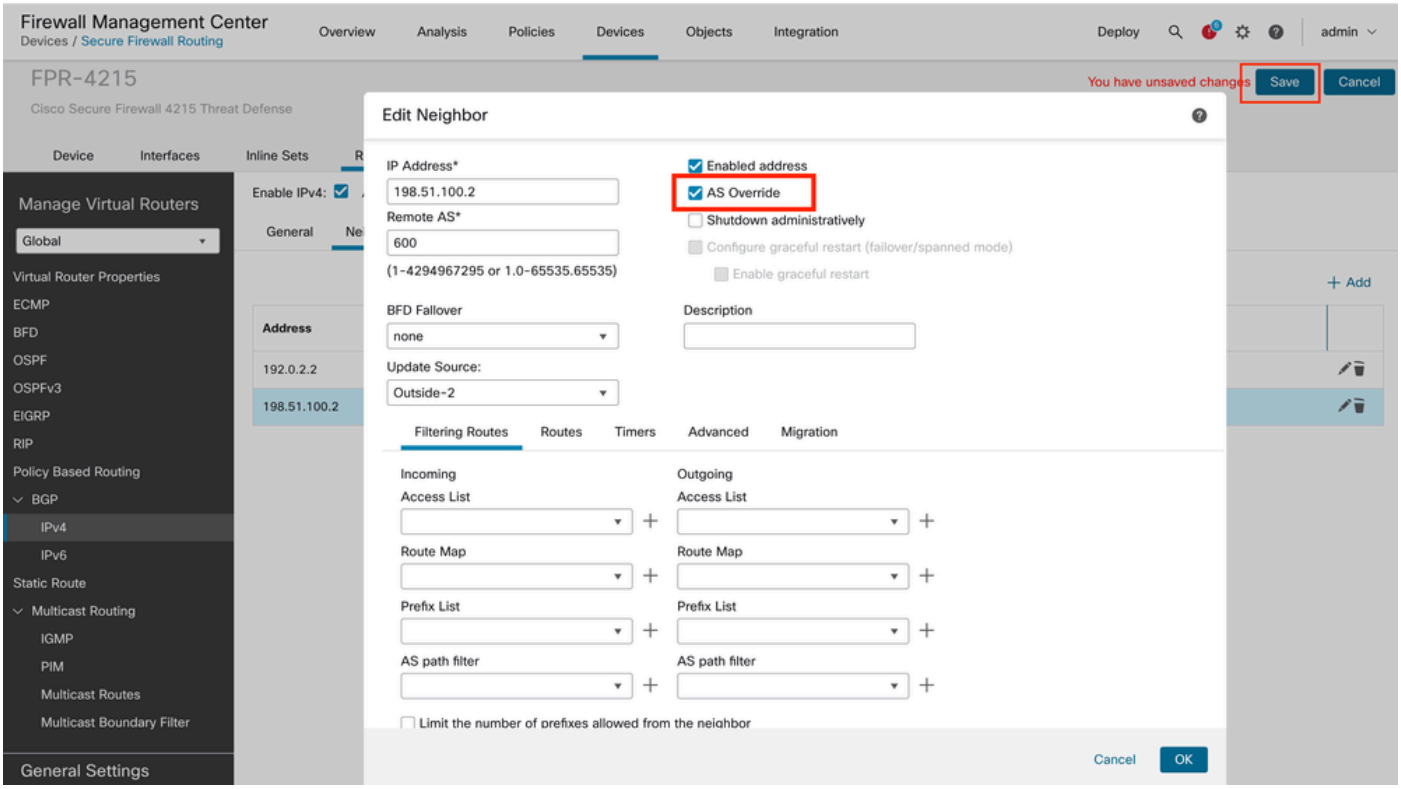
ステップ4:Enable BGPチェックボックスをオンにして、BGPルーティングプロセスを有効にします。



注:BGPルーティングの設定については、『Cisco Secure Firewall Management Centerデバイス設定ガイド、7.7』を参照してください。

BGP IPv4ネイバー

- 198.51.100.2ネイバーに対するAS Overrideを有効にします。
- save and deployをクリックします。



ASオーバーライドの有効化

確認

このセクションでは、設定が正常に動作していることを確認します。

FTD終了：

<#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
```

レシーバ終了：

<#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
```

