排除Umbrella安全Web网关上的516个错误

目录

简介

本文档介绍如何对Umbrella安全Web网关上增加516个错误进行故障排除。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Umbrella安全Web网关(SWG)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

使用HTTPS检查通过Umbrella Secure Web Gateway(SWG)代理浏览的用户可以从2023年10月下半年开始更频繁地收到516 Upstream Certificate CN Mismatch错误页面。

当网站的证书与客户端用于访问网站的域名不匹配时，就会出现516错误页面。

错误页面增加是由于Chrome浏览器对使用HTTP（未加密）方案的URL请求的处理发生变化。Chrome现在尝试首先使用HTTPS（加密）方案加载资源。当配置为HTTPS Inspection时，SWG检查网站的证书，如果证书不可接受，则返回显示错误代码（例如516）的网页。

要解决此问题，客户可以配置其Web策略以绕过请求的HTTPS检查，否则会导致516个错误。

516错误背景

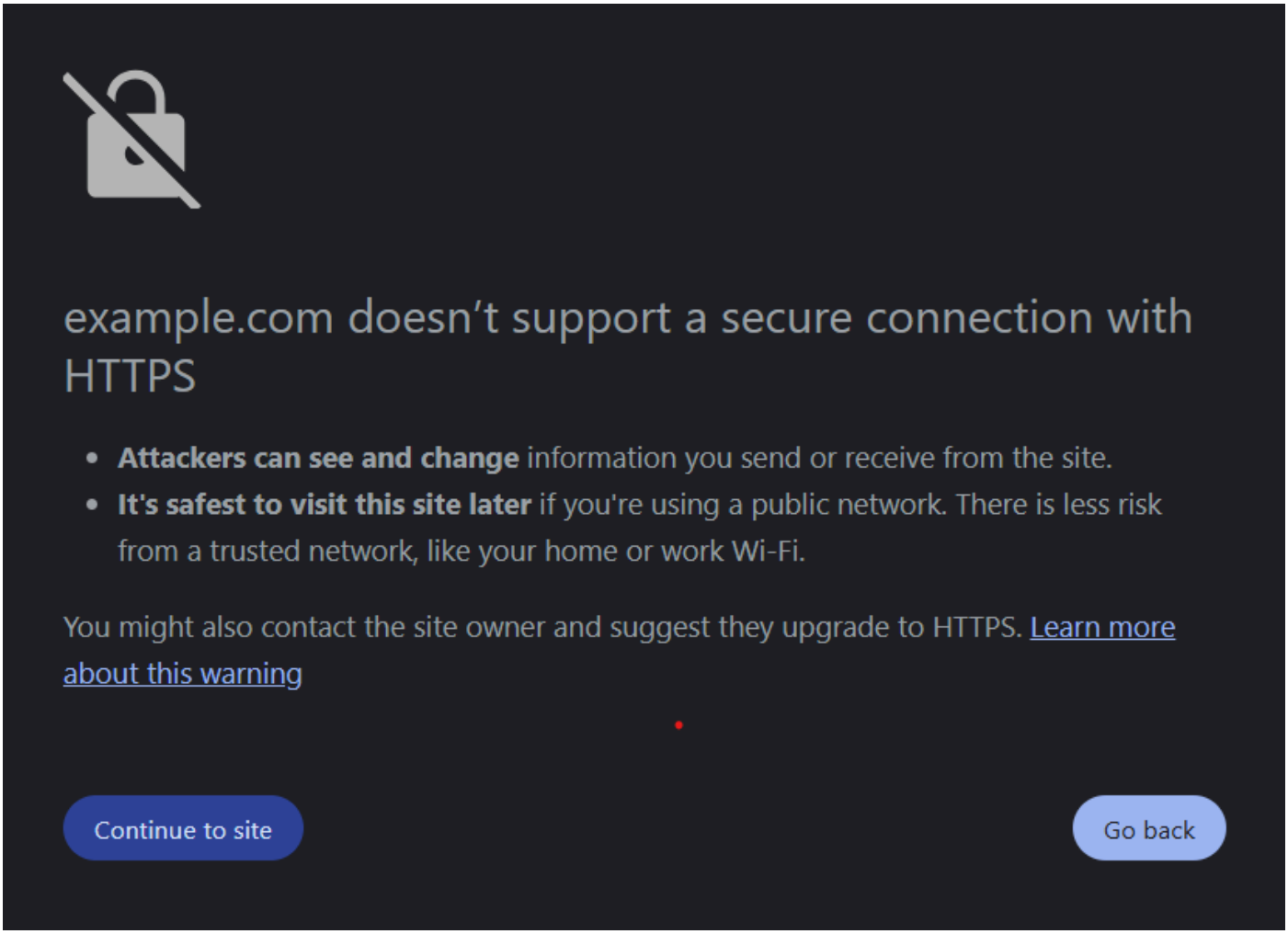
简而言之，当用于通过HTTPS访问网站的域名未出现在服务器的数字证书中时，Umbrella安全Web网关会返回516错误页面。有关描述安全网关返回516错误页面原因的其他信息，请参阅Umbrella知识库文章“516 Upstream Certificate CN Mismatch”错误。

