Troubleshoot SWG Website Access Issues

Contents

Introduction

Background Information

"Access Denied 403" Error Due to Upstream Block

"Access Denied 403" Error Due to Java Issue

High-Level Root Cause of Issue

- What is Java related issue with MPS?
  - Resolution

What is 502 Bad Gateway?

Common Factors for 502 Bad Gateway

- Unsupported SWG Cipher Suites
  - Resolution
- Client Certificate Authentication Request
- Headers Added by Proxy
  - Resolution

Introduction

This document describes how to troubleshoot website access issues seen with Umbrella Secure Web gateway (SWG) Proxy.

Background Information

Let us assume the website www.xyz.com is not accessible via SWG proxy and when users try to access the internet directly (without Umbrella SWG being in the picture), it works fine. Let us review various symptoms and different types of error messages reported when website is inaccessible via SWG. Most common ones are 502 bad gateway, 502 could not relay message upstream error, upstream certificate revoked, access denied 403 forbidden, upstream ciphers mismatch, website just timed out after spinning for sometime or similar.

"Access Denied 403" Error Due to Upstream Block

Webserver or upstream side is blocking or throttling our SWG proxy egress IP ranges. For example, Akamai WAF has block listed a couple of SWG egress IP ranges. To resolve this issue, only option is that reach out to website admins and have them unblock our IP ranges. Until then, bypass SWG using external domains management list for Anyconnect SWG and PAC file deployments. In short, this type of issue is not because of proxy itself, rather its due to incompatibility between proxy and Webservers. Here is the link to refer the KB specifically for "Access Denied 403" error due to Egress IP's block.

In addition, here is the link covering few possible reasons why Akamai has block listed IP addresses.

"Access Denied 403" Error Due to Java Issue

Website is not accessible and throwing "Access Denied or 403 Forbidden - Umbrella cloud security gateway error" when the request is sent through SWG MPS proxy with the file inspection setting enabled. But if File Inspection is disabled, websites loads successfully. Or if we put the website in bypass decryption, websites loads successfully.

High-Level Root Cause of Issue

What is Java related issue with MPS?

The site or web server in question returns a TLS warning regarding SNI or SSL alert back to the proxy after proxy tries to connect to the server. Basically, this happens after the client hello is sent. MPS proxy (which is based on Java and as such) by design, it treats any TLS alerts with "Unrecognized Name" in the description field as an error during SNI parsing and it terminates the transaction. More details found here

Please be aware that this is not SWG or MPS proxy issue. This is one of the incompatibilities with SWG or any other proxies due to misconfiguration on the server side. Browsers usually ignore this warning but SWG or other content security filter treats the SSL warning as a fatal error and terminates the session, which results in 403 forbidden error pages to the users. It can also report 502 Bad Gateway error, but with most of the examples what we have seen is 403 forbidden error, as shown in this image.

15151734443924

As MPS works at application layer, it has little to no control how the TLS layer handles the transaction based on the alerts produced in TLS protocol. It is the responsibility of the server to ensure their TLS endpoint/certificates are configured correctly. Please refer to this link.

To narrow down or troubleshoot the issue, it can be easily pointed out from SSL lab.

15152060146964

When the website is accessed without SWG proxy in the middle or bypass HTTPS inspection from SWG, the website works because the browser is ignoring the SNI Unrecognized name alert and continues communicating with the web server.

At the time of writing this article, the recommended workaround is the best mitigation we can suggest to you. In near future, with the new proxy architecture, we are able to handle these issues more gracefully.

