排除SWG网站访问问题

目录

简介

本文档介绍如何解决与Umbrella安全Web网关(SWG)代理有关的网站访问问题。

背景信息

假设无法通过SWG代理访问网站www.xyz.com，当用户尝试直接访问互联网时（图片中没有Umbrella SWG），该网站运行良好。 让我们回顾当通过SWG无法访问网站时报告的各种症状和不同类型的错误消息。最常见的是502坏网关、502无法中继消息上游错误、撤销上游证书、访问被拒绝403禁止、上游密码不匹配、网站旋转一段时间后超时或类似情况。

由于上游阻止导致“拒绝访问403”错误

Webserver或上游端正在阻止或限制SWG代理出口IP范围。例如，Akamai WAF的块列出了几个SWG出口IP范围。要解决此问题，唯一的选择是联系网站管理员并让他们取消阻止我们的IP范围。在此之前，使用外部域管理列表绕过SWG，进行Anyconnect SWG和PAC文件部署。简而言之，此类问题并非由于代理本身，而是由于代理与Web服务器之间的不兼容性。下面是因出口IP地址块而导致“访问被拒绝403”错误而专门参考知识库的一个链接。

此外，此链接还包括几个可能的原因，说明Akamai为何阻止列出的IP地址。

由于Java问题导致“Access Denied 403”错误

在启用了文件检查设置的情况下，通过SWG MPS代理发送请求时，无法访问网站并抛出“访问被拒

绝或403被禁止 — Umbrella云安全网关错误”。但是，如果文件检查被禁用，网站会成功加载。或者，如果对网站进行旁路解密，则网站加载成功。

问题的根本原因

MPS与Java相关的问题是什么？

有问题的站点或Web服务器在代理尝试连接到服务器后，将有关SNI或SSL警报的TLS警告返回给代理。基本上，这会在客户端hello发送后发生。根据设计，MPS代理（基于Java等）将描述字段中带有“Unrecognized Name”的任何TLS警报视为SNI解析过程中的错误，并终止事务。更多详细信息请参阅此处

请注意，这不是SWG或MPS代理问题。这是与SWG或任何其他代理的不兼容之一，因为服务器端配置错误。浏览器通常忽略此警告，但SWG或其他内容安全过滤器将SSL警告视为致命错误并终止会话，从而导致用户收到403个禁止的错误页面。它还可以报告502 Bad Gateway error，但在大多数示例中，我们看到的是403禁止错误，如下图所示。

