配置安全访问流量引导和同步客户端

目录

问题

查看思科安全访问流量控制配置时，VPN配置文件设置和XML文件不显示为流量控制配置的目标IP地址或域。这会造成有关安全访问客户端如何确定流量目标以进行指导决策，以及在管理门户中进行的配置更改如何同步到客户端的混乱。具体而言，管理员注意到，通过VPN配置文件管理接口配置流量控制设置时，对应的VPN配置文件XML文件不包含可以接受流量控制控制的目标地址或域的可见条目。

环境

- 思科安全访问解决方案
- 启用了流量引导的VPN配置文件配置
- 安全访问客户端部署

分辨率

思科安全访问中的流量引导通过动态规则交付机制运行，而不是VPN配置文件XML中的静态条目。接下来的部分将介绍此过程的工作原理以及如何验证配置。

流量控制规则交付

流量控制规则未存储在管理员可以查看的VPN配置文件XML文件中。相反，这些规则在VPN连接建立期间从安全访问前端动态推送到客户端。

该过程的工作原理如下：

1. — 建立VPN连接后，安全访问前端会将当前流量引导（拆分隧道）规则推送到连接的客户端。

2. — 客户端接收这些规则并将它们直接写入本地客户端路由表。

3. — 流量引导决策基于客户端路由表中的条目作出，而不是从VPN配置文件XML中可见的信息作出。

配置更改同步

对管理门户中的流量控制设置所做的更改遵循特定的同步模式：

- 在管理门户中进行的配置更改在活动VPN会话期间不会生效。
- 在下一次VPN连接建立时应用新的流量引导规则。
- 要在更改流量控制配置后验证行为，必须断开并重新连接VPN连接。

验证步骤

要验证流量控制配置更改，请执行以下操作：

1. — 对安全访问管理门户中的流量引导设置进行所需的更改。

2. — 断开客户端上的现有VPN连接。

3. — 重新连接VPN以接收更新的流量引导规则。

4. — 检查客户端路由表，确认新规则已应用。

原因

VPN配置文件XML中明显没有流量引导目标，这是设计原因。思科安全访问使用动态规则交付系统，在该系统中，流量引导规则在连接时推送到客户端，并通过路由表条目实施，而不是作为可见的配置元素存储在配置文件XML中。此架构支持实时策略更新和集中控制，同时保持安全性和性能。

相关内容

- ASA拆分隧道配置指南
- 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）。