Resolution

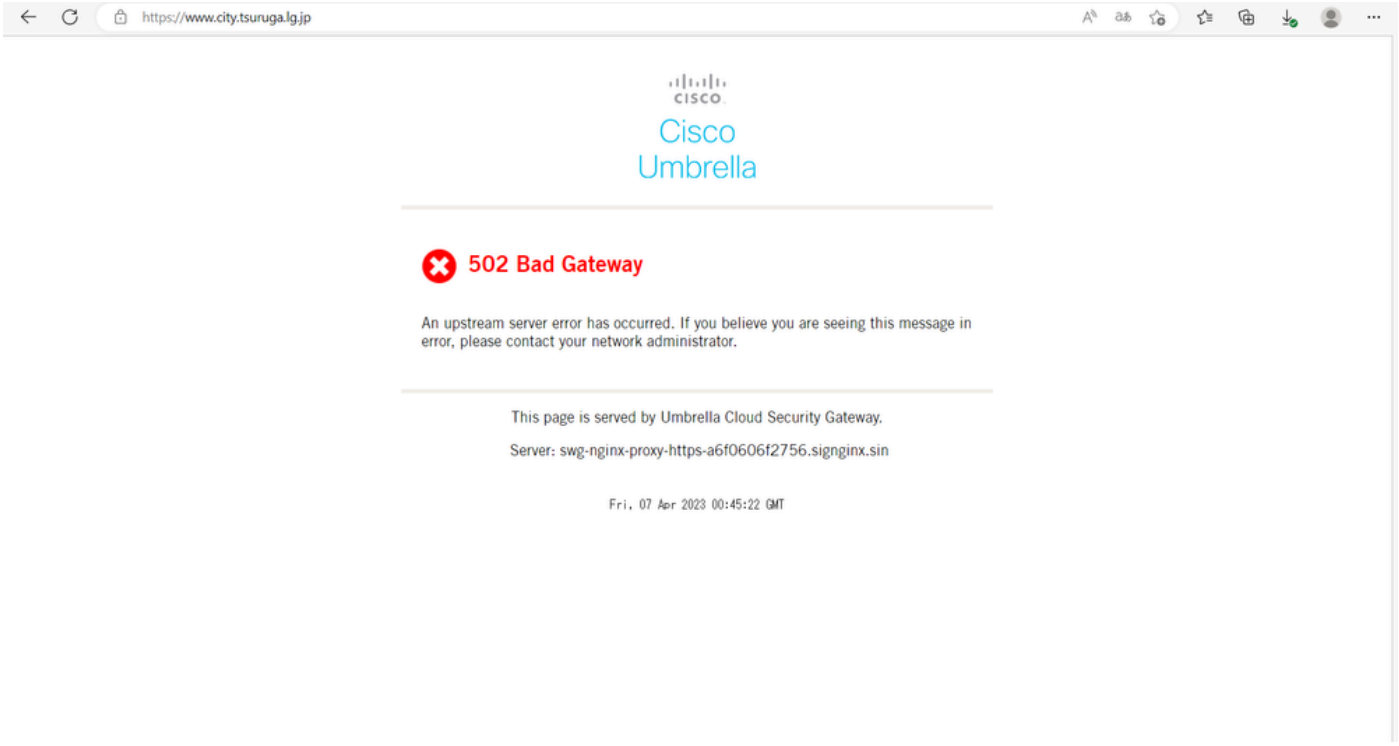
1. Disable Decryption for the affected domains - OR
2. Add the domain to a destination list and associate an allow rule (if you trust the site)

What is 502 Bad Gateway?

A 502 Bad Gateway Error means that the server was acting as a gateway or proxy and received an invalid response from the upstream server. When the user tries to access website via SWG Proxy, there are two flows of communication happen.

a) Client --> Proxy connection (Downstream)
b) Proxy--> End web server connection (Upstream)

502 Bad Gateway error occurs between SWG Proxy (MPS, Nginx) to end server connection.



15026978020884

Common Factors for 502 Bad Gateway

1. Unsupported SWG Cipher Suites

2. Client Certificate Authentication Request

3. Headers Added or Removed by SWG Proxy

Unsupported SWG Cipher Suites

Let us assume a web server reporting unsupported SWG cipher suites during TLS negotiation. Please note that SWG MPS (Modular Proxy Service) Proxy does not support the TLS_CHACHA20_POLY1305_SHA256 cipher suite. Please be aware that there is a separate article to cover SWG-supported cipher suites and TLS. We can easily pinpoint this issue by reviewing ther packets

captured during cipher suites exchange in client hello and server hello. As a troubleshooting step, utilize the CURL command enforcing usage of specific ciphers to narrow down the issue and to confirm it is due to cipher suites as shown in example 1 and 2.

Example of Curl Commands:

<#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:

