安全访问ZTNA配置与SSL解密和网络隧道同步错误

目录

问题

Cisco安全客户端零信任访问(ZTA)已成功注册，但在配置同步期间失败，HTTP 502响应和“BadResponse”服务器连接状态。来自Windows 11终端的DART日志显示注册成功，但配置同步重复失败。仅当终端使用带有Meraki AutoVPN隧道的安全访问/Umbrella代理连接到企业网络路径，而同一终端在没有代理或隧道基础设施的家庭网络上成功完成配置同步时，才会出现此问题。

环境

- 思科安全客户端ZTA版本5.1.16.4434
- Windows 11企业端点
- 集成AutoVPN的Meraki MX设备
- 使用网络隧道网关(NTG)的安全访问(SSE)
- Umbrella DNS和安全访问网络安全
- 在企业网络路径上启用SSL解密和HTTPS检查
- 系统提供的不解密列表(DND)最初未配置

分辨率

当使用具有安全访问的网络隧道时，通过为ZTA相关域实施适当的SSL解密旁路来解决配置同步故障。

步骤 1：确定SSL解密的影响

通过查看Secure Access中的Activity Search日志，了解与ZTA域相关的解密事件，验证SSL解密导致配置同步失败。

步骤 2：配置系统提供的DND列表

当使用具有安全访问的网络隧道网关(NTG)时，必须启用系统提供的DND，以正确绕过来自SSL检查的ZTA相关流量。

导航到Secure Access Dashboard > Secure > Do Not Decrypt Lists并修改System Provided Do Not Decrypt List。

步骤 3：为ZTA域创建安全配置文件

使用系统提供的DND列表将所需的ZTA相关域添加到新的安全配置文件：

- zpc.sse.cisco.com
- *.zpc.sse.cisco.com
- ztna.sse.cisco.com
- acme.sse.cisco.com
- devices.api.umbrella.com

步骤 4：将安全配置文件应用于测试规则

将包含ZTA域的新创建安全配置文件分配到测试规则以验证配置。

步骤 5：验证配置同步

从企业网络测试ZTA注册和配置同步。现在可以成功完成同步，而不出现HTTP 502错误。

步骤 6：与Meraki团队协调

要获得全面的覆盖范围，请与Meraki支持协调以验证可通过安全访问检查绕过的官方ZTA相关URL和域。请参阅以下Meraki文档：

- 云连接的上游防火墙规则
- Meraki控制面板URL更新 — PCI合规性

原因

配置同步失败是由企业网络上零信任访问流量的SSL解密和代理引起的。当网络隧道网关(NTG)与安全访问一起使用时，必须使用System Provided Do Not Decrypt List(DND)绕过ZTA相关的域。 如果没有此旁路配置，SSL检查会修改证书链并干扰ZTA控制平面通信，导致客户端在配置同步尝试期间收到HTTP 502响应。

相关内容

- 解决安全访问解密和SSL问题
- 安全访问零信任基于客户端的注册服务
- 安全访问的ZTA域要求
- 解决安全访问错误注册问题
- 安全客户端配置同步错误故障排除
- 收集详细的ZTNA日志以进行故障排除
- 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）。