

# 在安全防火墙中配置BGP AS覆盖

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[BGP AS覆盖数据包处理流程](#)

[配置](#)

[网络图](#)

[路由更新流程](#)

[功能概述](#)

[FMC的配置步骤](#)

[验证](#)

[故障排除](#)

[命令](#)

[调试](#)

[系统文件](#)

[相关信息](#)

---

## 简介

本文档介绍如何在思科安全防火墙威胁防御中配置BGP自主系统(AS)覆盖。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- BGP ( 边界网关协议 )
- 思科安全防火墙管理中心(FMC)
- 思科安全防火墙威胁防御(FTD)

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行版本7.7.0的思科安全防火墙管理中心。
- 运行版本7.7.0的思科安全防火墙威胁防御。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息

对于地理位置分散的大型企业，当多个站点使用同一个自治系统(AS)编号时，实现端到端可达性可能颇具挑战性。当前BGP行为是如果AS路径包含自己的AS编号则丢弃收到的路由更新，以避免网络中出现环路。

7.6版本引入了专门针对SD-WAN相关使用案例的as-override支持。但是，从7.7版本开始，由于核心路由要求，eBGP的as-override支持可用于所有部署。这使您可以拥有具有相同AS编号的相同站点。

应用和管理器：

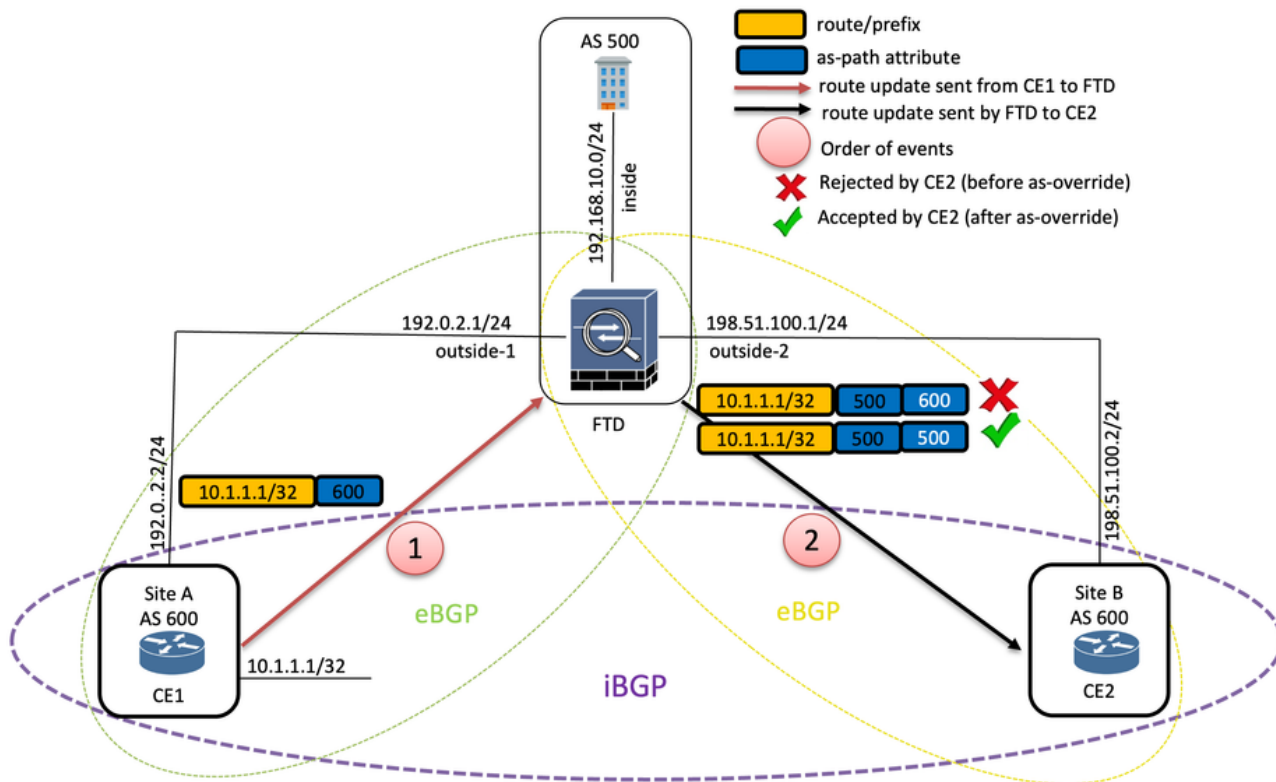
|              |               |
|--------------|---------------|
| FTD          | 所有FTD平台       |
| 7.7.0上的FMC   | Yes           |
| FMC REST API | Yes           |
| FTD支持版本      | 仅7.7.0        |
| Snort支持      | Snort 3       |
| 7.7.0上的FDM   | Not Supported |

## BGP AS覆盖数据包处理流程

- BGP通过UPDATE消息将路由更新发送到其对等体/邻居。
- 所有BGP对等体都会识别已知的、强制的属性，传递到所有对等体，并出现在所有UPDATE消息中。
- UPDATE消息中的AS-path属性包含此更新经过的所有自治系统的有序列表。
- 当启用as-override CLI时，每次出现邻居AS编号都会被as-path中的本地AS编号替换。