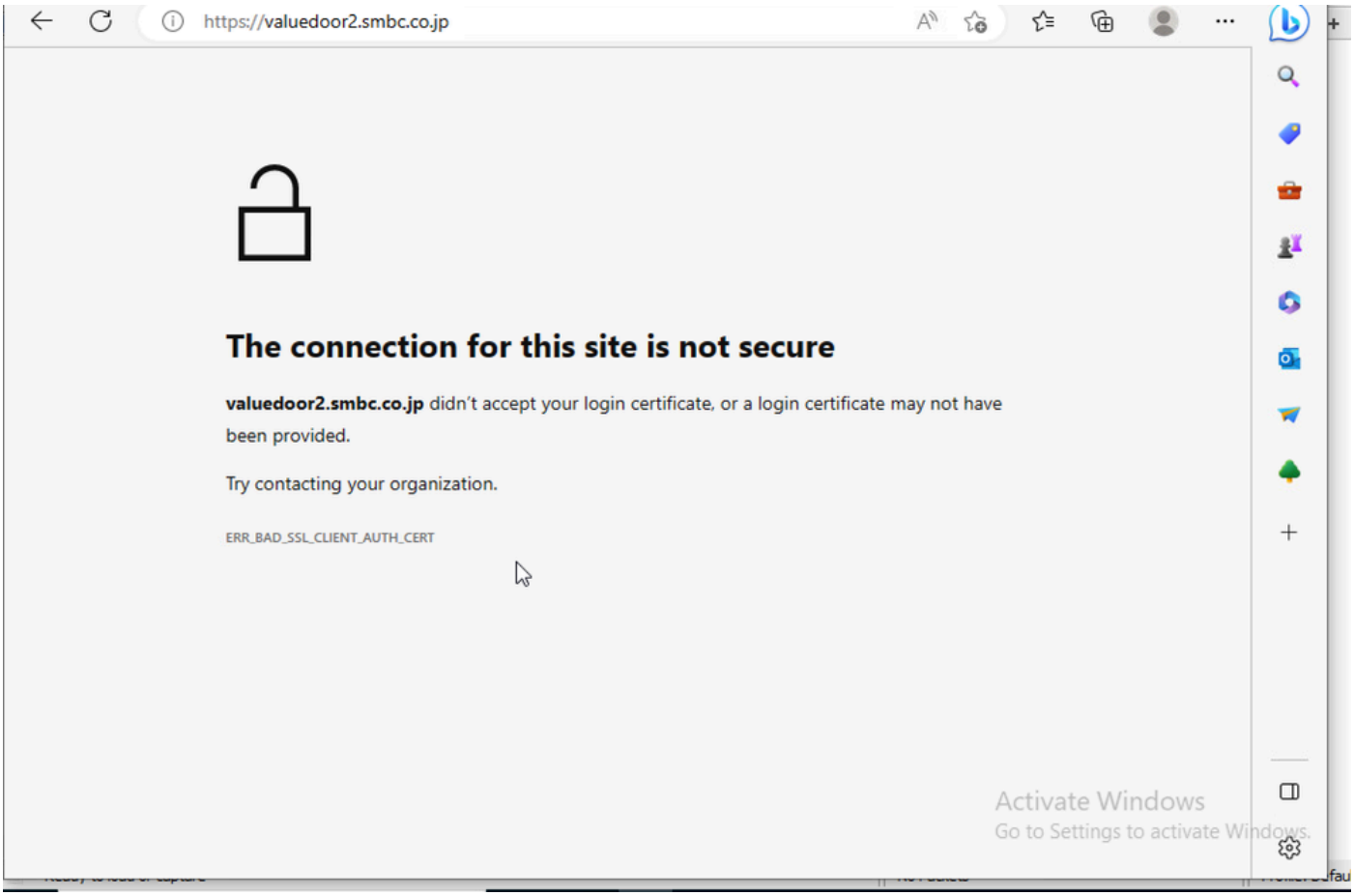
```
 - curl -vvv -o null -k -L www.cnn.com
```

