

安全访问网络隧道中的BGP路由通告差异

目录

[问题](#)

[环境](#)

[分辨率](#)

[步骤 1：确定特定的网络前缀](#)

[步骤 2：检验时间线和图案](#)

[步骤 3：记录BGP对等体配置](#)

[步骤 4：查看最近的配置更改](#)

[步骤 5：检查本地路由表](#)

[步骤 6：验证安全访问组织配置](#)

[原因](#)

[相关内容](#)

- [问题](#)
 - [环境](#)
 - [分辨率](#)
 - [步骤 1：确定特定的网络前缀](#)
 - [步骤 2：检验时间线和图案](#)
 - [步骤 3：记录BGP对等体配置](#)
 - [步骤 4：查看最近的配置更改](#)
 - [步骤 5：检查本地路由表](#)
 - [步骤 6：验证安全访问组织配置](#)
 - [原因](#)
 - [相关内容](#)
-

问题

使用边界网关协议(BGP)的安全访问站点到站点网络隧道遇到路由通告差异，其中BGP对等体将获取已配置的/23网络前缀作为/24前缀。预期路由在安全访问中配置为/23子网，但BGP对等体正在使用/24子网掩码接收和学习此网络，这会在两个BGP对等体之间的路由表中造成不一致。

环境

使用网络隧道(互联网协议安全(IPSec)、站点到站点)的思科安全访问

- BGP路由协议配置
- 站点到站点VPN隧道实施
- 使用/23和/24子网的网络前缀配置

分辨率

要解决此BGP路由通告差异，这些故障排除和验证部分概述了必须执行的步骤。

步骤 1：确定特定的网络前缀

确定路由差异中涉及的确切/23和/24前缀。记录BGP对等关系的哪一端正在通告/24前缀而不是预期的/23前缀。

步骤 2：检验时间线和图案

确定第一次观察问题的时间，并确定问题是连续出现还是间歇出现。此信息有助于识别与路由行为相关的潜在触发器或模式。

步骤 3：记录BGP对等体配置

收集有关BGP对等设备配置的详细信息。确定在安全访问中配置的特定网络隧道名称遇到此路由差异。

步骤 4：查看最近的配置更改

调查任何可能导致此问题的近期更改，包括：

- 配置修改
- 路由策略更新
- 网络地址转换(NAT)配置更改
- 软件版本更新
- 子网或网络地址更改

步骤 5：检查本地路由表

验证本地路由表中是否存在可以选择或通告的更具体的/24路由，而不是配置的/23前缀。这是BGP中意外路由通告的常见原因，其中更具体的路由优先于不太具体的路由。

步骤 6：验证安全访问组织配置

获取并验证安全访问组织ID，以确保正确访问安全访问管理界面中的配置详细信息和故障排除功能。

原因

此BGP路由通告差异最可能的原因是本地路由表中存在更具体的/24路由，该路由是正在选择和通告的，而不是配置的/23前缀。BGP遵循最长前缀匹配规则，其中更具体的路由（更长的子网掩码）优先于更少的具体路由。如果/24子网存在于/23范围内，BGP会将更具体的/24路由通告给它的对等体，而不是更宽泛的/23网络。

其他可能的原因包括路由策略配置、路由过滤或网络地址转换(NAT)配置，这些配置可以在BGP路由通告过程中修改通告的前缀长度。

相关内容

- [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）。