例如，假设一个站点以如下形式提供HTTP URL中的内容：http://www.example.com/path_to_content。如果用户请求等效的HTTPS URL，但站点没有其SAN匹配www.example.com(或许SAN仅匹配example.com)的证书，则如果请求由Umbrella的安全Web网关使用使用SWG的HTTPS检查功能的Web策略处理，则用户会收到516错误。

Chrome行为更改

2023年10月下半月，Google完成了Chrome浏览器新功能的推出。在该日期之后，系统将使用该URL的HTTPS版本自动发出对HTTP URL的请求。例如，当用户请求http://www.example.com时，Chrome会首先尝试使用https://www.example.com完成请求。

如果Chrome在请求HTTPS URL时收到与HTTPS相关的错误，则Chrome会尝试通过HTTP加载相同的内容。如果请求HTTP URL成功，Chrome会根据以下图像显示一个包含文本指示站点不安全的填隙页面和一个用户可选择继续的链接。



这是Chrome新功能中的回退行为。

但是，当通过HTTPS检查的SWG浏览时，如果HTTPS请求从站点产生与HTTPS相关的错误（如“ERR_CERT_COMMON_NAME_INVALID”），则SWG会拦截该错误，并将SWG错误页面返回到

Chrome（如516错误页面）。Chrome不会将此SWG内容视为与HTTPS相关的错误，因此不会生成回退行为，并且会显示SWG错误页面，而不是上一个图像中的页面。

有关新Chrome行为的详细信息，请参阅Chromium博客和功能的GitHub存储库。

确定错误的来源

现在，Chrome自动将HTTP URL升级到HTTPS URL，用户会更频繁地看到生成516个错误的网站。

要确认网站是否导致HTTPS相关错误（例如516响应），请从未使用Umbrella的桌面系统中使用Chrome浏览该网站。请务必在Chrome的Omnibox（类似地址栏）中显式手动输入HTTPS版本的URL，而不是点击HTTP超链接。如果超链接在SWG中生成516错误，则手动请求不带SWG的Chrome中的HTTPS URL时，可能会生成错误消息“ERR_CERT_COMMON_NAME_INVALID”。 此错误消息确认此问题是用于访问网站的域名的错误证书。

