由于安全访问AWS Direct Connect集成中的路由前缀限制，BGP会话抖动

目录

问题

BGP会话在Cisco Secure Access和AWS Direct Connect之间的站点到站点隧道上遇到抖动。这种不稳定性的发生是因为从安全访问通告的路由前缀数量超过了AWS Direct Connect的限制，从而阻止了稳定的路由交换，并影响了在安全访问和AWS之间建立一致连接的能力。

环境

- 思科安全访问(CSA)
- 采用BGP路由的AWS Direct Connect
- Secure Access和AWS之间的站点到站点隧道配置
- AWS Direct Connect BGP前缀限制为100个路由

分辨率

解决方法涉及多种方法来解决BGP前缀限制约束。

网络数据包分析显示BGP NOTIFICATION消息，指示已达到最大前缀数：

```
Border Gateway Protocol - NOTIFICATION Message
    Length: 28
    Type: NOTIFICATION Message (3)
    Major error Code: Cease (6)
    Minor error Code (Cease): Maximum Number of Prefixes Reached (1)
```

即时解决方法

选项 1：AWS端路由过滤

评估AWS端选项，以忽略或过滤来自Secure Access的传入路由前缀，使其保持在AWS Direct Connect规定的100前缀限制范围内。

选项 2：AWS传输网关实施

考虑迁移到AWS Transit Gateway作为替代连接模式。此方法可提供更灵活的路由选项，并可帮助绕过Direct Connect前缀限制。

长期解决方案

功能请求实施

已提交功能请求(CSE-I-4783)，以允许安全访问上的路由过滤或汇总功能。此增强功能将实现：

- 路由总结可减少通告的前缀的数量
- 路由过滤，控制将哪些前缀通告给AWS Direct Connect
- 从安全访问端更好地控制BGP通告

实施步骤

1:查看AWS Direct Connect限制。请参阅AWS Direct Connect限制文档以了解具体的限制条件。

2:评估当前路由通告。分析当前从安全访问通告的路由数量，确定有多少路由超过100前缀AWS限制。

3:立即实施应急方案。根据网络架构要求和业务需求，选择AWS端过滤或传输网关实施。

4:监控功能请求进度。与适用的思科客户团队合作，审核提议的路由过滤/汇总功能请求的可行性和影响。

原因

根本原因在于AWS Direct Connect中的基本限制，即将BGP路由通告限制为最多100个前缀。Cisco Secure Access正在通告100多个路由前缀，导致AWS Direct Connect发送BGP NOTIFICATION消息，其中含有错误代码“Maximum Number of Prefixes Reached”，然后中断BGP会话。这会创建一个会话建立和拆除的循环，导致观察到的BGP会话抖动行为。

相关内容

- AWS Direct Connect限制文档
- 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）。