Troubleshoot 516 Errors on Umbrella Secure Web Gateway

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Overview

516 Error Background

Chrome Behavior Change

Determining the Source of the Error

Workarounds

516 Errors and Email Systems

Introduction

This document describes how to troubleshoot an increase in 516 errors on Umbrella Secure Web Gateway.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Umbrella Secure Web Gateway (SWG).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

Users browsing through the Umbrella Secure Web Gateway (SWG) proxy with HTTPS Inspection can receive more frequent 516 Upstream Certificate CN Mismatch error pages beginning in the second half of October of 2023.

The 516 error page occurs when a website's certificate does not match the domain name used by the client to access the site.

The increase in error pages is due to a change in the Chrome browser's handling of requests for URLs which use the HTTP (unencrypted) scheme. Chrome now attempts to load the resource with the HTTPS (encrypted) scheme first. When configured for HTTPS Inspection, SWG inspects a website's certificate and returns a web page displaying an error code such as 516 if the certificate is not acceptable.

To work around this issue, customers can configure their Web policies to bypass HTTPS Inspection for

requests which otherwise result in 516 errors.

516 Error Background

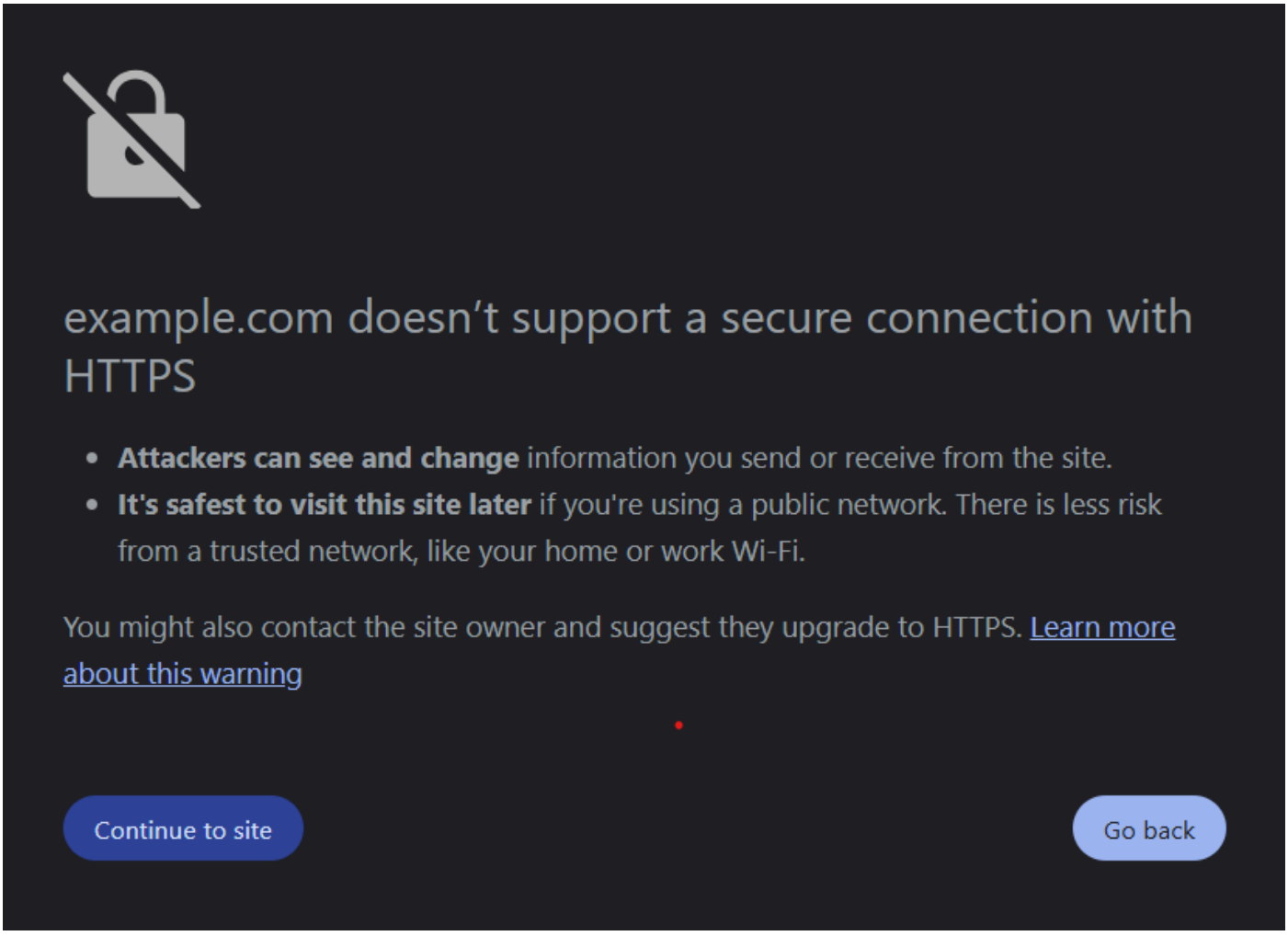
In brief, the Umbrella Secure Web Gateway returns a 516 error page when the domain name used to access a website via HTTPS does not appear in the server's digital certificate. For additional information describing the reason for Secure Web Gateway returning a 516 error page, review the Umbrella Knowledge Base article "516 Upstream Certificate CN Mismatch" error.

