從7.1開始的BGP中VPN路由通告的行為更改

目錄

簡介

本文檔介紹從版本7.1開始向BGP路由表注入VPN路由的行為變化。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower技術知識
- 有關配置BGP和路由通告的知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全防火牆管理中心(FMC)
- Cisco Firepower威脅防禦(FTD)

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

要求是透過BGP通告VPN路由。

正在使用下一跳匹配條件過濾VPN路由。

標準訪問清單配置為匹配下一跳0.0.0.0。

行為變更

在版本6.6.5中，VPN路由被注入BGP路由表中，下一跳設定為0.0.0.0。

在版本7.1中，VPN路由被注入到BGP路由表中，下一跳被設定為相應子網的網路IP地址。

組態

BGP配置：

router bgp 12345 bgp log-neighbor-changes bgp router-id vrf auto-assign address-family ipv4 unicast neighbor 172.30.0.21 remote-as 12346 neighbor 172.

路由對映配置：

firepower# sh run route-map VPN_INSIDE_OUT route-map VPN_INSIDE_PRI_OUT permit 10 match ip next-hop NextHopZeroes firepower# sh run acc

透過此配置，BGP僅通告下一跳定義為0.0.0.0的路由。

路由表中的VPN路由安裝：

firepower# sh route | inc 172.20.192
V 172.20.192.0 255.255.252.0 connected by VPN (advertised), VPN-OUTSIDE

show bgp的輸出：

在6.6.5版中

show bgp :
*> 172.20.192.0/22 0.0.0.0 0 32768 ?

可以看到，子網172.20.192.0/22安裝在BGP表中，下一跳IP定義為0.0.0.0。

在7.1版中

show bgp :
*> 172.20.192.0/22 172.20.192.0 0 32768 ?

可以看到子網172.20.192.0/22安裝在BGP表中，下一跳IP定義為子網網路IP ： 172.20.192.0。

影響案例

如果配置包括匹配下一跳IP為0.0.0.0的路由對映集，則路由過濾會受到影響，VPN路由不會通告。

解決方法

兩個可用的工作方案：

- 建立所有VPN子網的清單，並分別配置它們以便透過BGP進行通告。注意：此方法不可擴展。
- 配置BGP以通告本地生成的路由。套用此組態指令：

route-map <route-map-name> permit 10
match route-type local

透過實施前面討論的解決方案之一，FTD將透過BGP通告VPN注入的路由。

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）。