

在安全防火牆中配置BGP AS覆蓋

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[BGP AS覆寫封包處理流程](#)

[設定](#)

[網路圖表](#)

[路由更新流](#)

[功能概述](#)

[FMC的配置步驟](#)

[驗證](#)

[疑難排解](#)

[指令](#)

[值錯](#)

[系統檔案](#)

[相關資訊](#)

簡介

本檔案介紹如何在思科安全防火牆威脅防禦中設定BGP自主系統(AS)覆寫。

必要條件

需求

思科建議您瞭解以下主題：

- BGP (邊界閘道通訊協定)
- 思科安全防火牆管理中心(FMC)
- 思科安全防火牆威脅防禦(FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行版本7.7.0的Cisco Secure Firewall Management Center。
- 思科安全防火牆威脅防禦運行版本7.7.0。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

對於地理位置分散的大型企業，當多個站點使用相同的自治系統(AS)編號時，實現端到端可達性可能頗具挑戰性。當前BGP行為是如果AS路徑包含自己的AS編號，則丟棄接收的路由更新，以避免網路中出現環路。

7.6版本引入了專門針對SD-WAN相關使用案例的覆蓋支援。但是，從7.7版本開始，由於其核心路由要求，eBGP的as-override支援可用於所有部署。這樣，您就可以擁有具有相同AS編號的相同站點。

應用程式和管理程式：

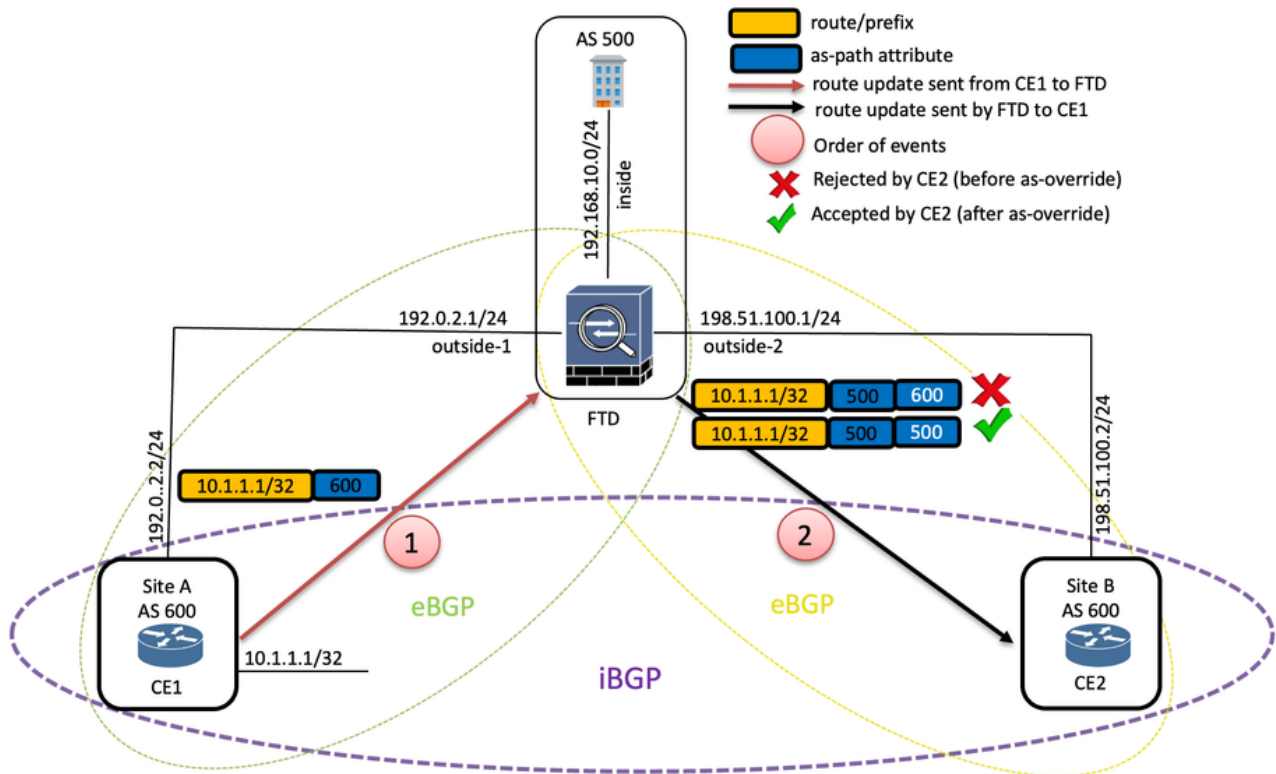
FTD	所有FTD平台
7.7.0上的FMC	是
FMC REST API	是
FTD支援版本	僅7.7.0
Snort支援	Snort 3
7.7.0上的FDM	不支援

BGP AS覆寫封包處理流程

- BGP通過UPDATE消息將路由更新傳送給其對等體/鄰居。
- 所有BGP對等體都會識別已知的強制屬性，並將其傳遞給所有對等體，並出現在所有UPDATE消息中。
- UPDATE消息中的AS-path屬性包含此更新所經過的所有自治系統的有序清單。
- 啟用as-override CLI後，每個出現的鄰居AS編號都會被as-path中的本地AS編號替換。

設定

網路圖表



拓撲

路由更新流

- 站點A和站點B是包含具有相同AS編號的裝置/對等體的兩個相同站點。
- 在本例中，10.1.1.1/32是正在通過FTD從站點A的CE1向站點B的CE2通告的字首/路由更新。
- 在啟用as-override之前，FTD將路由更新像現在一樣轉發到站點B的CE2。但是，CE2收到路由更新後，會放棄路由更新，因為它在as-path(600)中看到自己的AS編號。
- 啟用as-override後，FTD將as-path中CE1的AS編號替換為自己的本地AS編號(500)，從而將路由更新轉發到CE2。現在CE2接受路由更新。

