Verifying Network Connectivity Requirements for BigPanda Cloudflare WAF Implementation

Introduction

This guide will help you verify that your network devices and servers meet the necessary requirements to maintain connectivity with our web services after implementing Cloudflare WAF. This document covers the three key requirements:

(1) up-to-date root certificates
(2) Server Name Indication (SNI) support, and
(3) dual-stack (IPv4 and IPv6) support.

For legacy appliances that cannot be updated to support these requirements, you may need to deploy a proxy server as a workaround if you are unable to migrate to replace the appliances at this time.

The key points are:

- Devices connecting to BigPanda's Cloudflare WAF need the ISRG Root X1 certificate in their trust store
- Devices must support SNI for proper routing by the Cloudflare WAF
- Devices must support a dual-stack endpoint, supporting both IPv4 and IPv6, which is used by Cloudflare WAF
- For legacy servers and devices that cannot be updated, a proxy server like HAProxy can be used as a workaround
    - The proxy needs to add the SNI header and rewrite the Host header to match the Cloudflare endpoint
    - IPv4 DNS resolution should be preferred if the network is IPv4-only
    - Thorough testing is important before deploying a proxy server to production.
- This guide only applies to network servers and appliances that communicate to BigPanda API endpoints.

Verify Network Appliance Connectivity Requirements

Requirement 1. Check for Up-to-date Root Certificates

Your network devices and servers must have the latest root Certificate Authorities (CAs) installed in their local trust store. Specifically, the ISRG Root X1 CA must be present.

BigPanda's Cloudflare WAF endpoints use Let's Encrypt certificates, so the ISRG Root X1 is required for successful SSL/TLS handshakes. You can obtain this certificate from Let's Encrypt's official website.

To check if you have the ISRG Root X1 CA:

- Linux:
  - Check your trust store, typically located at `/etc/ssl/certs/ca-certificates.crt`
    - Confirm the trust store path on your server before running the next command
  - Command to check the local trust store:
    `openssl x509 -in /etc/ssl/certs/ca-certificates.crt -text`
  - Testing Certificate Trust:
    `openssl s_client -connect eu.bigpanda.io:443 -showcerts`
    - Check that the certificate chain includes ISRG Root X1
    - Verify there are no certificate validation errors

- Network Appliances:
  - Consult your device's documentation or vendor for instructions

If the ISRG Root X1 is missing, you will need to update your trust store to include it.

Requirement 2. Server Name Indication (SNI) Support

Your devices and applications must support and utilize Server Name Indication (SNI). SNI is an extension to the TLS protocol that allows the client to specify the hostname it is attempting to connect to during the SSL/TLS handshake.

Cloudflare WAF requires SNI for proper routing and security. Without SNI, the WAF may be unable to determine the correct backend server.

Older OpenSSL versions (i.e. pre-1.0.0) do not support SNI unless explicitly enabled with the `-servername` flag, while newer versions include it by default when a hostname is provided. By testing both with and without SNI explicitly set, you can deduce the server's capability.

- ### Step 1: Check OpenSSL Version

  First, run this on your legacy server to see what OpenSSL version you're working with:

  ```
  openssl version -a
  ```

  If the version is OpenSSL 0.9.8 or older, SNI is not supported natively, and the test will confirm this. If it is a version greater than 1.0 (e.g., OpenSSL 1.0.1), SNI is supported, and the failure might be due to another issue.

- ## Step 2: Test Without Explicit SNI

  Run this command on your legacy server:

  ```
  openssl s_client -connect eu.bigpanda.io:443
  ```

  This attempts a TLS connection to www.bigpanda.io on port 443. Older OpenSSL versions (e.g., 0.9.8) will not send an SNI header because SNI isn't supported or isn't included unless the parameter `-servername` is specified. On newer versions, SNI is often sent automatically using the hostname from `-connect`, which we will test in the next step. Error messages will indicate a lack of SNI support on the legacy device. Example errors:

  - no peer certificate available
  - No client certificate CA names sent
  - Cipher is (NONE)

- ## Step 3: Test With Explicit SNI (Control Test)

  Run this command on your legacy server:

  ```
  openssl s_client -connect eu.bigpanda.io:443 -servername eu.bigpanda.io
  ```

  This command explicitly includes the SNI header with the hostname www.bigpanda.io. Even on older OpenSSL versions that support SNI (e.g., 0.9.8 with patches or 1.0.0+), this should work if SNI is the only issue.

