企业防火墙后出现间歇性安全访问断开与IdleTimeout错误

目录

- 问题
- 环境
- 分辨率
  - 步骤 1：实施MX TTL缓冲区配置
  - 步骤 2：配置所需的域排除
  - 步骤 3：检验端口和协议允许情况
  - 步骤 4：监控和验证解决方案
- 原因
- 相关内容

问题

当终端连接到企业网络时，思科安全访问客户端会经历间歇性断开和立即重新连接。断开连接是随机发生的，客户端会在大约5秒后自动重新连接。当互联网流量通过零信任访问(ZTA)从位于Cisco FirePower和Meraki MX设备后的终端代理到安全访问时，会观察到此行为。

Windows事件日志捕获在这些断开事件期间的特定“idleTimeout”错误。当用户从家庭Internet连接进行连接时，不会出现断开模式，这表示该问题与公司网络基础设施特别相关。

该症状导致业务中断，从而为在公司网络环境中运营的用户保护远程访问连接，而远程用户仍不受此连接问题的影响。

环境

- 思科安全访问 — 优势部署
- 思科安全互联网接入(SIA)客户端软件
- 采用Cisco FirePower安全设备的企业网络基础设施
- 网络路径中的Meraki MX安全设备
- 将互联网流量代理到安全访问的零信任访问(ZTA)配置
- 具有事件日志记录功能的Windows终端
- 混合连接方案：公司网络（受影响）和家庭互联网连接（未受影响）

分辨率

解决方案涉及在Meraki MX设备上实施配置更改，并确保安全访问集成的适当域排除和端口许可。

步骤 1：实施MX TTL缓冲区配置

在Meraki MX设备上配置MX TTL缓冲区，以解决导致间歇性断开问题的DNS TTL缓存行为。此配置更改解决了DNS解析缓存和安全访问客户端连接期望之间的时间冲突。

步骤 2：配置所需的域排除

确保这些域被正确排除在拦截之外，并添加到Cisco FirePower和Meraki MX设备上的非解密列表：

- ztna.sse.cisco.com
- zpc.sse.cisco.com
- 策略配置中确定的其他安全访问服务域

步骤 3：检验端口和协议允许情况

配置企业防火墙基础设施，以允许通过FirePower和Meraki MX设备使用所需的安全访问端口和协议。确保正确处理流向安全访问服务端点的端口443的流量，而不会受到可能导致超时条件的安全检查的干扰。

步骤 4：监控和验证解决方案

实施MX TTL缓冲区配置后，请连续几天监控安全访问客户端的行为，以确认间歇性断开和重新连接模式已停止。

原因

间歇性断开是由企业网络基础设施和安全访问服务期望之间的DNS TTL（生存时间）缓存行为冲突引起的。思科工程分析显示，DNS TTL值会因解析程序缓存行为而变化，而由于Secure Access服务架构中的负载均衡机制，交替IP地址是预期行为。

当企业网络设备（Cisco FirePower和Meraki MX）处理安全访问终端的DNS响应时，缓存和TTL处理会生成时间不匹配，从而导致“idleTimeout”情况。此计时冲突导致安全访问客户端将连接解释为空闲并启动断开连接/重新连接循环。

此问题特定于企业网络环境，因为家庭互联网连接通常不会实施同一级别的DNS缓存和流量检查，这可能会干扰Secure Access客户端连接状态管理。

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）。