安全访问分割隧道配置挑战

目录

问题

为拆分隧道流量配置思科安全访问(TIA)功能时，在配置过程中遇到多种复杂情况，导致无法正确部署：

- 流量识别挑战：为分割隧道配置TIA时，需要从互联网安全检测中排除所有VPN流量。确定所需的流量非常困难，一些重定向URL的跟踪和分类尤其困难。
- 身份验证流量限制：某些拆分隧道方案要求从代理中排除身份验证流量。但是，根据现有策略，与身份验证相关的流量不能从代理绕过，从而导致策略冲突。
- VPN断开连接的安全风险：当VPN断开连接时，拆分隧道流量会暴露于开放的互联网，从而导致配置过程中需要考虑的其他安全风险。

在需要进一步分析和解决的过程中，还发现了其他配置问题。

环境

- 产品系列：SEACCS（安全访问）
- 技术：具有分割隧道功能的思科安全访问(TIA)
- 配置:使用现有策略的拆分隧道流量方案
- 身份验证:基于代理的身份验证流量处理
- 网络安全:VPN流量的互联网安全检查要求

分辨率

根据思科安全访问分割隧道确定的配置挑战，我们提交了一个全面的功能请求，以解决确定的限制和策略冲突。

功能请求提交

已打开功能请求(CSE-I-5636)，并提交相关工程团队进行审核，以解决这些配置挑战：

- 增强的流量识别功能，可将VPN流量排除在互联网安全检测之外
- 改进了难以跟踪和分类的重定向URL的处理
- 解决现有策略的身份验证流量绕行限制
- 在VPN断开期间减少分割隧道流量暴露的安全风险

原因

配置挑战源于思科安全访问(TIA)拆分隧道实施中的当前限制，这些限制无法充分解决复杂的企业部署方案。具体而言，系统缺乏对流量识别和分类的足够精细控制，策略到位时存在绕过身份验证流量的限制，且在VPN连接中断时没有为分离隧道流量提供足够的安全保障。

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）。