由于VPN配置文件名称长度限制，安全访问VPN管理员重置断开连接

目录

问题

远程访问VPN用户在活动会话期间，思科安全访问(CSA)会间歇性断开连接。思科安全访问(CSA)日志将这些断开事件记录为管理员重置，尽管当时未发生计划维护活动。断开连接会在正常业务操作期间影响远程访问用户，在用户主动连接到VPN服务时导致意外的会话终止。

断开事件在远程访问日志中显示为管理员重置条目，通常表示管理干预或系统启动的会话终止。但是，在报告的时限内，未对系统执行任何管理操作。

环境

- 思科安全访问(CSA) — 远程访问VPN服务
- 名称超过46个字符的VPN配置文件配置

分辨率

解决方法涉及实施解决导致管理员重置事件的VPN配置文件名称长度限制的解决方法：

即时解决方法

步骤 1：识别名称超过46个字符的VPN配置文件

检查Cisco Secure Access控制面板中的所有现有VPN配置文件配置，并确定名称超过46个字符的所有配置文件。

步骤 2：重命名VPN配置文件以符合字符限制

重命名所有超过46个字符的VPN配置文件，以确保其长度不超过46个字符。这可以通过思科安全访问管理界面完成。

步骤 3：监控断开连接事件

实施VPN配置文件名称更改后，监控远程访问日志以验证在正常操作期间不再发生管理员重置事件。

长期解决方案

正在开发永久修复程序，以解决GUI限制（允许VPN配置文件名称超过后端处理限制）。此修复在用户界面级别实施46个字符的限制，阻止使用导致后端处理问题的名称创建VPN配置文件。

开发团队正致力于在GUI中实施适当的验证，以在创建和修改期间限制VPN配置文件名称长度，从而防止在未来的配置中出现此问题。

其他注意事项

在某些情况下，客户端设备上的Wi-Fi适配器电源管理设置可能会导致连接问题。如果在实施VPN配置文件名称长度修复后断开仍然存在，请验证受影响的客户端设备上是否禁用了Wi-Fi适配器节能功能，因为这些设置可能导致重新连接事件，这些事件在日志中显示为管理员重置条目。

原因

管理员重置事件的根本原因是思科安全访问中的后端处理限制，其中VPN配置文件名称超过46个字符会导致会话管理期间出现系统错误。当后端系统遇到名称长于此限制的VPN配置文件时，会触发Administrator Reset以终止受影响的会话作为保护措施。

发生此问题的原因是GUI界面允许用户创建长度超过46个字符的VPN配置文件名称，但后端处理系统具有严格的46个字符限制。后端处理大字符串长度时，会导致记录Administrator Reset事件并强制断开关联VPN会话的连接。

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）。