在IKE重新生成密钥事件期间，安全访问网络隧道组与Azure VPN网关的间歇性抖动

目录

问题

在IKE重新生成密钥事件期间，思科安全访问和Azure VPN网关之间新配置的网络隧道组大约每4小时发生一次间歇性隧道抖动。

观察到以下特定错误消息和症状：

- BGP对等，保持计时器已过期
- 预警:失败的IKE重新生成密钥
- IKE隧道已断开

隧道抖动会导致定期中断、IKE密钥更新失败、完整性检查失败、隧道断开和BGP对等丢弃，从而影响到Azure资源的稳定连接。在重新生成密钥协商期间观察到身份验证失败。

环境

- 配置到Azure VPN网关的思科安全访问(CSA)网络隧道组
- 使用IKEv2的IPsec站点到站点VPN隧道
- 在主模式(MM)策略中配置AES-GCM-256加密的Azure VPN网关
- 使用端口4500在两端启用NAT-T（NAT穿越）
- 在终端之间配置BGP对等
- 默认IKE SA生存时间为4小时（28800秒）
- 初始IPsec SA生存期配置，后来修改为10800秒

- 未在Azure端启用PFS（完全向前保密）

分辨率

根据Azure VPN网关中的错误识别，通过更改配置来避免在主模式策略中使用AES-GCM密码来解决此问题。

步骤 1：Azure VPN网关调试分析

从Azure VPN网关端收集IKE调试，在重新生成密钥尝试期间显示以下行为：

```
SESSION_ID :{} Remote x.x.x.x:500: Local x.x.x.x:500: [SEND]Sending IPSec policy Payload for tunnel Id
SESSION_ID :{} Remote x.x.x.x:4500: Local x.x.x.x:4500: [SEND][CHILD_SA MM_REKEY] Sending IKE rekey res
SESSION_ID :{} Remote x.x.x.x:4500: Local x.x.x.x:4500: [LOCAL_MSG] IKE Tunnel closed for tunnelId x3 w
```

步骤 2：根本原因识别

Azure支持调查了重新生成密钥失败。Azure分析发现，当Azure使用AES-GCM-256启动MM-REKEY时，重新生成密钥数据包的格式不正确。本地设备不响应格式错误的密钥重新生成请求，从而导致隧道断开。

步骤 3：配置应急方案

根据Azure的建议，实施了以下缓解措施：

- 从网络隧道组配置的主模式(MM)策略中删除AES-GCM密码。
- 配置不使用GCM模式的备用加密方法。

请参阅https://securitydocs.cisco.com/docs/csa/olh/121327.dita中的步骤17。

步骤 4：替代缓解选项

Azure还提供了可考虑的其他缓解策略：

- 将本地MM生存期配置为大于28800秒，以便Azure始终启动重新生成密钥。
- 将Azure VPN网关设置为仅响应方模式，本地SA生存期小于Azure生存期。

原因

根本原因是Azure VPN网关中存在影响AES-GCM重新生成密钥操作的漏洞。当Azure使用AES-GCM-256启动MM-REKEY时，重新生成密钥数据包的格式不正确，导致本地思科安全访问设备无法响应格式不正确的重新生成密钥请求。这会导致IKE重新生成密钥失败、身份验证错误和后续隧道断开。

Azure已确认这是一个现有的Bug，并记录了在未来网关版本中计划实施的修复程序，该版本定于2026年中发布。

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）。