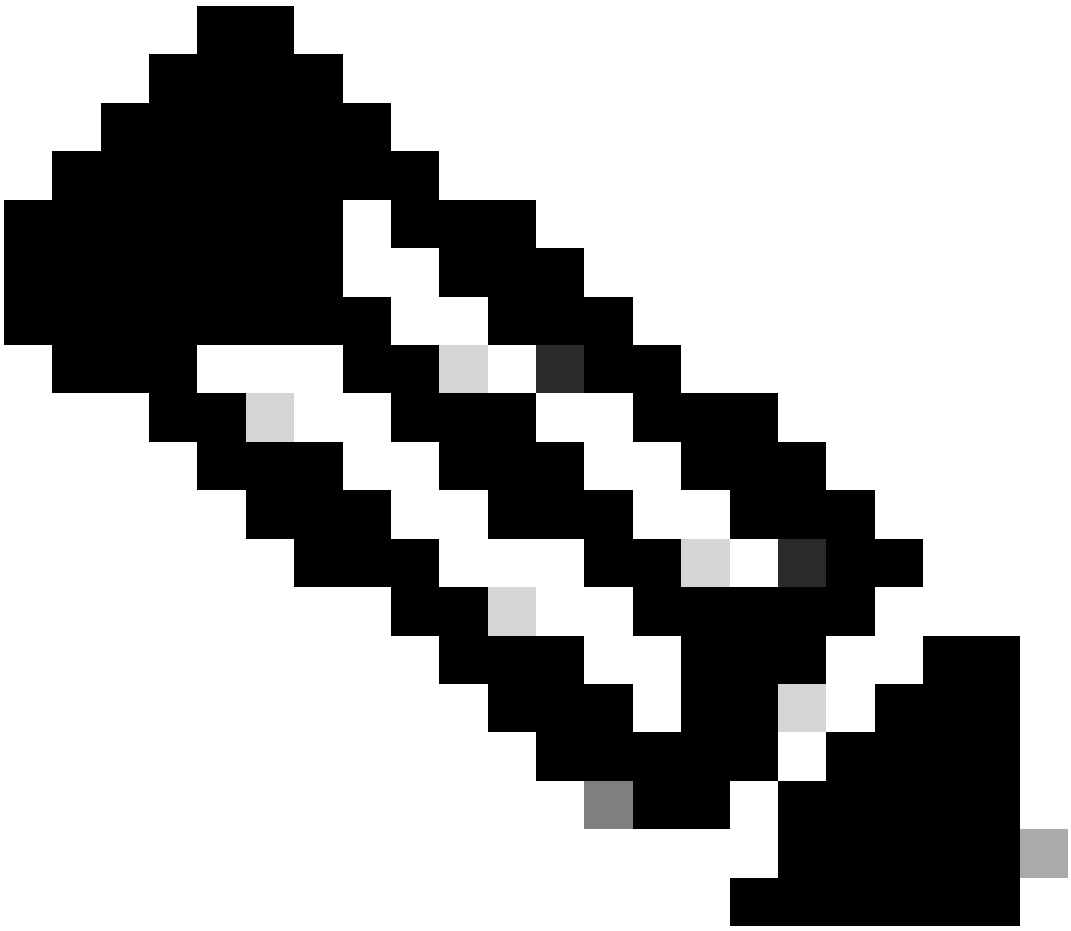
トラブルシュート

コマンド

- show run router bgp allでは、FTDでAS-override CLIが有効になっている必要があります。
- show bgp <ipv4/ipv6> unicast neighbors on FTDでは、as-overrideが有効であることを示す次のテキストを指定する必要があります。> ASは、アップデートを送信する前に、自分のASでネイバーASを上書きします。
- show bgp <ipv4/ipv6>受信側のユニキャストでは、パス情報が変更されている必要があります。

デバッグ

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



注:as-overrideを有効にする前と後のデバッグには変更がありません。

システムファイル

この口グファイルには、FMCからのas-override機能の展開に関する情報が含まれています。

/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
```

関連情報

シスコのテクニカルサポートとダウンロード

Cisco Secure Firewall Management Centerデバイス設定ガイド、7.7

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。