- ## Interpreting the Results

  1. **If Step 2 Fails and Step 3 Succeeds**:
     - Your server supports SNI but does not send it by default with just `-connect`. This indicates a slightly outdated OpenSSL version that requires `-servername`.
  2. **Both Fail**:
     - Your server uses a very old version of OpenSSL that **does not support SNI**, or it is too old to negotiate a modern TLS connection with Cloudflare (e.g., no TLS 1.2 support). Check the OpenSSL version and error details.
  3. **Both Succeed**: Your server supports SNI.

SNI is typically enabled by default on modern Linux distributions and applications using OpenSSL. Check your web client or network appliance's configuration to ensure SNI is enabled, referring to the vendor's documentation.

Requirement 3. Verify Compatibility with dual-stack endpoint (support for both IPv4 and IPv6)

Cloudflare's services are accessible via both IPv4 and IPv6. If the legacy network appliance supports IPv4-only, and the DNS resolution for the Cloudflare WAF endpoint returns both IPv4 and IPv6 addresses, the network appliance might attempt to connect using IPv6, which would fail.

To confirm that your Linux-based appliance does not support dual-stack endpoints (i.e., it can only use IPv4 and not IPv6 alongside it) when connecting to Cloudflare WAF, you will run commands to test IPv4 and IPv6 connections through your legacy network appliance. Since eu.bigpanda.io is behind Cloudflare, which supports dual-stack (IPv4 and IPv6) by default, you can test your network appliance by running OpenSSL commands to reveal any limitations.

To check if your legacy appliance supports dual-stack endpoints, you will test for IPv4 connections and then attempt to force an IPv6 connection:

- ### Step 1: Attempt Connection using IPv4

  Run this command on your legacy appliance:

  ```
  openssl s_client -connect eu.bigpanda.io:443 -servername eu.bigpanda.io
  ```

  On an IPv4-only system, the Linux network stack will only use the A record (IPv4) because it cannot handle AAAA (IPv6) records. If the server connects successfully, it is using IPv4. You will test IPv6 capability in the next step.

- ### Step 2: Attempt Connection using IPv6 address

  Attempt an IPv6 connection from the legacy server to test for dual-stack support. The connection will fail if the legacy server only supports IPv4.

  1. Get the endpoints IPv6 address:
     `dig eu.bigpanda.io AAAA +short`
     - For example, in Feb 2025 the IPv6 address returned is:
       `2606:4700:4400::6812:26fa`

  2. Use the IPv6 address to connect to the endpoint using OpenSSL:
     `openssl s_client -connect "[2606:4700:4400::6812:26fa]:443" -servername eu.bigpanda.io`
     - On an IPv4-only network appliance this command will fail immediately with an error like:
       ```
       connect: Network is unreachable
       connect: errno=101
       ```

- The failure happens because the legacy appliance's network stack does not support IPv6.
- Therefore, no TLS handshake occurs, indicating failure is at the network level.
- On a dual-stack system, this command would succeed, showing a completed TLS handshake with Cloudflare's certificate, the TLS version, and the cipher.

- Interpreting the Results

1. **If Step 1 Succeeds (IPv4 works) and Step 2 Fails (IPv6 unreachable)**:
   - This confirms that dual-stack endpoints are not supported by the legacy server.

2. **If Both IPv4 and IPv6 Test Connections are Successful:**
   - Your server supports dual-stack endpoints (IPv4 and IPv6) like Cloudflare WAF.

If you have a legacy appliance that only supports IPv4, it is possible your appliance will fail to connect, or have intermittent connection failures, if it fails to negotiate DNS properly and attempts to connect using IPv6 - which would fail.

Conclusion

Please check any legacy network appliances used to connect to BigPanda if you have any concerns about their ability to support the requirements in this document. All network traffic to BigPanda endpoints must meet these requirements to successfully connect to BigPanda once our Cloudflare WAF is enabled.

If you have legacy network appliances that cannot be updated to meet the network connection requirements described in this guide, you will either need to replace the legacy appliance or stand up an HAProxy server as a workaround to route your network traffic to BigPanda APIs. The proxy server would act as an intermediary, handling the SSL/TLS handshake with Cloudflare WAF on behalf of the legacy appliances.

Please contact BigPanda support team at support@bigpanda.io if you have any questions.