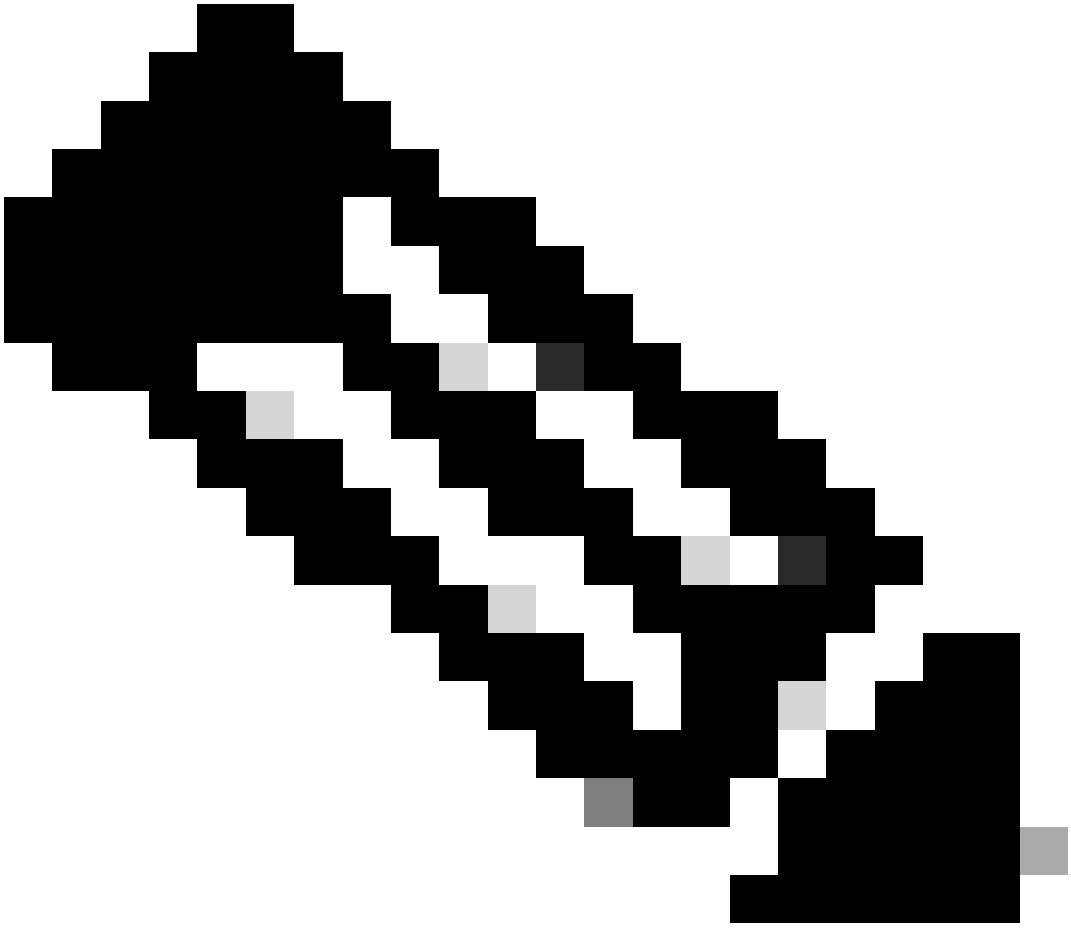
或者，使用在线工具(例如Qualys SSL Server Test site)诊断网站的问题。

