

ZTA Browser-Based Private Resource TLS Handshake Failure

Contents

Issue

Users are unable to access a browser-based private resource through Cisco Secure Access.

When attempting to connect, these symptoms occur:

- TCP three-way handshake completes successfully, but TLS negotiation fails after the Client Hello.
- Connection to the public SSE-mapped URL (<https://example-orgid.ztna.sse.cisco.io>) reaches Cisco authentication but returns HTTP 404 error.
- After adding the FQDN to the private resource configuration, traffic redirects to the authentication prompt but results in a blank page after authentication.
- HAR files show HTTP 200 responses, but TLS handshake does not complete.
- Block reason appears as: "Private Access: fetched posture data for device is too old/needs to be refreshed".

Environment

- Cisco Secure Access (SSE)
- Secure Access org ID: xxxx
- Browser-based Zero Trust Network Access (ZTNA)
- Private resource: example.net
- Working private resource for comparison: abc.net
- Wildcard certificate configuration

Resolution

The issue was resolved by configuring the private resource to use the same certificate configuration as a working private resource.

The steps outlined in the next sections were taken.

Step 1: Analyze Working Configuration

Compare the failing private resource (example.net) with a working private resource (abc.net) to identify configuration differences.

The working resource used:

- **Use a URL in your domain** option
- Reference to the existing wildcard certificate/key pair

Step 2: Packet Capture Analysis

Perform packet capture analysis using Wireshark to confirm the TLS handshake failure:

- Verify TCP three-way handshake completes successfully.
- Confirm TLS negotiation fails after Client Hello.
- Collect diagnostic artifacts: HAR files, DART bundle, and packet captures.

Step 3: Certificate Verification

Access the application over RAVPN connection to verify certificate presentation:

- Confirm the website example.net is presenting a wildcard certificate.
- Document certificate details for configuration reference.

Step 4: Configure Private Resource

Apply the same configuration approach used by the working private resource:

- Configure the private resource to use **Use a URL in your domain** option.
- Reference the existing wildcard certificate/key pair.
- Ensure the FQDN is properly configured in the private resource field.

Step 5: Validation

Test browser-based access to confirm the configuration resolves the issue:

- Verify successful TLS handshake completion.
- Confirm proper authentication flow.
- Validate application accessibility post-authentication.

Cause

The root cause was a configuration mismatch in the private resource setup. The failing private resource was not configured to properly reference the wildcard certificate that the target application was presenting. The TLS handshake failed because the private resource configuration did not align with the certificate configuration used by the application server. By configuring the private resource to use the **Use a URL in your domain** option and referencing the existing wildcard certificate/key pair (matching the working configuration), the TLS negotiation could complete successfully.

Related Content

- [Cisco Reference Guide for Secure Access](#)
- [Cisco Technical Support & Downloads](#)