CRYPTO_INTERNAL_ERROR during Google Drive Secure Downloads

Contents

Issue

Encrypted Google Sheets files fail to open when accessed through Cisco Secure Access with traffic decryption enabled. Users encounter a CRYPTO_INTERNAL_ERROR during Google Drive secure downloads. This issue occurs specifically when the Secure Web Gateway (SWG) inspection is active, as Range headers are ignored during the decryption and inspection process, leading to interference with the Google secure download mechanism.

The problem affects environments using RAVPN+ZTA implementation and impacts access to encrypted Google Sheets for large user populations.

Environment

- Technology: Cisco Secure Access (Solution Support)
- Sub-technology: Secure Access
- Implementation: RAVPN+ZTA (Remote Access VPN + Zero Trust Access)
- Component affected: ZTA Profile
- Affected domains: clients6.google.com and other Google Drive-related domains

Resolution

The resolution involves implementing temporary workarounds while monitoring for permanent vendor-side fixes.

The approaches outlined in the next sections have been validated to restore access to encrypted Google Sheets.

Temporary Workaround Options

Option 1: Disable Traffic Decryption

Completely disable traffic decryption for the affected user groups or policies. This restores Google Sheets access but removes all decryption-based security inspection capabilities.

Option 2: Exclude Google Drive Domains from Decryption

Add Google Drive-related domains to the do-not-decrypt list in the Secure Access policy configuration:

- clients6.google.com
- Other Google Drive-related domains as identified in traffic analysis

This approach maintains decryption for other traffic while allowing Google Sheets to function normally. However, this workaround has the trade-off of disabling CASB Google Drive upload block functionality for the excluded domains.

Technical Analysis and Monitoring

The Cisco analysis confirmed that Secure Web Gateway inspection ignores Range headers to enable comprehensive security scanning of file content. This behavior interferes with the Google Drive secure download process, which relies on Range headers for proper decryption flow.

Google has acknowledged the issue and identified that proxy behavior (including Cisco Umbrella/network proxy) interferes with Google Drive secure download requests by removing or rewriting Range headers. This forces a full-file download that breaks the Google decryption mechanism. Google is developing a client-side fix, though no estimated time of arrival has been provided.

Implementation Considerations

Organizations implementing the workarounds ought to consider the security implications:

- Evaluate the risk of excluding Google Drive domains from decryption inspection.
- Review CASB policies that can be affected by the domain exclusions.
- Document the temporary nature of the workaround for future policy reviews.
- Monitor for updates from Google regarding their client-side fix development.

Cause

The root cause is a compatibility issue between Cisco Secure Access SWG inspection behavior and the Google Drive secure download mechanism.

Specifically:

Cisco Secure Web Gateway inspection ignores Range headers during the decryption and security scanning process to ensure complete file analysis. However, Google Drive encrypted file access relies on Range headers to properly handle the decryption flow for secure downloads. When these headers are removed or modified during the proxy inspection process, Google client-side decryption fails, resulting in the CRYPTO_INTERNAL_ERROR.

This represents a fundamental incompatibility between security inspection requirements (full file scanning) and the Google encrypted file delivery mechanism (range-based secure downloads).

Related Content

- Cisco Technical Support & Downloads