

基于ZTA浏览器的私有资源TLS握手失败

目录

问题

用户无法通过Cisco Secure Access访问基于浏览器的私有资源。

尝试连接时，会出现以下症状：

- TCP三次握手成功完成，但TLS协商在客户端Hello后失败。
- 与公共SSE映射URL(<https://example-orgid.ztna.sse.cisco.io>)的连接到达Cisco身份验证，但返回HTTP 404错误。
- 将FQDN添加到私有资源配置后，流量重定向到身份验证提示，但在身份验证后会生成空白页面。
- HAR文件显示HTTP 200响应，但TLS握手没有完成。
- 阻止原因显示为：“私有访问：已获取的设备状态数据太旧/需要刷新”。

环境

- 思科安全访问(SSE)
- 安全访问组织ID:xxxx
- 基于浏览器的零信任网络访问(ZTNA)
- 专用资源：example.net
- 用于比较的专用工作资源：abc.net
- 通配符证书配置

分辨率

通过将私有资源配置为使用与工作私有资源相同的证书配置来解决问题。

随后将采取以下各节概述的步骤。

步骤 1：分析工作配置

比较故障专用资源(example.net)与工作专用资源(abc.net)，找出配置差异。

使用的工作资源：

- 使用域中的URL选项
- 现有通配符证书/密钥对的引用

步骤 2：数据包捕获分析

使用Wireshark执行数据包捕获分析以确认TLS握手失败：

- 检验TCP三次握手是否成功完成。
- 在客户端Hello后确认TLS协商失败。
- 收集诊断对象：HAR文件、DART捆绑包和数据包捕获。

步骤 3：证书验证

通过RAVPN连接访问应用程序以验证证书演示：

- 确认网站example.net提供通配符证书。
- 记录证书详细信息，以供配置参考。

步骤 4：配置专用资源

应用工作专用资源使用的相同配置方法：

- 配置专用资源以使用Use a URL in your domain选项。
- 参考现有的通配符证书/密钥对。
- 确保已在专用资源字段中正确配置FQDN。

步骤 5：验证

测试基于浏览器的访问以确认配置解决了问题：

- 检验TLS握手成功完成。
- 确认正确的身份验证流程。
- 验证身份验证后的应用程序可访问性。

原因

根本原因是专用资源设置中的配置不匹配。失败的私有资源未配置为正确引用目标应用程序提供的通配符证书。TLS握手失败，因为私有资源配置与应用服务器使用的证书配置不一致。通过将私有资源配置为使用Use a URL in your domain选项并引用现有的通配符证书/密钥对（匹配工作配置），TLS协商可以成功完成。

相关内容

- [思科安全访问参考指南](#)
- [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）。