安全客户端TND手动VPN连接行为和URL阻止注意事项

目录

问题

当使用具有受信任网络检测(TND)功能的VPN配置文件时，如果用户使用Cisco安全客户端手动发起连接，则位于受信任网络内的终端仍可以成功建立VPN连接。

尽管将TND配置设置为在受信任网络上检测到终端时断开VPN会话，仍会发生此行为。

确定的具体关注问题包括：

- 通过标准TND配置无法控制或阻止来自受信任网络终端的手动VPN连接
- 不确定思科安全访问(CSA)设置能否阻止来自受信任网络终端的手动VPN连接
- 有关VPN配置文件连接URL(xxxx.vpn.sse.cisco.com)的稳定性以及它是否定期更改的问题，这可能会影响基于防火墙的阻止策略

环境

- 思科安全访问(CSA)部署
- 配置VPN配置文件的Cisco安全客户端
- 已启用受信任网络检测(TND)功能
- 配置为断开的TND受信任网络设置
- 位于已配置受信任网络内的终端
- 用于网络访问控制的防火墙基础设施

分辨率

了解使用手动VPN连接的TND行为

观察到的行为与记录的思科安全客户端功能一致。根据思科文档，TND不会断开或阻止用户在受信任网络上手动启动的VPN会话。这是预期行为，无论TND配置设置如何。

主要技术事实如下：

- TND自动断开功能仅适用于自动建立的VPN连接。
- 用户发起的手动VPN连接会绕过TND断开行为。
- 不存在CSA配置设置以阻止来自受信任网络终端的手动VPN连接。

运营缓解战略

控制来自受信任网络端点的手动VPN连接的主要方法是通过网络级控制：

步骤 1：实施防火墙URL阻止：配置受信任网络防火墙以阻止对VPN配置文件连接URL(xxxx.vpn.sse.cisco.com)的访问。 这会阻止受信任网络上的终端访问VPN服务终端。

步骤 2：验证URL稳定性：VPN配置文件URL标识符（xxxx部分）是租户特定的，预计不会定期更改。这为防火墙阻止规则提供了稳定的目标。

验证和测试

测试确认，在受信任网络防火墙上阻止VPN配置文件连接URL成功阻止了终端建立VPN连接，即使用户尝试通过Cisco安全客户端进行手动连接也是如此。

原因

此行为是思科安全客户端TND实施中的设计行为。TND功能专门设计用于根据网络信任状态管理自动VPN连接，但它不会有意干扰用户发起的手动VPN连接。此设计允许用户在必要时覆盖自动行为，同时仍为典型使用案例提供自动网络检测和连接管理。

相关内容

- 思科安全客户端管理员指南 — TND配置
- 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）。