15151734443924

由于MPS工作在应用层，因此TLS层根据TLS协议中产生的警报处理事务的方式几乎不受控制。服务器负责确保其TLS终端/证书配置正确。请参阅此链接。

要缩小范围或排除故障，可以从SSL实验轻松指出问题。

15152060146964

如果访问网站时中间没有SWG代理，或者绕过SWG的HTTPS检查，则网站工作正常，因为浏览器忽略SNI无法识别的名称警报，并继续与Web服务器通信。

在撰写本文时，我们向您建议的最佳缓解措施是推荐的解决方法。在不久的将来，通过新的代理架构，我们能够更妥善地处理这些问题。

分辨率

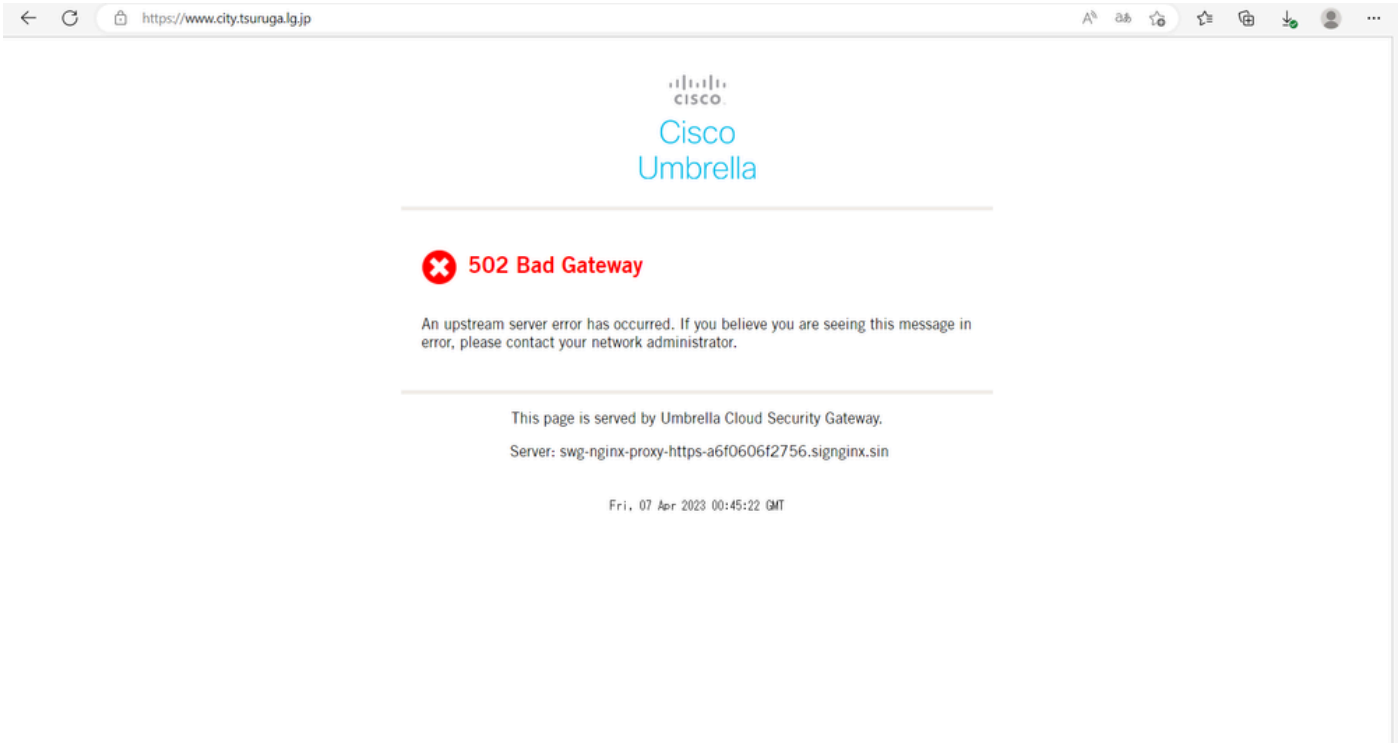
1.禁用受影响域的解密 — 或
2.将域添加到目标列表并关联允许规则（如果信任该站点）

什么是502 Bad Gateway?

502 Bad Gateway Error表示服务器充当网关或代理，并从上游服务器收到无效响应。当用户尝试通过SWG代理访问网站时，会出现两个通信流。

a)客户端 — >代理连接（下行）
b)代理 — >结束Web服务器连接（上行）

502 SWG代理(MPS、Nginx)与终端服务器连接之间出现错误网关错误。



15026978020884

502不良网关的常见因素

1.不支持的SWG密码套件

2.客户端证书身份验证请求

3. SWG代理添加或删除信头

不支持的SWG密码套件

让我们假设Web服务器在TLS协商期间报告不受支持的SWG密码套件。请注意，SWG MPS（模块化代理服务）代理不支持TLS_CHACHA20_POLY1305_SHA256密码套件。请注意，有单独的文章介绍支持SWG的密码套件和TLS。我们可以通过查看在客户端hello和服务器hello中的密码套件交换期间捕获的其他数据包来轻松查明此问题。作为故障排除步骤，使用CURL命令强制使用特定密码

来缩小问题范围并确认其是由密码套件引起的，如示例1和2所示。

Curl命令示例:

<#root>

```
curl -vvv "" --ciphers TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 >> /dev/null
curl -vvv "" --ciphers ECDHE-RSA-AES256-GCM-SHA384 >> /dev/null
```

Testing website With Proxy:

```
 - 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" >> null
```

Testing website without Proxy

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

Mac/Linux:

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

Windows:

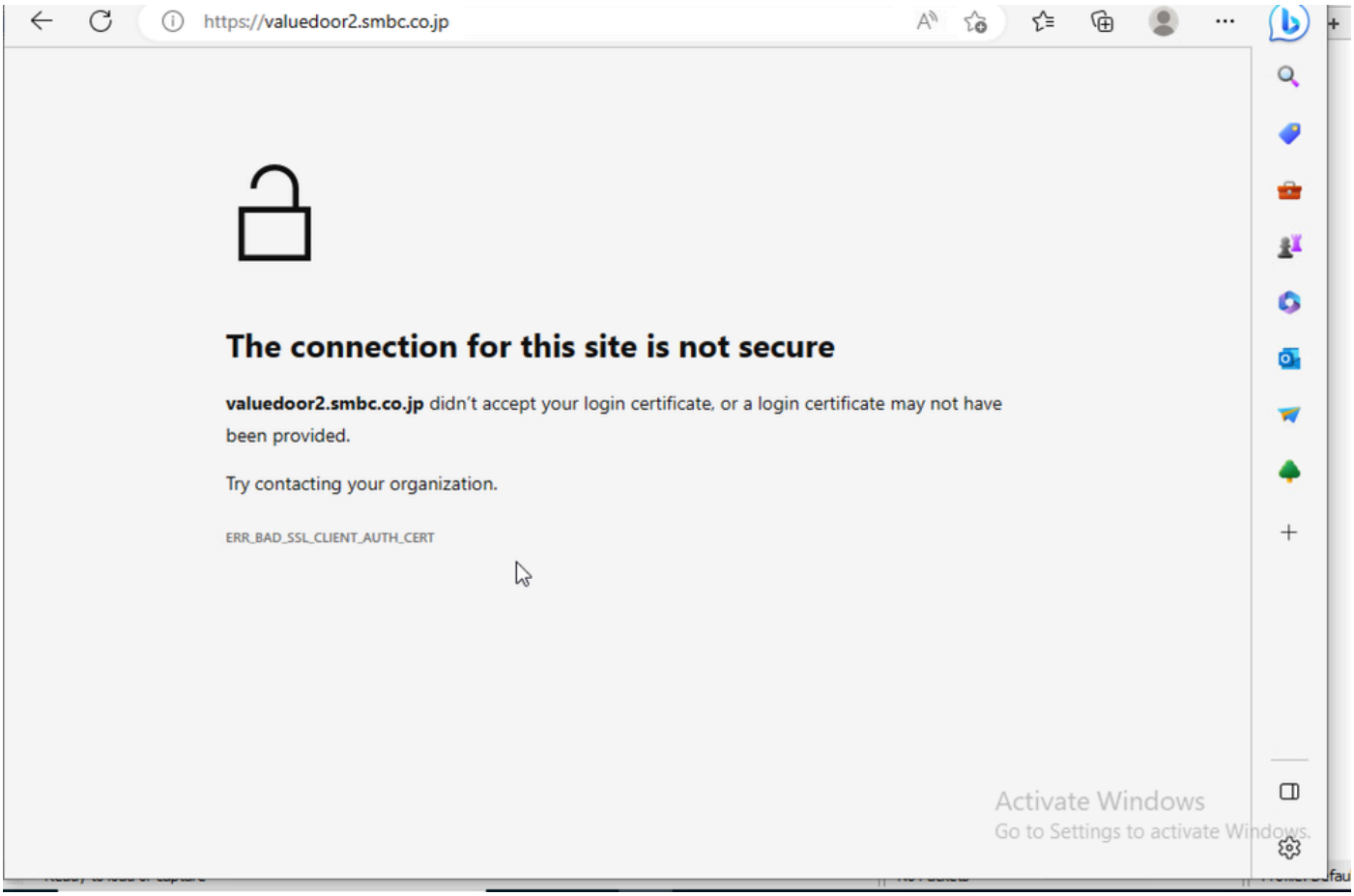
```
 - curl -vvv -o null -k -L www.cnn.com
```

