从7.1开始的BGP中VPN路由通告的行为更改

目录

简介

本文档介绍从版本7.1开始向BGP路由表注入VPN路由的行为变化。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower技术知识
- 有关配置BGP和路由通告的知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全防火墙管理中心(FMC)
- 思科Firepower威胁防御(FTD)

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

要求是通过BGP通告VPN路由。

VPN路由使用下一跳匹配条件过滤。

将标准访问列表配置为匹配下一跳0.0.0.0。

行为更改

在版本6.6.5中，VPN路由被注入下一跳设置为0.0.0.0的BGP路由表。

在版本7.1中，VPN路由会插入到BGP路由表中，并且下一跳设置为相应子网的网络IP地址。

配置

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.

路由映射配置：

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

使用此配置，BGP仅通告下一跳定义为0.0.0.0的路由。

VPN**路由安装在路由表中**：

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

show bgp的输出：

在版本6.6.5中

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

可以看到子网172.20.192.0/22安装在BGP表中，下一跳IP定义为0.0.0.0。

在7.1版中

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

可以看到子网172.20.192.0/22安装在BGP表中，下一跳IP定义为子网网络IP ： 172.20.192.0。

影响情景

如果配置包括匹配下一跳IP为0.0.0.0的路由映射集，则路由过滤会受到影响，并且VPN路由不会通告。

解决方法

两个可用的解决方法：

- 创建所有VPN子网的列表并单独配置它们以通过BGP进行通告。注意：此方法不可扩展。
- 配置BGP以通告本地生成的路由。应用此配置命令：

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

通过实施之前讨论的解决方案之一，FTD将通过BGP通告VPN注入的路由。

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）。