在安全访问和Azure/AWS中托管的C8000Vs之间的IPSec隧道抖动

目录

问题

C8000V/Cisco IOS-XE路由器与us-east-2区域中的思科安全访问网络之间的IPsec网络隧道出现抖动。

所有隧道组都会受到影响，从而导致内部路由器与思科安全访问网络之间的隧道关闭。

环境

- 技术：解决方案支持（SSPT — 需要合同）
- 子技术：安全访问 — 网络隧道（IPSEC、站点到站点、专用资源）
- 产品系列：SEACCS
- 路由器：C8000V / Cisco IOS-XE路由器（内部）
- 远程终端：思科安全访问网络（美国东部2地区）
- 软件版本：未指定
- 错误消息、日志、调试
- 在中断期间没有受影响的最终用户

分辨率

从CNHE Splunk日志

端口= 1409

sourceIpAddr = x.x.x.x

端口= 1408

sourceIpAddr = x.x.x.x

1. 检测到远程终端更改（端口已更新）
2. Cortex在此更新时触发子项重新生成密钥
3. 在使用新端口重新生成密钥时客户端没有响应，因此cortex会耗尽重试并终止隧道
4. 在客户端使用新端口重新发起后不久，隧道将启动

从CSA Splunk日志。

2026-02-02T16:36:02.188+00:00触发使用本地IP的ike更新的子密钥重新生成密钥

：x.x.x.x，ike_spi:new_datanode:

2026-02-02T16:36:04.207+00:00重新传输1个请求，带消息ID 0

2026-02-02T16:36:08.207+00:00重新传输2个请求，带消息ID 0

2026-02-02T16:36:16.207+00:00重新传输3个请求，带消息ID 0

2026-02-02T16:36:32.207+00:00重新传输4个请求，带消息ID 0

2026-02-02T16:37:04.207+00:00重新传输5个请求，带消息ID 0

2026-02-02T16:38:08.208+00:00在5次重新传输后放弃

2026-02-02T16:38:08.208+00:00终止IKE，子SA重新生成密钥失败

从调试日志1769305781091_vJY_CENTRAL_R2.log中:

无效的SPI错误 — 经常发生：

*1月24日07:55:04.209: %CRYPTO-4-RECVD_PKT_INV_SPI:decaps: rec'd IPSEC数据包的spi无效，目标为destaddr=x.x.x.x prot=50,spi=,srcaddr=x.x.x.x，input interface=Tunnel12

*1月24日07:56:06.829: %CRYPTO-4-RECVD_PKT_INV_SPI:decaps: rec'd IPSEC数据包的spi无效，对于destaddr=x.x.x.x，prot=50,spi=,srcaddr=x.x.x.x，input interface=Tunnel11

隧道抖动 — 多个隧道关闭/开启实例：

*Jan 24 08:33:12.069: %LINEPROTO-5-UPDOWN：接口Tunnel12上的线路协议，状态更改为down

*Jan 24 08:33:14.459: %LINEPROTO-5-UPDOWN：接口Tunnel11上的线路协议，状态更改为down

*Jan 24 08:33:15.275: %LINEPROTO-5-UPDOWN：接口Tunnel11上的线路协议，状态更改为up

原因

如果客户端的端口出现抖动，这似乎是一个不稳定的客户端问题。

在Azure中进行更改后，抖动似乎暂时保持稳定。

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）。