Configure ESA Anti-Spam Settings to Improve Spam Detection

Contents

[Introduction](#)

[Basic Setup](#)

[Enable SBNP](#)

[SBRS Rationale](#)

Introduction

This document describes how to improve Cisco Email Security Appliance (ESA) anti-spam efficacy and reduce spam that bypasses filtering.

Issue

Spam messages bypass ESA filtering or are not handled as expected by inbound mail policies.

Environment

- Cisco Email Security Appliance (ESA) with Anti-Spam enabled and a valid Anti-Spam feature key.
- Inbound and outbound mail flow configured on separate listeners (recommended for SenderBase settings).
- SenderBase Reputation Score (SBRS) and SenderBase Network Participation (SBNP) available in the deployment.

Resolution

Complete the procedures in these sections to verify Anti-Spam operation, confirm scanning, tune thresholds, and optimize SBRS and mail flow policies.

Cause

- Anti-Spam disabled, missing feature key, or rule updates not current.
- Messages bypass scanning due to allowlists, message filters, or scan-size limits.
- Permissive Host Access Table (HAT) policies or SBRS thresholds.

- Increased spam volume over time.

Setup

Procedure 1: Verify Anti-Spam is enabled

1.- Ensure that all Mail Exchange (MX) records (including lower-priority MX records) relay mail through the ESA.

2.- Verify that the appliance has a valid Anti-Spam feature key.

3.- Ensure that Anti-Spam is enabled for all appropriate incoming mail policies.

Procedure 2: Verify Anti-Spam Rule Updates

Navigate to **Security Services > Anti-Spam** and verify that the most recent rule update time stamps are within the last 2 hours.

Procedure 3: Verify Messages are Scanned by Anti-Spam

1.- Inspect a sample of missed spam messages for the header **X-IronPort-Anti-Spam-Result:**

2.- If the header is missing, complete these checks:

- Verify that no allowlist entries or filters bypass **spam** scanning.
- Verify that messages do not bypass scanning due to the maximum message scan size (default 262144 bytes).
- Review each Host Access Table (HAT) entry and confirm that **spam_check=on** is set for inbound mail flow policies.
- Review message filters and verify that no filters use **skip-spamcheck** unless required.
- Use a recent **spam** example (time, date, recipient) and review mail_logs to confirm that Anti-Spam returned a negative verdict.

Procedure 4: Verify Actions for Spam-positive Messages

Review inbound mail policies and verify that spam-positive and suspected-spam messages are dropped or quarantined in the default policy, and that other policies either inherit the default behavior or intentionally override it.

Procedure 5: Tune Spam Thresholds (Optional)

1.- Reduce the Positive Spam Threshold to 80 (default 90) when false positives are acceptable at the certain threshold.

2.- Reduce the Suspected Spam Threshold to 40 (default 50) when false positives are acceptable at the suspect threshold.

3.- When complaints are limited to a subset of recipients, create a separate mail policy for those recipients with lower thresholds.

Procedure 6: Optimize SBRS settings and HAT Policies

1.- Adjust SBRS ranges for **blocklist** and suspect sender groups based on organizational tolerance for false positives.

2.- When policy requires stricter validation, add **SBRS none** to a suspect sender group that uses a throttled policy.

3.- Set the maximum number of recipients per hour to 5 for the throttled policy.

4.- Optionally create multiple throttled policies with different recipient-per-hour limits for different SBRS ranges.

Procedure 7: Enable Sender Verification for Throttled Mail Flow

1.- When policy requires stricter validation, add senders with non-existent or improperly configured Domain Name System (DNS) to a suspect sender group.

2.- Consider a separate mail flow policy that returns a custom 4xx response indicating why messages are rejected.

Procedure 8: Enable LDAP accept and Directory Harvest Attack Protection

1.- Enable Lightweight Directory Access Protocol (LDAP) accept to reduce spam sent to invalid recipients.

2.- If LDAP accept is enabled, configure Directory Harvest Attack Protection (DHAP) for each inbound listener with maximum invalid attempts between 5 and 10 per IP.

Procedure 9: Enable Content Dictionaries (Optional)

The ESA includes two content dictionaries: profanity.txt and sexual_content.txt. Apply these dictionaries only where required because they can increase false positives.

Procedure 10: Report Misclassified Messages

Submit false positives and false negatives to Cisco TAC for analysis.

Procedure 11: Disable SBRS for Outbound Scanning

Enable SBNP

1.- Ensure that inbound and outbound mail are on separate listeners.

2.- Disable SenderBase lookups for outbound email. **Navigate to Network > Listeners**. **Select** the outbound listener. **Click Advanced**. **Clear** the **Use SenderBase IP profiling** check box.

SenderBase Network Participation (SBNP) can increase the effectiveness of reputation filters, Anti-Spam, and Virus Outbreak Filters. SBNP has no noticeable performance impact when Anti-Spam is enabled and is secure.



Note: The volume of spam that your organization receives changes over time. It is possible that more spam gets through the ESAs simply because the organization receives more spam than in the past. Track this behavior over time by looking at the Incoming **Mail Overview** page and adding the **stopped by reputation filtering** and **spam messages detected** line items.

SBRS Rationale

The primary concern with false positives is that important email can be lost. In this context, quarantining or dropping spam-positive email can be problematic. If a legitimate email is sent to a quarantine or a spam folder, it requires a proactive search to identify that legitimate email was misclassified as spam.

In contrast, blocklist and rate-limited emails are blocked in such a way that the sender is notified immediately. If this sender is not a spammer, the sender likely finds another way to make contact. In fact, as an overall policy, blocking by default and then accepting trusted partners on request, is a better position for some businesses.

Throttling, if set properly, rarely if ever affects partners, but provides protection from domains that get infected with viruses. Throttling also is off-putting to spammers. A known spammer technique is to purchase large numbers of IPs, generate enough good email to get a decent SBRS score, and then start sending spam. A larger suspect list range catches the spam, limit the damage they do and it can eventually cause them to stop sending spam to your domain.

Related Content

- How are SenderBase Reputation Scores (SBRS) determined, and what do they mean?