For example, consider a site which serves content from HTTP URLs in the form: http://www.example.com/path_to_content. If a user requests the equivalent HTTPS URLs, but the site does not have a certificate whose SANs match www.example.com (perhaps the SAN only matches example.com) then the user receives a 516 error if the request is handled by Umbrella's Secure Web Gateway with a Web policy that uses SWG's HTTPS Inspection feature.

Chrome Behavior Change

In the second half of October 2023, Google completed the roll-out of a new feature for the Chrome browser. After that date, a request for an HTTP URL is automatically made using the HTTPS version of that URL. For example, when a user makes a request for http://www.example.com, Chrome first tries to fulfill the request using https://www.example.com.

If Chrome receives an HTTPS-related error when requesting the HTTPS URL, Chrome then attempts to load the same content over HTTP. If the request for the HTTP URL is successful, Chrome displays an interstitial page with text indicating that the site is not secure and a link which gives the user the option to proceed, per the image below.



This is the fallback behavior in Chrome's new functionality.

However, when browsing via SWG with HTTPS Inspection, if the HTTPS request produces an HTTPS-related error such as "ERR_CERT_COMMON_NAME_INVALID" from the site, SWG intercepts the error and returns an SWG error page to Chrome such as the 516 error page. This SWG content is not considered an HTTPS-related error by Chrome, so does not produce the fallback behavior, and the SWG error page is displayed, rather than the page in the previous image.

More information on the new Chrome behavior can be found from the Chromium blog and the feature's GitHub repository.

Determining the Source of the Error

Now that Chrome automatically promotes HTTP URLs to HTTPS URLs, websites which generate 516 errors are seen more frequently by users.

To confirm that a website is causing an HTTPS-related error such as the 516 response, browse the site with Chrome from a desktop system not using Umbrella. Be sure to manually enter the HTTPS version of the URL explicitly into Chrome's Omnibox (like the address bar) rather than clicking on an HTTP hyperlink. If a hyperlink produced a 516 error with SWG, then manually requesting the HTTPS URL in Chrome without SWG can produce the error message "ERR_CERT_COMMON_NAME_INVALID." This error message confirms that the issue is an incorrect certificate for the domain name used to access the website.

