

在FTD上設定具有軟式重新設定限制的BGP路由

目錄

[問題](#)

[環境](#)

[解析](#)

[功能限制](#)

[替代方法 \(路由更新功能\)](#)

[原因](#)

[相關內容](#)

- [問題](#)
 - [環境](#)
 - [解析](#)
 - [功能限制](#)
 - [替代方法 \(路由更新功能\)](#)
 - [原因](#)
 - [相關內容](#)
-

問題

使用者嘗試使用防火牆管理中心(FMC)在防火牆威脅防禦(FTD)中的BGP對等點上設定邊界閘道通訊協定(BGP)軟式重新設定時，無法透過標準FMC BGP介面完成設定。此外，嘗試使用FlexConfig對象實現此功能會導致在BGP neighbor soft-reconfiguration命令的各個部分的文本輸入過程中出錯。具體要求是在BGP鄰居上啟用軟重新配置入站以儲存接收的路由，以用於策略評估和故障排除目的。

環境

- 硬體：安全防火牆3100。其他硬體平台也受到影響。
- 軟體：FTD(此限制也適用於調適型安全裝置(ASA))。
- FMC 7.4.6版。其他軟體版本也受到影響。

- FTD版本7.4.6。其他軟體版本也受到影響。
- FTD具有BGP路由通訊協定組態。

解析

撰寫本文時，FTD裝置不支援傳統BGPneighbor inbound soft-reconfiguration(BGP命令neighbor x.x.x.x soft-reconfiguration inbound)，這些裝置或是透過FMC BGP使用者介面，或是作為支援的FlexConfig方法。

功能限制

以下BGP軟重新配置功能不可用：

- FMC BGP配置沒有為鄰居軟重新配置入站提供配置選項。
- 嘗試通過FlexConfig配置等效的CLI失敗，因為它不是受支援的FTD/FMC管理的BGP配置項。

替代方法（路由更新功能）

與BGP對等點交涉時，FTD支援BGP路由刷新功能。這為在策略更改後的動態軟重置行為提供了支援的機制，儘管它與傳統的軟重新配置入站功能不同。

推薦的方法包括：

- 繼續通過FMC支援的BGP配置工作流配置BGP鄰居、字首清單、路由對映和過濾。
- 確認BGP對等體協商路由刷新功能：

```
<#root>
```

```
device#
```

```
show bgp neighbors 192.0.2.2
```

```

BGP neighbor is 192.0.2.2, context single_vf, remote AS 65535, internal link
BGP version 4, remote router ID 192.0.2.2
BGP state = Established, up for 00:17:39
Last read 00:00:31, last write 00:00:31, 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)

```

<----- BGP Route Refresh capability is enabled on both peers
  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

      Sent      Rcvd
Opens:         1         1
Notifications: 0         0
Updates:       1         3
Keepalives:    17        20

```

Route Refresh: 1 0

```

<----- The neighbor sent 1 BGP Route Refresh message
Total:         20         24

```

- 使用路由刷新行為進行策略重新評估，而不是嘗試啟用入站軟重新配置，例如：

```
<#root>
```

```
device#
```

```
clear bgp 192.0.2.2 in
```

- 若要瞭解稽核所有接收和拒絕的路由的操作要求，請從BGP對等體/路由器端進行驗證。

比較

功能	BGP路由刷新功能	入站軟重新配置
FTD/ASA上支援	是	否

工作方式	路由器向鄰居傳送一條明確的BGP路由刷新請求消息，要求其重新通告其路由表。	路由器分配額外的RAM，以將鄰居BGP表的未過濾的原始副本儲存到本地記憶體中。
配置要求	無.預設情況下在FTD和ASA上自動啟用。	需要手動設定(neighbor x.x.x.x soft-reconfiguration inbound)，但FTD/ASA不支援此命令。
記憶體消耗	非常低。RAM中未儲存額外的路由表。	非常高。該鄰居的路徑佔用更多記憶體。
觸發器命令	# clear bgp x.x.x.x in	ASA/FTD上不受支援。
鄰居依賴關係	會。遠端BGP對等體還必須支援並接受路由刷新功能。	不。它完全位於防火牆本地；對等鄰居不知道它已啟用。
指令:show bgp neighbor x.x.x.x received-routes	不支援/失敗。路由器不儲存本地副本。運行此命令將返回錯誤(% Inbound soft reconfiguration not enabled on x.x.x.x)。	支援 .在應用策略之前，立即顯示當前快取到路由器RAM中的原始未過濾路由。

原因

這是FTD和ASA裝置的功能限制。FMC BGP組態介面中或作為FTD裝置支援的FlexConfig選項未實作BGP鄰居傳入軟重新設定功能。此限制追蹤為思科錯誤ID [CSCvy97220](#)的軟體增強功能。

相關內容

- [FMC BGP組態設定指南\(10.x\)](#)
- [適用於BGP鄰居和摘要可見性的FTD命令參考](#)
- [思科錯誤ID CSCvy97220 - BGP鄰居入站軟重新配置支援的增強請求](#)
- [思科技術支援與下載](#)

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）。