

在FTD上配置具有软重新配置限制的BGP路由

目录

[问题](#)

[环境](#)

[分辨率](#)

[功能限制](#)

[替代方法 \(路由更新功能\)](#)

[原因](#)

[相关内容](#)

- [问题](#)
 - [环境](#)
 - [分辨率](#)
 - [功能限制](#)
 - [替代方法 \(路由更新功能\)](#)
 - [原因](#)
 - [相关内容](#)
-

问题

当用户尝试使用防火墙管理中心(FMC)在防火墙威胁防御(FTD)中的BGP对等设备上配置边界网关协议(BGP)软重新配置时，配置无法通过标准FMC BGP接口完成。此外，尝试使用FlexConfig对象实现此功能会导致在BGP neighbor soft-reconfiguration命令的各个部分的文本输入过程中出错。具体要求是在BGP邻居上启用软重新配置入站，以存储接收的路由，用于策略评估和故障排除。

环境

- Hardware:Secure Firewall 3100.其他硬件平台也受到影响。
- 软件：FTD(此限制也适用于自适应安全设备(ASA))。
- FMC版本7.4.6。其他软件版本也受到影响。
- FTD版本7.4.6。其它软件版本也受到影响。

- FTD具有BGP路由协议配置。

分辨率

在撰写本文时，传统BGP邻居入站软重新配置（BGP命令neighbor x.x.x.x soft-reconfiguration inbound）在FTD设备上不受支持，无论是通过FMC BGP用户界面还是作为支持的FlexConfig方法。

功能限制

以下BGP软重新配置功能不可用：

- FMC BGP配置不提供邻居软重新配置入站的配置选项。
- 尝试通过FlexConfig配置等效的CLI失败，因为它不是受支持的FTD/FMC管理的BGP配置项。

替代方法（路由更新功能）

在与BGP对等体协商时，FTD支持BGP路由刷新功能。这在策略更改后动态软重置行为提供支持的机制，尽管它不同于传统的软重新配置入站功能。

推荐的方法包括：

- 继续通过FMC支持的BGP配置工作流程配置BGP邻居、前缀列表、路由映射和过滤。
- 确认BGP对等体协商路由刷新功能：

<#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

- 使用路由刷新行为进行策略重新评估，而不是尝试启用入站软重新配置，例如：

```
<#root>  
device#  
  
clear bgp 192.0.2.2 in
```

- 有关审核所有已接收和已拒绝路由的操作要求，请从BGP对等体/路由器端进行验证。

比较

功能	BGP路由刷新功能	入站软重新配置
FTD/ASA上支持	Yes	无
工作原理	路由器向邻居发送显式BGP路由刷新请求	路由器分配额外的RAM以将邻居

	消息，要求其重新通告其路由表。	BGP表的未过滤的原始副本保存到本地内存中。
配置要求	无.默认情况下，在FTD和ASA上自动启用。	需要手动配置(<code>neighbor x.x.x.x soft-reconfiguration inbound</code>)，但FTD/ASA上不支持该命令。
内存消耗	超低.RAM中不会存储额外的路由表。	非常高.为该邻居的路径消耗更多内存。
触发器命令	<code># clear bgp x.x.x.x in</code>	ASA/FTD不支持。
邻居依赖关系	Yes.远程BGP对等体还必须支持并接受路由刷新功能。	不。它完全位于防火墙的本地；对等邻居不知道它已启用。
命令: <code>show bgp neighbor x.x.x.x received-routes</code>	不支持/失败。路由器不存储本地副本。运行此命令会返回错误(% Inbound soft reconfiguration not enabled on x.x.x.x)。	受支持.在应用策略之前，立即显示当前缓存到路由器RAM中的未过滤的原始路由。

原因

这是FTD和ASA设备的功能限制。BGP邻居入站软重新配置功能尚未在FMC BGP配置接口中实现，也没有作为FTD设备支持的FlexConfig选项实现。此限制作为软件增强漏洞ID [CSCvy97220](#)进行跟踪。

相关内容

- [FMC BGP配置指南\(10.x\)](#)
- [BGP邻居和摘要可视性的FTD命令参考](#)
- [Cisco Bug ID CSCvy97220 - BGP邻居入站软重新配置支持的增强请求](#)
- [思科技术支持和下载](#)

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）。