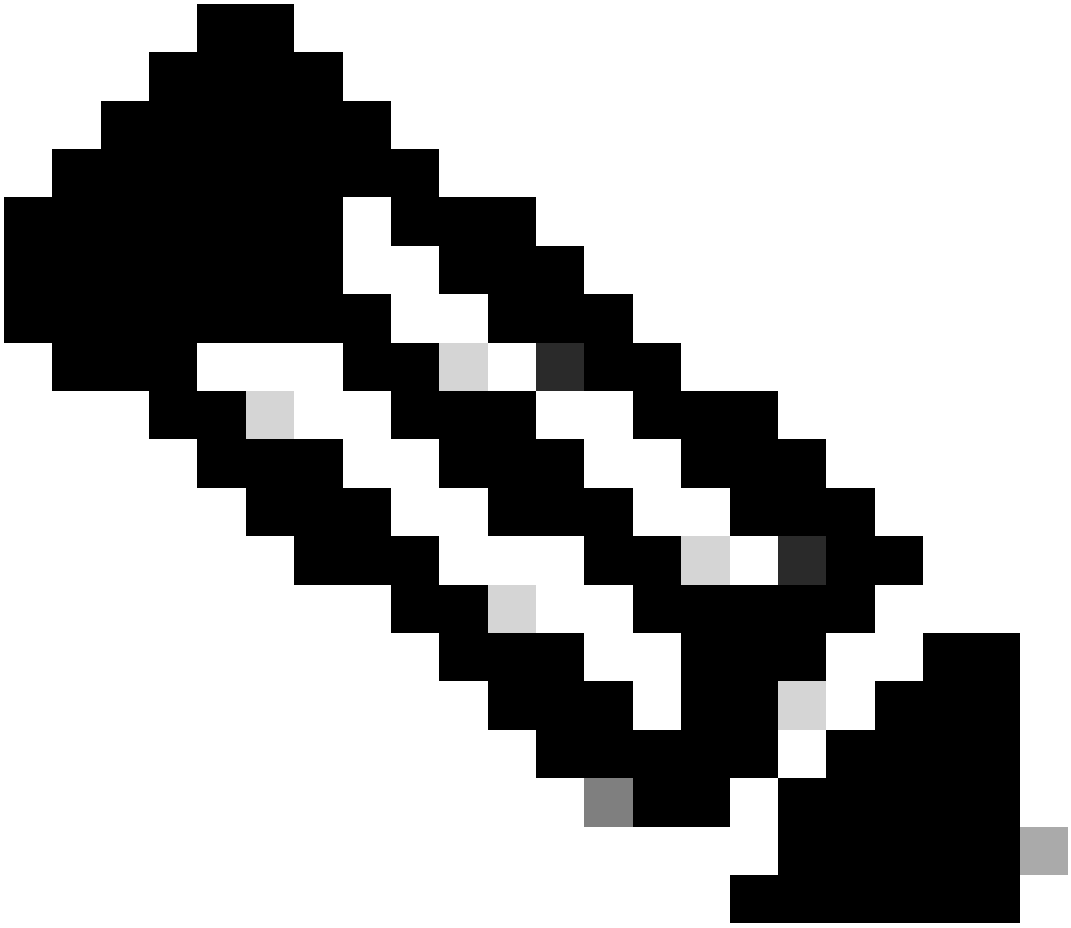
Alternatively, use an online tool such as as the Qualys SSL Server Test site to diagnose the problem with the website.

Workarounds

Umbrella administrators can workaround the issue with one of the these options:

1. Create a Destination List specifically for these sites and add the list to a Web policy without HTTPS Inspection.

2. Create a Selective Decryption List of sites which produce 516 error pages and add the **Selective Decryption List** to all relevant Web policies



