Verify Brotli Compression Support for Secure Web Gateway

Contents

Introduction

This document describes a specific SWG limitation where SSL inspection disables Brotli compression support, which can cause web loading issues.

Background Information

When SSL inspection (HTTPS decryption) is enabled in Cisco Secure Web Gateway (SWG), a key limitation is that SWG currently does not support Brotli compression. This limitation affects how content encoding headers are handled during SSL decryption, which can lead to issues with content and incomplete web asset loading.

Problem

Actually SWG's lack of Brotli support causes the proxy to strip or alter the Accept-Encoding header that includes Brotli (br). As a result, the server can respond with unexpected MIME types such as **application/x-gzip** instead of the correct **application/javascript**. This MIME type mismatch triggers browser security features like Chrome's Opaque Response Blocking (ORB), which blocks the content to prevent potential security risks. Consequently:

- Assets compressed with Brotli can not be properly handled or recognized by SWG during SSL decryption.
- The proxy's removal of Brotli from the Accept-Encoding header causes the server to serve content with incorrect MIME types.
- Browsers block the content, causing failures in loading essential web assets.

Solution

To mitigate this issue, it is recommended to bypass SSL decryption for affected domains by adding them to the "Do Not Decrypt" list. This prevents the MIME type mismatch and content blocking. Additionally, it is expected that Cisco Secure Web Gateway support Brotli compression and provide improved handling of modern web content encoding in the near future.

Related Information

- Cisco Technical Support & Downloads
- Other Secure Access Docs