# Cisco Email Security Appliance (ESA) Anti-Spam Efficacy Checklist

## Contents

[Introduction](#)
[Basic Setup](#)
[Enable SBNP](#)
[SBRS Rationale](#)

## Introduction

The following procedures and recommendations are "best practices" for reducing the amount of spam getting through the ESA. Note that every customer is different and that some of these recommendations may increase the number of legitimate emails classified as spam (false positives).

## Basic Setup

1. Make sure Anti-Spam is turned on:

   Check to make sure that all your MX records (including lower priority) MX records are relaying mail through ESAs.Make sure your appliances have a valid Anti-Spam feature key.Ensure Anti-Spam is enabled for all appropriate incoming mail policies.

2. Verify that you are receiving anti-spam rule updates. Check to confirm that the **most recent** time stamps for updates under Security Services > Anti-Spam are from within the last 2 hours.

3. Make sure that messages are being scanned by Anti-Spam:

   Check a sample of missed spam messages for the following header: X-IronPort-Anti-Spam-Result:If that header is missing:

   Check to make sure you do not have any allowlist entries or filters causing spam to bypass spam scanning (see below).Check to make sure that messages are not bypassing scanning because they exceed the maximum messages scan size (default is 262144 bytes). Reducing this setting does not greatly improve performance and can result in missed SPAM. During an evaluation, it's also important to make sure the IPAS setting is the same as any other products being tested.Go through each HAT entry and confirm that "spam_check=on" for all inbound mail flow policies. As long as the default has "spam_check= on", and none of the mail flow policies explicitly turn it off, this is configured properly. Pay special attention to the TRUSTED/allowLIST settings. Often times customers inadvertently add a sender to their allowlist that is forwarding spam - for example, by adding the domain of an ISP or partner that forwards both spam and legitimate email to the allowLIST sender group.

Do a quick check through the message filters to make sure there are not any filters that "skip-spamcheck". If there are, make sure they are doing what they should (keeping in mind that matching a single rcpt-to can match on messages with 30+ recipients).

Find a recent SPAM example (time, date, rcpt, etc.), and reference the mail_logs to see what happened. Confirm that Anti-Spam returned a negative verdict.

4. Make sure you are taking the desired actions on spam positive messages. Check the Inbound Mail Policies for how Anti-Spam verdicts are handled. Make sure SPAM positive and suspect messages are dropped or quarantined in the default policy, and that all other policies either use the default behavior or deliberately override the default.

5. Apply more aggressive spam thresholds if false-positives are less of a concern than missed spam:

   Reduce the Positive Spam Threshold to 80 (default is 90) if false-positives are not a concern at the 'certain' threshold.

   Reduce Suspected Spam Threshold to 40 (default is 50) if false-positives are not a concern at the 'suspect' threshold.

   If most of your spam complaints are coming from a subset of recipients, you can create a separate mail policy for these users with lower spam thresholds in order to filter more aggressively for just these recipients.

   Changes to these values should not be taken lightly, nor should they be enacted without any hard data to ascertain what the repurcussive effects will be.

   Also, do not necessarily adjust values in the other direction only to avoid False Positives.Please make sure that False Positives and False Negatives are submitted to TAC.

6. Optimize your SBRS settings and HAT Policies:

   Most organizations are comfortable adding SBRS -10 to -3.0 to their Blocklist and SBRS -3.0 to -1.0 to their SUSPECTLIST. More aggressive customers can blocklist SBRS -10 to -2.0 and add -2.0 to -0.6 to the SUSPECTLIST.

   In some cases, the fact that a sender does not yet have a SenderBase Reputation Score is evidence that this sender may be a spammer. You can add SBRS "none" directly to a sender group that gets the "Throttled" policy, for example to your SUSPECT sender group.

   Change the max number of recipients per hour to 5 for the "Throttled" policy.

   Consider creating more than one "Throttled" policy to enforce different recipient per hour limits - for example rate limiting senders with an SBRS between -2 and -1 to 5 recipients per hour and senders with an SBRS between -1 and 0 to 20 recipients per hour.

7. Enable Sender Verification for the "Throttled" Mailflow policy:

   Customers may choose to add senders with non-existent or improperly configured DNS to the SUSPECTLIST sender group.

   Connecting host PTR record does not exist in DNS.Connecting host PTR record lookup fails due to temporary DNS failure.

   Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A).

   There is some risk of false-positives from senders with mis-configured DNS, so customers may want to setup a separate Mailflow policy that returns a custom 4xx response indicating the reason messages are rejected.

   Check the Online Help or AsyncOS User Guide  for more information about sender verification

8. Enable LDAP accept and Directory Harvest Attack Protection:

   Many spammers send emails to a high number of invalid addresses, so blocking senders who send to invalid recipients can also decrease spam.

   If LDAP accept is already on, make sure Directory Harvest Protection (DHAP) is also configured for each inbound listener with maximum invalid attempts between 5 and 10 per IP.

9. Enable content dictionaries:

   Your ESA comes with two content dictionaries: profanity.txt and sexual_content.txt. While using these dictionaries may generate false positives, some customers have found that filtering their mail stream for inappropriate words may reduce the risk of the "wrong person" getting the "wrong email". These filters may only be applied to the "squeaky wheels" by enabling them for a group of users in a specific mail policy.

10. Report mis-classified messages to Cisco TAC.

11. To prevent a large number of false positives, SBRS should be disabled for outbound scanning. This is because SBRS looks at the reputation of incoming IPs, and in an internal network, most of these IPs are dynamic. Follow the steps in the next section.

## Enable SBNP

1. Make sure inbound and outbound mail are on separate listeners.

2. Disable SenderBase lookups for outbound email per below. To do this from the GUI, go to Network > Listeners, select any outbound listeners, choose "Advanced" and uncheck the box next to "Use SenderBase IP profiling".

SenderBase Network Participation (SBNP) can significantly increase the effectiveness of Reputation Filters, Anti-Spam and Virus Outbreak Filters. SBNP also has no noticeable performance impact if enabled when using Anti-Spam and is highly secure.

**Note**: The volume of spam that your organization receives will change over time. It is possible that more spam is getting through the ESAs simply due to the fact that you are receiving more spam than in the past. You can 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 big concern with False Positives is that important email could get lost. In this context, the practice of Quarantining or Dropping SPAM Positive email is problematic. If a legitimate email is sent to a Quarantine or a spam folder, it requires a proactive search to go in and "notice" that ham 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, they will likely find another way to make contact with you. 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, should rarely if ever affect partners, but will provide protection from domains that get infected with viruses. Throttling will also be off-putting to spammers. We are aware of a spammer technique to purchase large numbers of IP's, generate enough "good" email to get a decent SBRS score and then start spamming. A larger suspect list range should catch these, limit the damage they do and it may eventually cause them to stop sending spam to your domain.