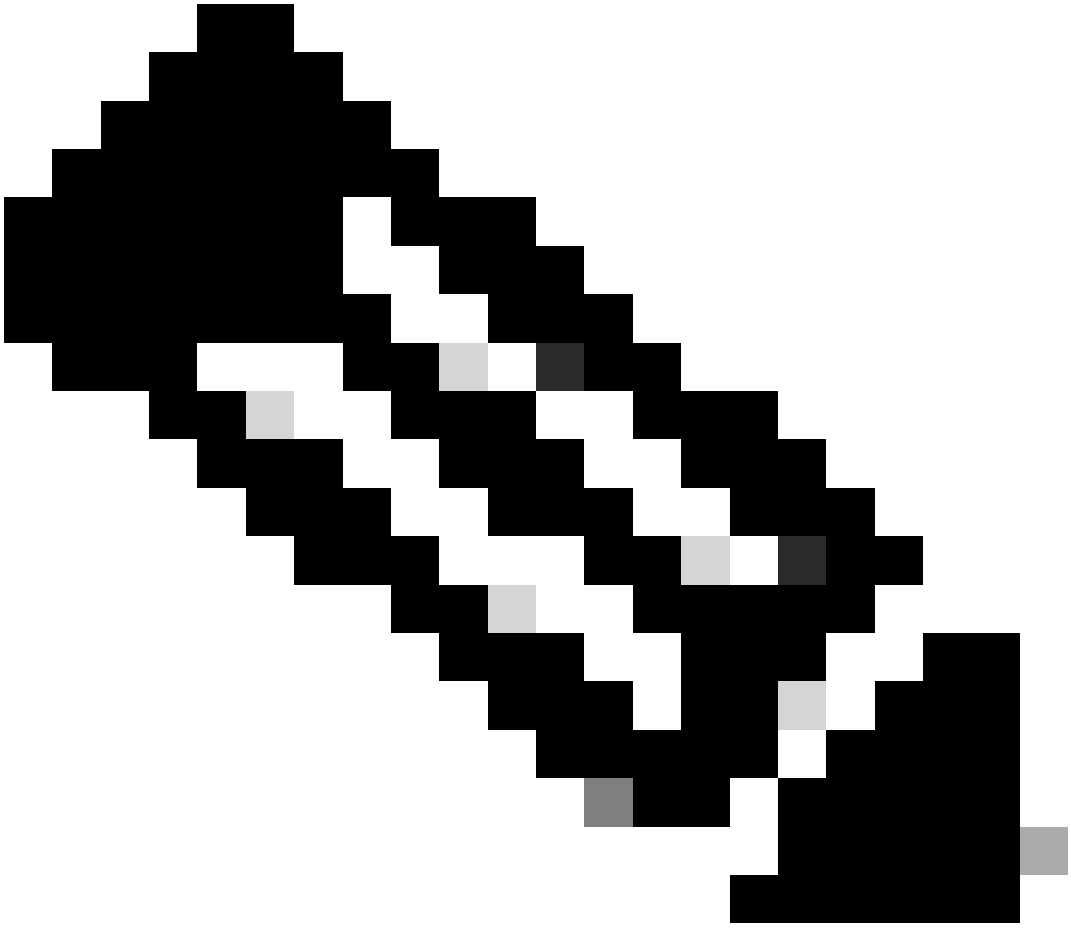
Note: Factors such as HTTP redirects or email security systems which substitute their service's HTTPS URLs for the original HTTP URLs can obscure the needed domain name. Identifying the correct domain name for a Destination List or Selective Decryption List can require investigation, including use of specific tools (curl, Chrome Developer Tools, an email security vendor's log, and so on).

516 Errors and Email Systems

An increase in 516 error frequency can result from email systems that display emails in HTML format and permit hyperlinks in the emails. When composing an email, if the sender types or pastes a domain name into the email body, many email systems automatically promote a plain text domain name to a hyperlink. Typically, when the link is created, the scheme is HTTP rather than HTTPS.

For example, typing the string `example.com` in an email can result in an email containing the HTML code `<a href="http://www.example.com">` which is displayed as the hyperlink www.example.com.

If a recipient of such an email clicks that HTTP hyperlink, the request initially uses HTTPS if the click opens Chrome, or if Chrome is already being used to view the email.



Note: Other browsers can also promote HTTP to HTTPS.

Additionally, a hyperlink in an email that intentionally uses the HTTP scheme is handled similarly.

Some common cloud services send emails from their 3rd-party transactional email service providers with HTTP hyperlinks rather than HTTPS hyperlinks. The HTTPS site that Chrome automatically attempts to load can respond with a certificate error to the domain name in the email link like in this example from Seegrid.

When these emails have large recipient lists, many users whose clicks (or requests) are sent via SWG can report errors such as the 516 error. Please contact your email service provider or the organization which sent the email to have the certificate error addressed.