

由于ESN协商导致与Versa网络路由器的安全访问IPsec隧道连接问题

目录

问题

在使用Versa-Network Router作为边缘设备的分支机构部署Cisco Secure Access期间，尽管两个IPsec隧道都显示为运行正常，但仍遇到连接问题。 T

具体症状包括：

- 分支机构无法连接到思科安全访问
- 通过静态路由的Internet访问不起作用
- 观察到的单向加密流量（仅出站到安全访问）
- 路由器统计信息，显示正在发送的出站数据包，但没有收到进站数据包
- 在SD-WAN路由器和安全访问之间双向运行的失效对等体检测
- 出站流量正确匹配的安全参数索引(SPI)值
- 隧道抖动（重置）未解决连接问题
- 数据包捕获和屏幕截图证实了进站流量不足
- 将隧道密码从CBC更改为GCM未解决此问题

调查发现，由于校验和错误，流量无法在Cisco端解密，这些校验和错误追溯到Versa路由器协商ESN（扩展序列号）功能。

环境

- 思科安全访问部署

- Versa-Networks路由器作为边缘设备
- IP身份隧道配置
- 使用CBC和GCM密码尝试的IPsec隧道配置

分辨率

解决方法是在Versa路由器上禁用扩展序列号(ESN)协商，以防止校验和错误，这些错误导致思科安全接入头端的解密失败。

解决步骤

步骤 1：确定根本原因

调查确定Versa路由器正在协商ESN（扩展序列号），从而导致思科安全访问前端接收校验和错误，并且无法解密ESN构建的数据包。

步骤 2：在Versa路由器上禁用ESN

联系Versa Networks支持或路由器管理员，禁用Versa路由器配置上的ESN检查和协商。这解决了导致ESN协商不当的已知Versa漏洞。

步骤 3：检验连通性

禁用ESN协商后，确认已建立双向流量并恢复从分支机构到安全访问和Internet的完全连接。

步骤 4：监控流量

验证路由器上的入站和出站数据包统计信息显示两个方向上的正确流量，确认单向流量问题成功解决。

原因

根本原因确定为已知的Versa网络Bug(Versa支持Bug ID:122437 - ESN不得由VOS协商，其中Versa路由器在IPsec隧道建立期间错误地协商扩展序列号(ESN)功能。此ESN协商会导致Cisco安全访问前端接收带有校验和错误的数据包，从而阻止正确解密并导致单向流量。Versa路由器成功发送出站数据包，但由于ESN相关的解密失败，返回流量无法正确处理。

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）。