SSL Decryption Certificate Error Handling in Secure Access

Contents

Issue

Users are experiencing certificate-related error pages when SSL decryption is enabled in Cisco Secure Access. Multiple inquiries have been received regarding three specific types of certificate errors:

- Origin server certificate expired errors
- Certificate CN/SAN mismatch errors where the Common Name or Subject Alternative Names listed on the certificate do not match the accessed domain
- Certificate Revocation List (CRL) link embedded in the origin server certificate causing connectivity issues

These certificate errors are similar to warnings that would normally be displayed in web browsers. The question arises whether Cisco Secure Access can handle certificate-related errors by displaying warning pages (similar to browsers or content filters) and then allowing access after displaying the warning, or permitting access in all cases. Additionally, there is a need to understand the behavior when SSL decryption is disabled and whether traffic passes through regardless of certificate issues.

Environment

- Cisco Secure Access - Internet Access (Roaming Module, VA, DNS, SWG, PAC, IPS, Certificates)
- SSL decryption functionality enabled
- Multiple domains experiencing certificate validation issues
- Origin servers with various certificate problems including expiration and domain mismatch

Resolution

Certificate Error Handling Limitations

Certificate-related error handling is not available in Cisco Secure Access. The product does not support:

- Presenting browser-like warning pages for certificate issues
- Domain-specific certificate error handling configuration
- Custom error handling based on destination domains
- Content filter-style warning pages with user override options

SSL Decryption Exclusion Workaround

The recommended approach is to exclude problematic domains from SSL decryption using the security profile decryption settings. This can be configured through:

Navigate to the **Security Profile > Decryption Settings** section to exclude specific domains from SSL inspection.

When domains are excluded from SSL decryption, this behavior occurs:

- Traffic for excluded domains bypasses SSL inspection entirely
- Certificate validation is not performed by Secure Access
- Users do not encounter certificate error pages generated by Secure Access
- The original certificate errors are possibly still be visible in the user browser if the certificate issues persist

SSL Decryption Disabled Behavior

When SSL decryption is disabled for a domain or globally, Cisco Secure Access passes the traffic through (forward) regardless of any certificate problems. The product does not inspect or validate certificates when decryption is not enabled, effectively allowing all HTTPS traffic to pass through transparently.

Cause

The certificate errors are caused by legitimate certificate validation issues on the origin servers, including expired certificates, CN/SAN mismatches, and CRL connectivity problems. Cisco Secure Access performs certificate validation as part of its SSL decryption process, and when these validation failures occur, the product generates error pages to prevent potentially insecure connections. This is the intended security behavior of the SSL inspection feature.

Related Content

- Cisco Secure Access Decryption Configuration Documentation
- Cisco Technical Support & Downloads