## 配置

网络图



拓扑

## 路由更新流程

- 站点A和站点B是包含具有相同AS编号的设备/对等体的两个相同站点。
- 在本例中，10.1.1.1/32是通过FTD从站点A的CE1向站点B的CE2通告的前缀/路由更新。
- 在启用as-override之前，FTD会按原样将路由更新转发到站点B的CE2。但是，CE2收到更新后，会丢弃路由更新，因为它在as-path(600)中看到自己的AS编号。
- 启用as-override后，FTD将路由更新转发到CE2，方法是将其as-path中的CE1的AS编号替换为其自己的/本地AS编号(500)。现在CE2接受路由更新。

## 功能概述

- 在FMC中新建复选框以启用AS覆盖。
- 作为此功能的一部分，BGP中引入了新的CLI命令neighbor <neighbor-ip-address> as-override。



注意：BGP AS覆盖功能仅可通过安全防火墙管理中心(FMC)进行配置。

---

## FMC的配置步骤

步骤 1：导航到Devices > Device Management，然后编辑威胁防御设备。

步骤 2：选择路由。

步骤 3：（对于虚拟路由器感知设备）在General Settings下，单击BGP。

步骤 4：选中Enable BGP复选框以启用BGP路由进程。

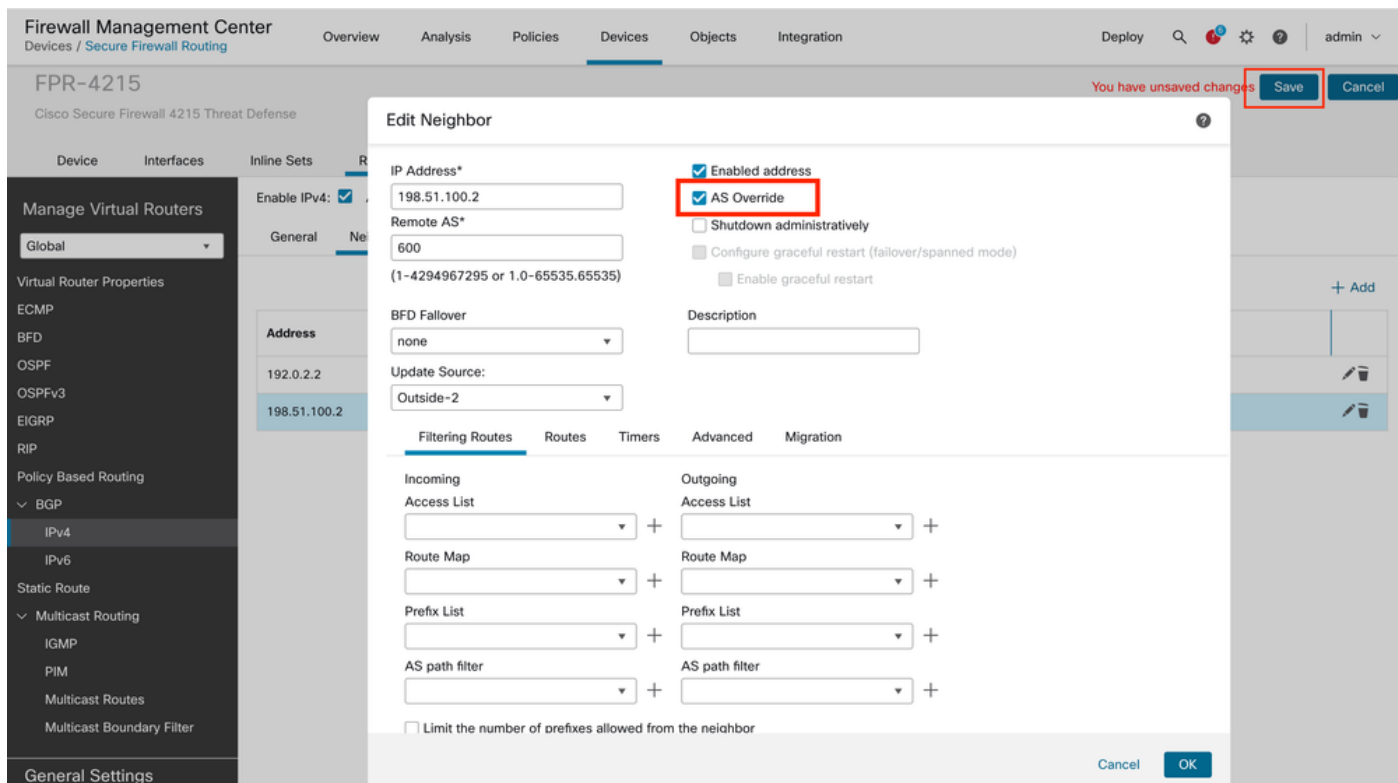


注意：要配置BGP路由，请参阅[Cisco安全防火墙管理中心设备配置指南7.7](#)

---

## BGP IPv4邻居

- 为198.51.100.2邻居启用AS Override。
- 单击save和deploy。



启用AS覆盖

## 验证

使用本部分可确认配置能否正常运行。

FTD结束：

<#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

接收器结束：

<#root>

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

```
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
```

## 故障排除

### 命令

- show run router bgp all必须在FTD中启用AS覆盖CLI。
- show bgp <ipv4/ipv6> unicast neighbors on FTD必须指定此文本，指示as-override已启用 —>在发送更新之前，使用我的AS覆盖邻居AS。
- 接收端的show bgp <ipv4/ipv6>单播必须具有已更改的路径信息。

### 调试

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



注意：启用as-override前后调试没有变化。

---

## 系统文件

此日志文件包含与从FMC部署as-override功能相关的信息。

/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
```

## 相关信息

[思科技术支持和下载](#)

[思科安全防火墙管理中心设备配置指南，7.7](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。