功能概述

- FMC中新增覈取方塊以啟用AS覆蓋。
- 作為此功能的一部分，BGP中引入了新CLI命令neighbor <neighbor-ip-address> as-override。



附註：BGP AS Override功能只能通過安全防火牆管理中心(FMC)進行配置。

FMC的配置步驟

步驟 1:導覽至Devices > Device Management，然後編輯threat defense裝置。

步驟 2:選擇Routing。

步驟 3: (對於虛擬路由器感知裝置) 在General Settings下，按一下BGP。

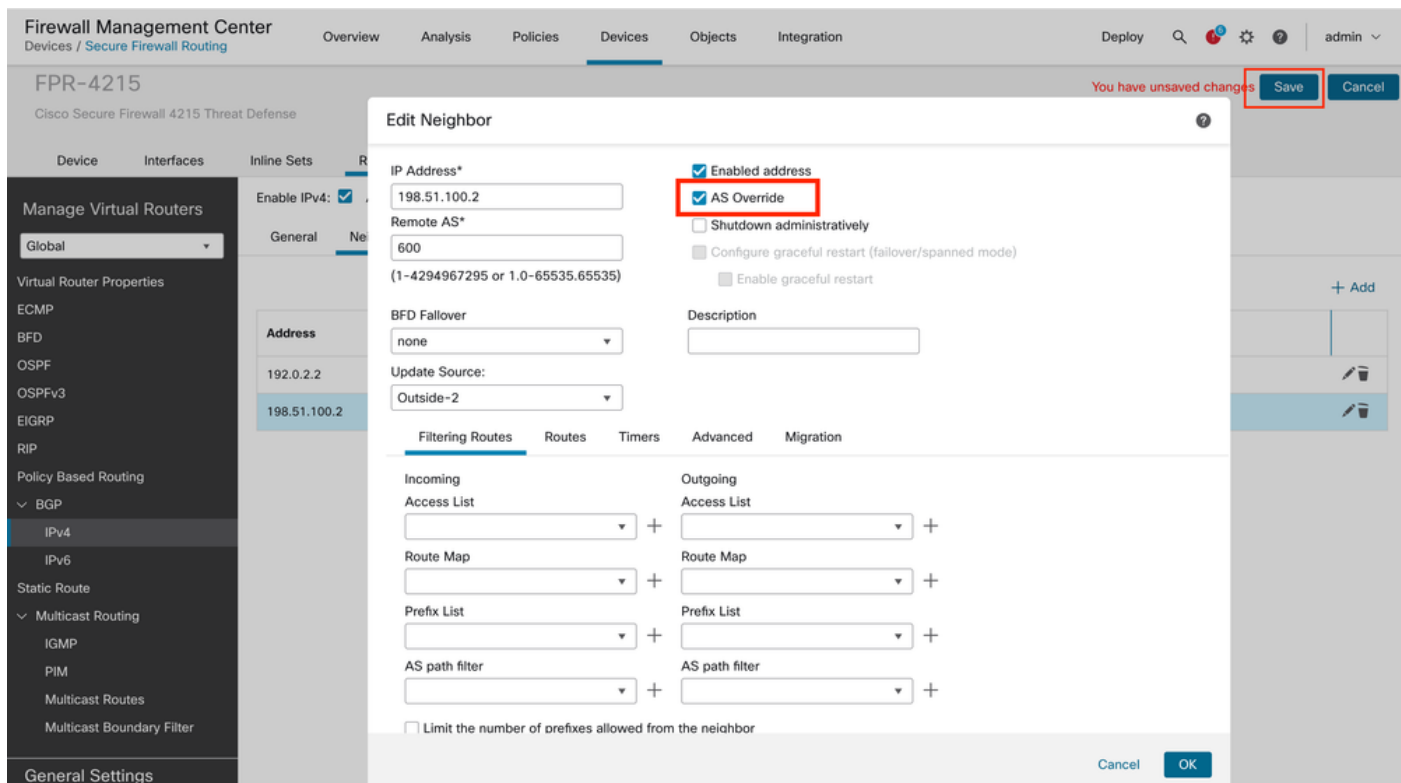
步驟 4:勾選「Enable BGP」覈取方塊以啟用BGP路由進程。



附註：要配置BGP路由，請參閱[思科安全防火牆管理中心裝置配置指南7.7](#)

BGP IPv4鄰居

- 為198.51.100.2鄰居啟用AS Override。
- 按一下「save」和「deploy」。



啟用AS覆蓋

驗證

使用本節內容，確認您的組態是否正常運作。

FTD結束：

<#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

接收器結束：

<#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
```

疑難排解

指令

- show run router bgp all必須在FTD中啟用AS覆寫CLI。
- show bgp <ipv4/ipv6> FTD上的單點傳播鄰居必須指定此文字，指示as-override已啟用 — >在傳送更新之前，使用我的AS覆寫鄰居AS。
- 接收端的show bgp <ipv4/ipv6>單點傳播必須包含已變更的路徑資訊。

偵錯

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



附註：啟用as-override前後的debug沒有變化。

系統檔案

此日誌檔案包含與從FMC部署as-override功能相關的資訊。

/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
```

相關資訊

[思科技術支援與下載](#)

[思科安全防火牆管理中心裝置配置指南7.7](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。