Resolution

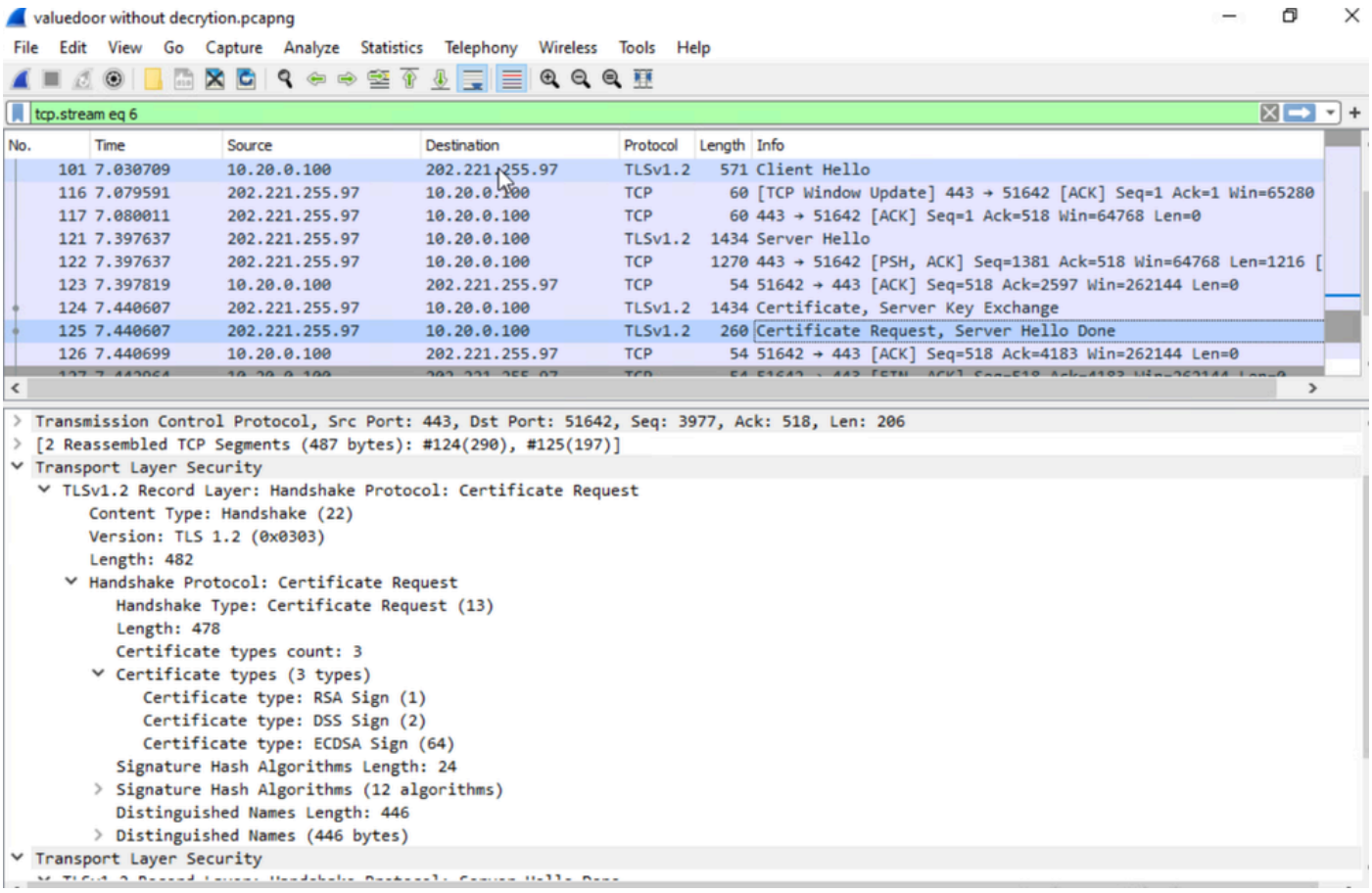
To resolve the issue, skip the inspection for the problematic website using selective decryption list.

Client Certificate Authentication Request

During the TLS handshake between SWG Proxy and upstream, the upstream webserver expects Client certificate authentication. As client certificate authentication is not supported, we need to bypass those domains from proxy using external domains management list, and bypassing just https inspection is not enough. For example: https://valuedoor2.smbc.co.jp.



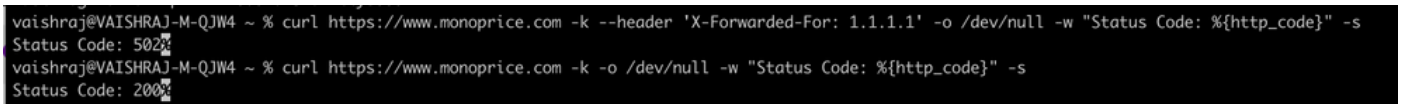
15027182308884



15027192992276

Headers Added by Proxy

The web server is reporting 502 bad gateway error due to X-Forward-For header (XFF) added by SWG Proxy when https inspection is enabled. We can easily narrow down most of the 502 bad gateway issues by first troubleshooting the issue with or without https inspection, and with or without file inspection to rule out file scanning issue with MPS Proxy.



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
```

We use XFF header when the HTTPS inspection is turned on, so that the upstream server can provide optimal geo-location content based on client IP (which provides the user's physical location).

When HTTPS inspection is not enabled, this header is not added by the proxy, so there is not a 502 Bad Gateway error. This is not a SWG proxy issue . This error is due to the upstream web server which is misconfigured to not support standard XFF header.

Resolution

To resolve the issue, bypass HTTPS inspection for specific domain(s) using selective decryption lists.

- 517 Upstream Certificate Revoked
- Certificate and TLS Protocol Errors
- Select SWG DC Manually for Internal Testing