分辨率

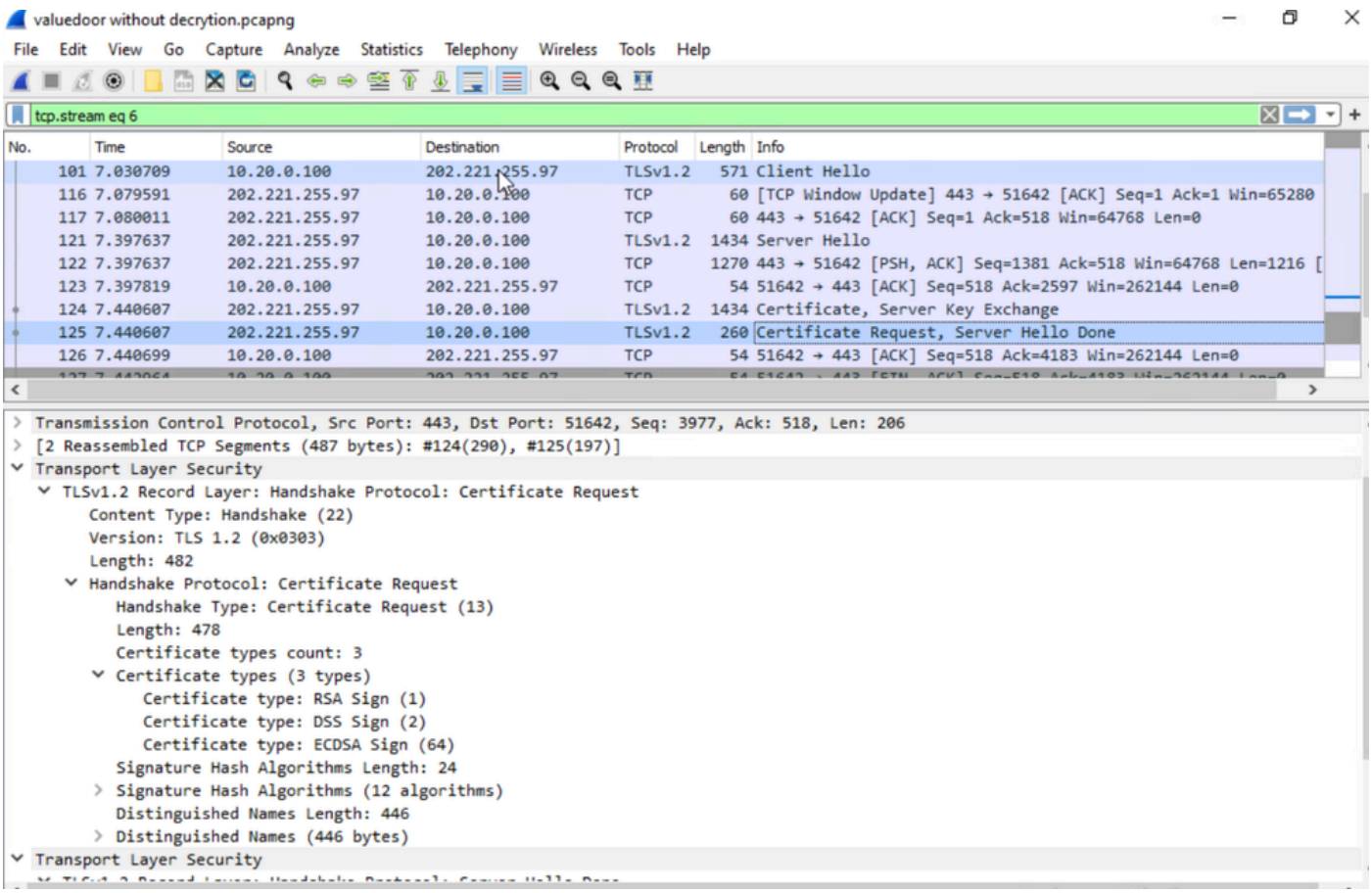
要解决此问题，请使用选择性解密列表跳过对有问题的网站的检查。

客户端证书身份验证请求

在SWG代理和上游之间的TLS握手期间，上游Web服务器需要客户端证书身份验证。由于客户端证书身份验证不受支持，我们需要使用外部域管理列表从代理绕过这些域，仅绕过https检查是不够的。例如：https://valuedoor2.smbc.co.jp。



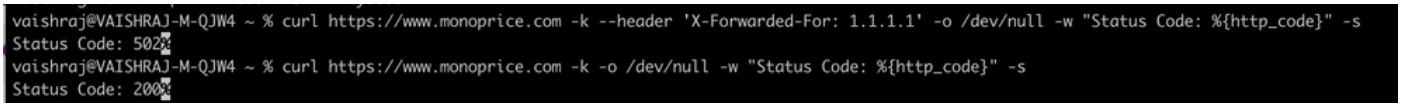
15027182308884



15027192992276

由代理添加的信头

Web服务器报告了502个错误网关错误，原因是SWG代理在启用https检查时添加了X-Forward-For报头(XFF)。我们可以通过首先使用https检查或不使用https检查排除问题，以及使用https检查或不使用文件检查排除MPS代理的文件扫描问题，轻松缩小502个不良网关问题中的大部分。



15123666760340

```
curl https://www.xyz.com -k --header 'X-Forwarded-For: 1.1.1.1' -o /dev/null -w "Status Code: %{http_co
Status Code: 502
curl https://www.xyz.com -k -o /dev/null -w "Status Code: %{http_code}" -s
Status Code: 200
```

启用HTTPS检查时，我们使用XFF报头，以便上游服务器可以根据客户端IP（提供用户的物理位置）提供最佳地理位置内容。

如果未启用HTTPS检查，代理不会添加此报头，因此不会出现502 Bad Gateway错误。这不是SWG代理问题。此错误是由于上游Web服务器配置错误，不支持标准XFF报头。

分辨率

要解决此问题，请使用选择性解密列表绕过特定域的HTTPS检查。

- 517上游证书已吊销
- 证书和TLS协议错误
- 手动选择SWG DC进行内部测试

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）。