解决安全Web网关SWG网站访问问题

目录

简介

本文档介绍通过基于云的代理（安全Web网关/SWG）路由但不使用直接互联网接入(DIA)时，诊断网站访问问题的结构化方法。

- 范围：适用于Cisco Umbrella SIG和思科安全访问。

前提条件和重要警告

- 检验是否对可重现的问题执行了所有故障排除。
- 收集HAR（HTTP存档）文件和同步数据包捕获(PCAP)以提供准确的数据进行分析。
- 对代理策略的更改（例如，绕过解密或检查）可能会影响安全状态；仅适用于故障排除或按照建议应用。

确定代理级错误

常见的代理干扰指示器包括：

- 502错误网关
- 515上游证书不受信任
- 517上游证书已吊销
- 403禁止
- 已撤销的证书
- 密码套件不匹配
- 网站连接超时

故障排除方法

步骤 1：确认流量通过代理

- 数据收集:当问题发生时，生成HAR文件和PCAP。
- 标题分析：检查HTTP响应中的Via报头。如果存在`s_proxy`（Nginx代理）或`m_proxy`（模块化代理服务/MPS），则确认流量已代理。
- TCP数据流：在Wireshark中，遵循TCP数据流确保连接到代理的IP，而不是目标IP。

步骤 2：验证TLS解密状态

- 浏览器检查：点击浏览器地址栏中的锁定图标。如果Cisco安全访问根证书出现在证书链中，则HTTPS检查处于活动状态。
- 验证：交叉引用HAR/PCAP文件中的Via报头。
- OpenSSL命令：检查证书链：
  `openssl s_client -connect www.example.com:443 -showcerts`
  此命令检查服务器提供的证书链。从遍历代理的计算机运行它以进行直接验证。

步骤 3：隔离和消除过程

1. 阶段A — 测试HTTPS检查（Nginx层）：
   - 将有问题的域添加到SWG“不解密”列表。
   - 保持文件检测处于启用状态。
   - 如果问题得到解决：根本原因可能是Nginx SSL/TLS检查。分析PCAP是否存在密码不匹配或SNI问题。使用带和不带代理的`curl`比较行为。
   - 如果问题仍然存在：进入B阶段。
2. 阶段B — 测试文件检查（扫描层）：
   - 禁用特定流量的文件检查。
   - 如果问题得到解决：根本原因在于文件扫描引擎。检查PCAP和HAR，在实验室中复制，并确定特定文件或扫描签名是否触发了问题。
   - 如果问题未解决：请联系支持部门，提供全面的日志和调查结果。

常见问题和错误代码

515上游证书不受信任

当SWG代理无法验证目标服务器的证书时，会发生此错误。原因包括证书链已过期、自签名或不完整。

- 上的HTTPS检查+文件检查在：网站工作；无证书错误。
- 打开HTTPS检查+关闭文件检查：发现515错误，匹配用户报告。
- HTTPS检测关闭+文件检测关闭（不解密列表中的域）：未发现问题。

技术详细信息：如果上游服务器依靠授权信息访问(AIA)获取缺少的中间证书，Nginx代理可能会失败，因为Nginx对AIA的处理不如文件扫描代理服务顺利。TLS握手期间的SNI和SAN不匹配也会触发故障。

517上游证书已吊销

517错误表示SWG代理的CRL或OCSP检查发现上游服务器的证书已吊销。

- 故障排除：使用SSL Labs或OpenSSL等外部工具确认撤销状态。
- 文档：
  - 思科故障排除错误517 — 已撤销上游证书
  - 了解常见证书和协议错误

证书错误处理选项

Cisco Secure Access将引入称为“证书错误处理选项”的新功能，可在不完全禁用解密的情况下进行精细错误旁路。可以使用此功能而不是广泛的“不解密”列表来管理由于检查而触发证书错误的域。此功能目前在Umbrella SIG中存在。CSA的功能请求详细信息。

502错误网关

502错误表明SWG代理在充当中间服务器时收到来自上游服务器的无效响应。

— 下游：客户端到SWG代理
— 上游：SWG代理到目标服务器

由于协议错误、TCP重置或报头格式错误，该错误始终出现在上游连接中。

常见502原因

- 不支持的SWG密码套件

- 客户端证书身份验证请求
- SWG代理添加的报头

不支持的密码套件

原因：服务器需要SWG不支持的密码（例如，TLS_CHACHA20_POLY1305_SHA256）。
分辨率：将该域添加到Selective Decryption列表。

测试命令：
使用代理：

```
curl -x proxy.sig.umbrella.com:80 -v xyz.com:80
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vvv -k "https://www.cnn.com" >>空
```

无代理：

```
curl -v www.xyz.com:80
```

Mac/Linux:

```
curl -vvv -o /dev/null -k -L www.cnn.com
```

Windows 窗口版本:

```
curl -vv -o null -k -L www.cnn.com
```

客户端证书身份验证请求

原因：上游服务器需要客户端证书，SWG不支持该证书。
分辨率：使用外部域管理列表(Umbrella SIG)或绕过安全代理（思科安全访问）从代理绕过域。 仅绕过HTTPS检查是不够的。

由代理添加的信头

原因：启用HTTPS检查时，某些服务器会拒绝带有SWG添加的X-Forwarded-For(XFF)标头的请求。
分辨率：比较具有/不具有HTTPS和文件检查的行为。如果错误仅在存在XFF时发生，则Web服务器可能配置错误。

示例：

```
curl https://www.xyz.com -k –header 'X-Forwarded-For:1.1.1.1' -o /dev/null -w "状态代码：%{http_code}" -s
```

状态代码：502

```
curl https://www.xyz.com -k -o /dev/null -w "状态代码：%{http_code}" -s
```

状态代码：200

添加了XFF报头用于地理定位。如果服务器无法处理它，则会出现502错误。

可能有害的PUA或损坏的文件

如果SWG无法使用文件检查扫描文件（例如，受保护、请求范围或损坏的文件），则会阻止下载并报告 — 已阻止 — 可能有害的应用程序（受保护文件）

- 故障排除：在阻止事件期间捕获HAR。使用“覆盖安全性”作为临时解决方法。如果文件已损坏或恶意，必须在源头对其进行更正。

潜在有害的类别和信誉块

- 使用Talos检查Web信誉(WBRS)。 如果域分类错误，请向Talos提交COG Jira请求以供审核。Talos被归类为安全或有利的，但仍SWG块，因此我们需要从SWG的烧杯服务进行检查。

Akamai拒绝访问SWG出口IP

- SWG使用共享出口IP。如果这些服务被IP信誉服务（例如Brightcloud）列入黑名单，则可能会拒绝对某些站点的访问。

已知问题：Youtube登录僵尸程序和视频不可用

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）。