

Secure Access Password-Protected ZIP File Download Configuration

Contents

Issue

After migrating to Cisco Secure Access, users are unable to download password-protected (encrypted) ZIP files. The downloads fail consistently when attempting to access encrypted file content through the Secure Access service. This issue occurs despite having configured internet-bound traffic policies on a C8200 device with multiple security rules including category-based blocking, SSL inspection controls, and sandbox functionality.

Users experience complete download failures when attempting to access password-protected ZIP files that were previously accessible before the Secure Access migration. The issue persists across multiple tunnel groups and affects all 15 configured locations.

Environment

- Cisco Secure Access (Secure Access OrgID: 8320925)
- C8200 device managing internet-bound traffic policies
- Multiple tunnel groups across 15 locations (TK-TG and others)
- SSL inspection policies with both enabled and disabled configurations
- Sandbox security profiles enabled on certain policies
- IPS profiles configured on specific access rules

Resolution

The resolution for allowing password-protected ZIP file downloads in Cisco Secure Access involves configuring the **Allow access to encrypted files** setting and implementing appropriate workarounds when necessary.

Primary Configuration Method

Step 1: Access the Cisco Secure Access Policy Configuration

Navigate to the specific access policy that handles the affected traffic in your Cisco Secure Access dashboard.

Step 2: Enable Encrypted File Access

In the policy **Advanced Settings**, locate and enable the **Allow access to encrypted files** option. This setting is configured on a per-rule basis and controls whether encrypted content can be accessed through that specific policy.

Step 3: Apply the Configuration

Save and apply the policy changes to make them active for user traffic.

Alternative Workaround Method

If the primary method does not resolve the issue, implement the workaround described in the next sections.

Step 1: Identify Affected URLs

Determine the specific URLs or domains where password-protected ZIP files are hosted and causing download failures.

Step 2: Configure Do Not Decrypt List

Add the identified URLs to the **Do Not Decrypt** list in your Cisco Secure Access configuration. This prevents SSL inspection on these specific URLs.

Step 3: Create SSL Inspection Bypass Policy

Ensure that an access policy with SSL inspection disabled is configured to handle traffic to these URLs.

This policy must have:

- SSL inspection disabled
- All security profiles disabled
- Higher priority than SSL inspection enabled policies

Policy Configuration Reference

The policy order outlined in the next subsections and their respective configurations can be used as a reference for proper traffic handling.

Policy 1: Category-based Blocking Rule

- Policy Name: IA-To-InternetContentBlock
- IPS Profile: None
- Purpose: Block specific content categories
- Target: All tunnel groups

Policy 2: SSL Inspection Disabled Rule

- Policy Name: IA-SSL-Inspection-MUKOU
- IPS Profile: Disabled

- Security Profiles: All disabled
- Target: All tunnel groups

Policy 3: SSL Inspection-enabled Rule

- Policy Name: IA-SSL-Inspection
- IPS Profile: Enabled
- Security Profiles: Sandbox functionality enabled
- Target: All tunnel groups

Important Configuration Notes

No Global Settings equivalent exists for the **Allow access to encrypted files** functionality. This setting must be configured on individual access policies as needed. Each policy that requires encrypted file access must have this setting explicitly enabled in its Advanced Settings configuration.

When testing configuration changes, allow sufficient time for policy propagation across the Cisco Secure Access infrastructure before validating functionality. Service incidents or maintenance windows can affect testing results and must be considered when troubleshooting.

Cause

The issue occurs because Cisco Secure Access, by default, blocks access to encrypted files as a security measure. When SSL inspection is enabled and encounters password-protected or encrypted content, the service prevents download unless explicitly configured to allow such access. The **Allow access to encrypted files** setting in the Advanced Settings of access policies controls this behavior, and without this setting enabled, encrypted ZIP files and similar content is blocked during the download process.

Additionally, SSL inspection policies can interfere with encrypted file downloads when the inspection process cannot properly handle the encrypted content, requiring either the encrypted file access setting or SSL inspection bypass for affected URLs.

Related Content

- [Advanced Security Controls](#)
- [Cisco Technical Support & Downloads](#)