Troubleshoot Realtime DLP issues with Cisco Secure Access

Contents

Introuduction

This document describes the troubleshooting steps for Inline or Realtime Data Loss Prevention (DLP) issues within the Secure Web Gateway (SWG) environment.

Prerequisites and Warnings

- **HTTPS Inspection:** Ensure HTTPS inspection is enabled. DLP cannot scan encrypted traffic. Make sure website is getting decrypted with Cisco Secure Access Root CA or custom CA.
- **QUIC Protocol:** Disable the QUIC protocol in all browsers. QUIC uses UDP, which bypasses the SWG and prevents DLP scanning.
- **IPv6:** Disable IPv6 if traffic is not hitting the SWG, as dual-stack functionality must cause bypasses.
- **Security Policy:** Ensure that the access rule does not have "Allow – Override Security" or "Isolation" enabled.

Overview

Inline DLP is an extended scanning feature of the SWG. It monitors or blocks the upload of sensitive, confidential, or personally identifiable data in files uploaded via the SWG proxy. Customers create Data Classifications using Cisco-defined identifiers (for example, credit cards or social security numbers) or custom keywords. These classifications are applied to DLP Policies assigned to specific identities and

destinations. The DLP engine scans HTTP POST, PUT, and PATCH methods only.

General Troubleshooting Checklist

If DLP detection is not occurring, verify the outlined steps:

- **Connectivity:** Confirm the client is using the SWG by visiting http://policy.test.sse.cisco.com. Verify that the correct SWG data center is applied and the test result shows "protected by Secure Access."
- **Decryption:** Ensure SSL Decryption is enabled in the Security Profile. Verify there are no Selective Decryption or "Do Not Decrypt" list exclusions.
- **Traffic Steering:** Ensure there is no External Domain Bypass configured in Internet Settings.
- **Identity:** If DLP policies rely on Active Directory groups, confirm the user is a member of the correct group.
- **Application Settings:** Ensure Office 365 Bypass or M365 Compatibility settings are disabled if a Microsoft domain is being used for DLP.
- **Activity Search:** Use *Reporting > Activity Search* to ensure the full URL is visible (decrypted) and the expected identity is associated with the traffic. Check *Reporting > Data Loss Prevention* to confirm if monitor or block activity is logged.
- **Policy Configuration:** Verify the DLP policy is configured for the correct identity and destination application.
- **Testing:** Use a known good destination (for example, pastebin.com or dlptest.com) and a known good sample test string from the Cisco documentation.
- **Support Data:** Gather a HAR file from the user to verify traffic is routed through the SWG and check for SWG headers.

Troubleshoot False Negatives

If DLP is active but a specific classifier fails to trigger, investigate the following areas:

Classifiers, Files, and Strings

- **File Status:** Ensure the file is not encrypted or unscannable. Test with a simple text file.
- **Thresholds:** Check the Threshold and Proximity settings in *Policy > Data Classification*. The classifier may require a higher number of hits or proximity to a custom string.
- **Regex Patterns:** Use an online tool (for example, regexr.com) to visualize patterns. Simplify the pattern to catch a smaller part of the string and expand gradually.

File Labels

- **Compatibility:** File label detection does not work for Confluence or JIRA.
- **Metadata:** Open Document Properties in a Microsoft application. The value must exactly match the Umbrella File label; this is case-sensitive.

- **Encryption:** Label detection does not work for password-protected or encrypted files.

Websites and Destinations

- **Supported Apps:** Review the list of supported applications. For unsupported apps or "All Destinations," only specific mime-types are scanned.
- **Vetted Applications:** Vetted applications (for example, dlptest.com) are scanned more comprehensively. Random websites may only be scanned for file violations.
- **File Names:** The system searches file names only for certain vetted applications.

Troubleshoot False Positives

If DLP matches content unexpectedly, check the classifier name and DLP rule in *Reporting > Data Loss Prevention*. If the detection is legitimate but unwanted, adjust the Thresholds or Proximity settings to refine the policy.

Desktop Application Support

Support for desktop-based applications (for example, Outlook, Teams, or Google Workspace) is provided on a best-effort basis. Effectiveness depends on the message format used during file uploads, which may differ between web-based and desktop versions. For non-vetted applications, there is no assurance that file uploads will be supported.

DLP Classifier Gotchas

- **Credit Card Numbers:** The Luhn algorithm is used for validation. Test only with valid credit card numbers.
- **Person Names:** Requires 2-3 words, and each word must be capitalized.
- **Name Combinations:** A separator string is required between the name and other data (for example, "Viagra - John Smith" matches, but "Viagra John Smith" does not).
- **Date of Birth:** Must be near a keyword or header such as "dob" or "birth date."
- **Objectionable Content:** Certain exception strings prevent this classifier from firing if the text resembles a book or report.
- **Postcode:** Must be within proximity to specific location-related keywords.

Exact Data Matching (EDM)

Before investigating EDM, confirm that general DLP scanning is functional. For EDM-specific issues, check that the "Last Edit" field is current in the dashboard and verify the indexing tool output.

Command Usage:

Run the indexing tool with the `-d` option to generate a bloom filter file (.blm). This command is used to validate the EDM index and troubleshoot why records must be skipped. The `-d` flag instructs the tool to output the diagnostic bloom filter file, which should be shared with support along with a sample file or HAR/web developer tool data.