解决方法

Umbrella管理员可以使用以下选项之一解决此问题：

1.专门为这些站点创建目标列表，并将该列表添加到无HTTPS检查的Web策略。

2.创建产生516个错误页的站点的选择性解密列表，并将选择性解密列表添加到所有相关的Web策略



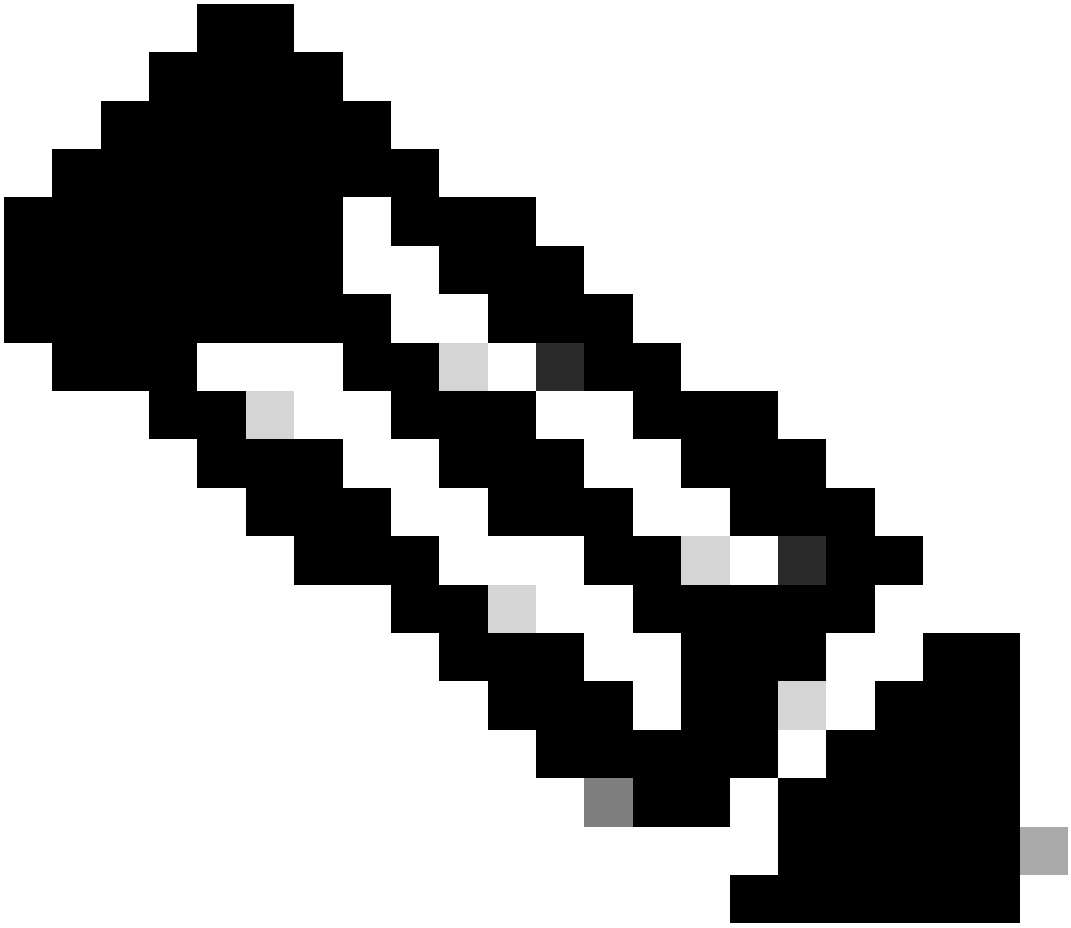
注意：HTTP重定向或邮件安全系统等以服务的HTTPS URL代替原始HTTP URL的因素可以掩盖所需的域名。确定目标列表或选择性解密列表的正确域名可能需要调查，包括使用特定工具（curl、Chrome开发工具、邮件安全供应商的日志等）。

516错误和电子邮件系统

如果电子邮件系统以HTML格式显示电子邮件并允许电子邮件中的超链接，则可能会增加516的错误频率。撰写邮件时，如果发件人键入域名或将其粘贴到邮件正文中，许多邮件系统会自动将纯文本域名提升为超链接。通常，创建链路时，方案是HTTP而不是HTTPS。

例如，在电子邮件中键入字符串`example.com`可生成包含HTML代码`<a href="http://www.example.com">`的电子邮件，该代码显示为超链接www.example.com。

如果此类电子邮件的收件人点击该HTTP超链接，则如果点击打开Chrome或已经使用Chrome查看电子邮件，请求最初将使用HTTPS。



注意：其他浏览器也可以将HTTP升级到HTTPS。

此外，邮件中故意使用HTTP方案的超链接的处理方式也类似。

一些常见的云服务会通过HTTP超链接而不是HTTPS超链接发送来自第三方事务性电子邮件服务提供商的电子邮件。Chrome自动尝试加载的HTTPS站点可以在电子邮件链接中响应域名错误，如本示例中的Seegrid。

当这些电邮的收件人列表较大时，许多通过SWG发送其点击（或请求）的用户可能会报告错误，例如516错误。请联系您的电子邮件服务提供商或发送电子邮件的组织，解决证书错误问题。

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）。