基于客户端的安全客户端ZTNA流量引导问题

目录

问题

当通过FQDN或直接IP地址访问时，基于客户端的零信任网络访问(ZTNA)无法提供对内部应用的访问，而通过VPN连接仍可访问相同的应用。

观察到的具体症状包括：

- 当VPN断开连接时，安全客户端ZTNA无法通过FQDN或直接IP访问内部应用。
- 基于浏览器的ZTNA访问可针对相同应用正常工作。
- 当VPN关闭时，活动日志中不会显示ZTNA事件，这表示客户端流量未通过ZTNA路径路由。
- 私有应用定义已经过验证，可以将VPN可路由资源与正确的IP/端口/FQDN配置相匹配。
- 已确认ZTNA策略与测试用户和组分配匹配。

由于基于浏览器的ZTNA验证后端发布和执行是否正常运行，因此该问题专门针对安全客户端ZTNA流量引导或实施机制进行隔离。

环境

- 技术：安全访问 — 零信任网络访问(ZTNA)
- 组件:基于客户端的ZTNA、状态、注册、私有资源访问
- 具有共存VPN配置文件的安全客户端
- 可通过FQDN和直接IP寻址访问私有应用
- 基于浏览器的ZTNA功能确认工作正常
- 在最特定匹配实施模式下配置的策略实施

分辨率

解决方案涉及对ZTA配置文件的配置调整和策略验证。下面几节中介绍的步骤用于恢复基于客户端的ZTNA功能。

步骤 1：将私有资源添加到ZTA配置文件

私有资源已添加到ZTA配置文件配置中。更改后，阻止的事件开始显示在活动日志和屏幕截图中，表明客户端流量现在正通过ZTNA路径正确路由。

步骤 2：策略验证和测试

添加了一个临时“permit any”规则以验证流量。当此规则处于活动状态时，基于客户端的ZTNA访问正常工作，确认流量引导机制正在工作，但策略实施需要调整。

步骤 3：策略细化

临时的permit-any规则已删除，并且特定访问策略已验证。已确认使用平台的最特定匹配实施模式在名为Private Resources_Cyril的访问策略下可以访问私有资源。

步骤 4：配置验证

用户确认基于客户端的ZTNA访问在配置更改后开始一致运行。无需进行其他策略修改或系统更改即可解决问题。

原因

根本原因是ZTA配置文件中的私有资源配置不完整。如果没有在ZTA配置文件中定义正确的私有资源，客户端流量将不会通过ZTNA实施路径引导，导致其回退到本地路由机制。这导致流量完全绕过ZTNA策略，这解释了当VPN断开连接时，活动日志中为什么没有出现ZTNA事件。

此问题特定于基于客户端的ZTNA流量引导配置，而基于浏览器的ZTNA继续运行，因为它使用的是正确配置的不同流量处理机制。

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）。