安全客户端计算机隧道身份验证弹出窗口导致不可信网络上的断开连接

目录

问题

连接计算机隧道时，Cisco安全客户端(AnyConnect)反复提示输入用户名和密码，尤其是当用户从不受信任的网络连接时。身份验证弹出窗口会中断计算机隧道连接并导致断开，从而影响用户保持稳定远程访问的能力。尽管正确建立并验证机器隧道，但还是会发生此问题，因为弹出窗口出现意外，并且中断了VPN会话连续性。

环境

- 带机器隧道配置的Cisco安全客户端(AnyConnect)
- 启用了信任网络检测(TND)功能的远程访问VPN配置文件
- 连接到计算机隧道的用户计算机
- 用于客户端配置文件分发的组策略对象(GPO)
- 使用TND设置配置的用户隧道和机器隧道配置文件

分辨率

通过修改机器隧道和用户隧道配置文件的信任网络检测(TND)配置设置，解决了此问题。解决方案包括配置TND操作行为以防止在不受信任的网络上出现不必要的身份验证提示。

步骤 1：配置不受信任网络的TND设置

将Trust Network Detection（信任网络检测）操作设置为Do nothing（对机器隧道配置文件和用户隧道配置文件上的不受信任网络不执行任何操作）。此配置可防止客户端在连接到不受信任的网络时提示输入其他凭证。

步骤 2：配置受信任网络的TND设置

对于受信任网络，将Trust Network Detection操作设置为Disconnect，以维护已知安全网络环境的预期安全行为。

步骤 3：部署配置更改

通过组策略对象(GPO)推送部署更新的TND设置，以将配置更改分发到所有受影响的客户端计算机。

步骤 4：重新启动客户端计算机

在配置文件更新后重新启动客户机，以确保新的TND设置正确生效。

步骤 5：验证测试

测试跨多个不受信任网络的机器隧道连接，以验证：

- 不再显示身份验证弹出窗口
- 机器隧道始终保持连接
- 无凭证提示中断VPN会话
- 用户可以保持稳定的远程访问，而无需断开连接

实施这些更改后，用户确认成功解决问题，多个用户测试在各种网络条件下验证稳定的VPN会话连续性。

原因

根本原因是思科安全客户端配置文件上的信任网络检测(TND)设置配置错误。TND功能在用户从不受信任的网络连接时触发身份验证提示，即使机器隧道已正确进行身份验证并建立。用户隧道和机器隧道配置文件的TND操作未针对网络环境进行优化配置，导致客户端不必要地请求其他凭证，并中断机器隧道连接。

相关内容

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）。