Troubleshoot Secure Web Gateway SWG website access issues

Contents

Introduction

This document describes the structured methodology for diagnosing website access issues when routed through a Cloud-Based Proxy (Secure Web Gateway/SWG), but not when using Direct Internet Access (DIA).

- **Scope:** Applies to both Cisco Umbrella SIG and Cisco Secure Access.

Pre-requisites and Important Warnings

- Verify all troubleshooting is performed on reproducible issues.
- Collect a HAR (HTTP Archive) file and a simultaneous Packet Capture (PCAP) to provide accurate data for analysis.
- Changes to proxy policies (for example, bypassing decryption or inspection) may impact security posture; apply only for troubleshooting or as recommended.

Identify Proxy-Level Errors

Common proxy interference indicators include:

- 502 Bad Gateway
- 515 Upstream Certificate Untrusted
- 517 Upstream Certificate Revoked
- 403 Forbidden
- Revoked certificates
- Cipher suite mismatches
- Website connection timeouts

Troubleshooting Methodology

Step 1: Confirm Traffic Traverses the Proxy

- **Data Collection:** Generate a HAR file and PCAP when the issue occurs.
- **Header Analysis:** Inspect the **Via** header in HTTP responses. Presence of `s_proxy` (Nginx proxy) or `m_proxy` (Modular Proxy Service/MPS) confirms traffic is proxied.
- **TCP Stream:** In Wireshark, follow the TCP stream to ensure the connection is to the proxy's IP, not the destination IP.

Step 2: Verify TLS Decryption Status

- **Browser Inspection:** Click the lock icon in the browser address bar. If the Cisco Secure Access Root Certificate appears in the certificate chain, HTTPS inspection is active.
- **Validation:** Cross-reference the **Via** headers in HAR/PCAP files.
- **OpenSSL Command:** To inspect certificate chains:
  `openssl s_client -connect www.example.com:443 -showcerts`
  This command checks the certificate chain presented by the server. Run it from a machine that traverses the proxy for direct validation.

Step 3: Isolation and Process of Elimination

1. **Phase A – Test HTTPS Inspection (Nginx Layer):**
   - Add the problematic domain to the SWG "Do Not Decrypt" list.
   - Keep File Inspection enabled.
   - **If the issue is resolved:** The root cause is likely Nginx SSL/TLS inspection. Analyze the PCAP for cipher mismatches or SNI issues. Use `curl` with and without proxy to compare behavior.
   - **If the issue persists:** Proceed to Phase B.
2. **Phase B – Test File Inspection (Scanning Layer):**
   - Disable File Inspection for the specific traffic.
   - **If the issue is resolved:** The root cause lies within the file-scanning engine. Review PCAP and HAR, reproduce in lab, and determine if a specific file or scanning signature triggers the issue.
   - **If not resolved:** Contact Support with comprehensive logs and findings.

Common Issues and Error Codes

515 Upstream Certificate Untrusted

This error occurs when the SWG proxy cannot validate the destination server’s certificate. Causes include expired, self-signed, or incomplete certificate chains.

- **HTTPS Inspection ON + File Inspection ON:** Website works; no certificate errors.
- **HTTPS Inspection ON + File Inspection OFF:** 515 error is observed, matching user report.

- **HTTPS Inspection OFF + File Inspection OFF (domain on Do Not Decrypt list):** No issues observed.

Technical Detail: Nginx proxy may fail if the upstream server relies on Authority Information Access (AIA) fetching for missing intermediate certificates, as Nginx does not handle AIA as gracefully as File Scanning proxy service. SNI and SAN mismatches during TLS handshake can also trigger failures.

517 Upstream Certificate Revoked

The 517 error means the SWG proxy's CRL or OCSP check found the upstream server's certificate revoked.

- **Troubleshooting:** Use external tools such as SSL Labs or OpenSSL to confirm revocation status.
- **Documentation:**
  - Cisco Troubleshooting Error 517 – Upstream Certificate Revoked
  - Understand Common Certificate and Protocol Errors

Certificate Error Handling Options

Cisco Secure Access will be introducing new feature called "Certificate Error Handling Options" for granular error bypass without disabling decryption entirely. Domains that trigger certificate errors due to inspection can be managed using this feature instead of broad "Do Not Decrypt" lists.
This feature exists in Umbrella SIG as of today. Feature Requests details for CSA.

502 Bad Gateway

The 502 error indicates the SWG proxy received an invalid response from the upstream server while acting as an intermediary.

- Downstream: Client to SWG Proxy
- Upstream: SWG Proxy to Destination Server

The error is always in the upstream connection—due to protocol errors, TCP resets, or malformed headers.

Common 502 Causes

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

Unsupported Cipher Suites

Cause: Server requires a cipher not supported by SWG (for example, TLS_CHACHA20_POLY1305_SHA256).
Resolution: Add the domain to Selective Decryption list.

Testing Commands:
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
```
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
```

Client Certificate Authentication Request

Cause: The upstream server requires client-side certificates, which SWG does not support.
Resolution: Bypass the domain from the proxy using the External Domains management list (Umbrella SIG) or Bypass Secure Proxy (Cisco Secure Access). Bypassing HTTPS inspection alone is insufficient.

Headers Added by Proxy

Cause: Some servers reject requests with the X-Forwarded-For (XFF) header added by SWG when HTTPS inspection is enabled.
Resolution: Compare behavior with/without HTTPS and file inspection. If the error only occurs when XFF is present, the web server is likely misconfigured.

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

The XFF header is added for geolocation. If the server cannot process it, a 502 error results.

Potentially Unwanted PUA or Corrupted Files

If SWG cannot scan a file using file inspection (for example, protected, range-requested, or corrupted files),

it blocks the download and reports - Blocked – Potentially Unwanted Application (Protected File)

- Troubleshooting: Capture a HAR during the block event. Use Override Security as a temporary workaround. If the file is corrupted or malicious, it must be corrected at the source.

Potentially Harmful Categories and Reputation Blocks

- Use Talos to check web reputation (WBRS). If a domain is wrongly categorized, submit a COG Jira request to Talos for review. Talos categorized as safe or favorable but still SWG block then we need check from Beaker service of SWG.

Access Denied by Akamai for SWG Egress IPs

- SWG uses shared egress IPs. If these are blacklisted by IP reputation services (for example, Brightcloud), access to certain sites may be denied.

Known Issues: Youtube Sign-In Bot and Video Unavailabl