

设备注册期间安全客户端Umbrella模块 SSL/TLS信任故障

目录

问题

在使用Umbrella模块部署思科安全客户端期间，设备停止与控制面板同步，并报告为“非活动”。受影响的客户端在尝试注册到devices.api.sse.cisco.com时遇到SSL/TLS信任失败，导致设备注册和保护覆盖无法成功。

UI显示Umbrella处于非活动状态，并显示以下状态消息：

- Umbrella处于非活动状态。
- 您当前不受安全Web网关保护。
- 安全Web网关未获得许可/已禁用。

诊断结果显示注册期间出现一致的SSL/TLS信任故障，安全客户端日志中会显示以下错误消息：

```
[ERROR] < 10> Device Registration: Registration failed against https://devices.api.sse.cisco.com/deploy
```

环境

- 在2,000多个端点部署带Umbrella模块的思科安全客户端
- 具有路由策略的SD-WAN基础设施
- 旧式伞形隧道到位
- 根据思科文档允许所有所需目标的网络配置

- 边界上的思科目标没有活动的SSL解密

分辨率

解决方案涉及识别和纠正导致设备注册流量通过传统Umbrella隧道错误定向的路由配置问题。

根本原因识别

对数据包捕获数据的分析显示，为API连接提供的TLS证书是Cisco Umbrella证书，而不是预期的Cisco Secure Access/Let's Encrypt证书。确定devices.api.sse.cisco.com的IP地址。

进一步调查发现与146.112.0.0/16子网匹配的SD-WAN路由策略，导致指向devices.api.sse.cisco.com的流量被路由到传统Umbrella隧道而不是预期目的地。

配置更改

为了解决此问题，采取了以下步骤：

- 步骤 1：删除有问题的静态路由。从SD-WAN配置中删除了指向146.112.0.0/16到传统Umbrella隧道的静态路由。
- 步骤 2：验证连接。删除静态路由后，对受影响的客户端进行了测试，以确保它们可以成功连接并注册到devices.api.sse.cisco.com。

确认

devices.api.sse.cisco.com的预期证书链应如下所示：

```
openssl s_client -connect devices.api.sse.cisco.com:443
CONNECTED(00000003)
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
```

```
depth=1 C = US, O = Let's Encrypt, CN = R13
verify return:1
depth=0 CN = api.sse.cisco.com
verify return:1
---
Certificate chain
 0 s:CN = api.sse.cisco.com
  i:C = US, O = Let's Encrypt, CN = R13
  a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
  v:NotBefore: Mar  5 14:13:56 2026 GMT; NotAfter: Jun  3 14:13:55 2026 GMT
 1 s:C = US, O = Let's Encrypt, CN = R13
  i:C = US, O = Internet Security Research Group, CN = ISRG Root X1
  a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
  v:NotBefore: Mar 13 00:00:00 2024 GMT; NotAfter: Mar 12 23:59:59 2027 GMT
```

实施配置更改后，受影响的客户端成功连接和注册，部署成功完成。

原因

根本原因是与146.112.0.0/16子网匹配的SD-WAN路由策略，导致通过传统Umbrella隧道错误路由发往devices.api.sse.cisco.com(146.112.59.104)的设备注册流量。这会导致显示错误的TLS证书（Cisco Umbrella证书而不是预期的Cisco Secure Access/Let's Encrypt证书），从而导致设备注册过程中发生SSL/TLS信任故障。

相关内容

- [Cisco安全客户端网络要求文档](#)
- [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）。