Troubleshoot Common Email Security Appliance Errors

Contents

[Introduction](#)

[What are the common configuration errors on the ESA?](#)

[HAT](#)

[Policy](#)

[Incoming relays](#)

[DNS](#)

Introduction

This document describes common configuration errors on the Cisco Email Security Appliance (ESA).

Environment

- **Product**:Cisco Email Security Appliance (ESA)
- **Software**:AsyncOS for ESA (version varies by deployment)
- **Scope**: Apply this guidance to inbound and outbound mail policies as applicable; review each section before making changes.

Prerequisites

- Administrative access to the ESA (GUI or CLI)
- Ability to review mail logs and message tracking for validation
- Reputation services SenderBase Reputation Score SBRS enabled if using SBRS-based sender groups
- Awareness that the Host Access Table (HAT) classifies connecting hosts before mail policy evaluation, which affects how later controls apply

General Verification

- Use **Monitor > Overview** and message tracking to confirm expected sender group classification, policy matches, and delivery outcomes after changes. Success means the expected sender group, policy, and delivery result appear after the change.
- Monitor quarantines and false positives for 7–144 days after tightening reputation or filtering settings, and adjust for known business partners as needed.

Common Configuration Errors on the Email Security Appliance ESA)

Use these checks to identify and correct common configuration errors on the Email Security Appliance ESA). Each subsection uses a consistent issue, cause, resolution, and verify pattern so the problem can be diagnosed and corrected quickly.

Host Access Table (HAT)

Symptoms

- Spam is accepted due to overly permissive reputation-based sender groups.
- Legitimate mail is throttled or blocked due to overly strict connection controls.

Cause

- Sender groups are configured with inappropriate SenderBase Reputation Score (SBRS) ranges or Domain Name System (DNS) verification settings.

Resolution

1. Do not add positive SBRS values (for example, +5 or +7) to the allow list. For SBRS-based allow lists, use only scores from 9.0 to 10.0, and validate with message tracking.
2. Configure the unknown senders list andDNS verification features only when required. If not required, disable **UNKNOWNLIST**, **Envelope SenderDNS Verification**, and **Connecting HostDNS Verification**.



Note: The ESA user interface uses the legacy termUNKNOWNLIST for the unknown senders list.

---

3. To avoid inconsistent per-policy settings, configure global defaults: choose **Mail Policies > Mail Flow Policies > Default Policy Parameters** and set message size and other default parameters there.
4. Set a reasonable default maximum connections value for most senders (for example, 3) and apply it as the default for new mail flow policies; adjust for known high-volume senders as needed.
5. Configure the block list SBRS range based on your risk tolerance. In many deployments, blocking SBRS -10.0 to -2.0 can result in low false-positive rates. Validate with message tracking and adjust for business partners.

Policy

Symptom/Impact

- Mail is scanned or quarantined unexpectedly because non-default mail policies override global defaults.
- Outbound mail triggers unnecessary Anti-Spam/Outbreak Filter actions, increasing processing time and false positives.
- Messages appear blank because infected attachments are stripped and the message body contains only the removed content.

Cause

- Non-default policies duplicate or override default Anti-Spam, Anti-Virus, Content Filter, or Outbreak Filter settings without a specific requirement.
- Outbound policies apply inbound-focused scanning features.

Resolution

1. Name mail policies for the recipients they apply to (for example, **Inbound_Executives**) and name content filters for the action they take (for example, **Q_basic_attachments** and **Dspooferss**).
2. For non-default policies, select **Use Default Settings** for Anti-Spam, Anti-Virus, Content Filters, and Outbreak Filters unless a documented exception is required.
3. Clear the check box for **Drop infected attachments** to avoid delivering messages with stripped content that can appear blank.
4. For outbound Anti-Virus actions, notify the sender instead of the recipient.
5. Disable Outbreak Filters and Anti-Spam on outbound mail policies unless an explicit outbound use case exists.

Verify

- Use message tracking to confirm the intended mail policy is matched and that default scanning settings are inherited where expected.
- Send a controlled outbound test message and confirm Anti-Spam/Outbreak Filters are not applied unless configured by exception.

Incoming relays

Symptoms

- Internal mail servers are treated as external senders, which can cause unexpected throttling, filtering, or reputation-based actions.

Cause

- Internal mail server IP addresses or networks are not configured as incoming relays, or the Incoming Relay feature is disabled.
- The internal relay hosts are not classified in a dedicated HAT sender group, which can result in unintended connection limits or Directory Harvest Attack Prevention (DHAP) behavior.

Resolution

1. In the GUI, choose **Mail Policies > Incoming Relays**, and add your internal mail server IP addresses or networks.
2. Ensure the Incoming Relay feature is enabled (do not only add entries to the table).
3. Create a dedicated Host Access Table (HAT) sender group for internal relays listed in the allow list in the preceding list for reporting purposes. Configure no rate limiting and no **Directory Harvest Attack Prevention (DHAP)** if appropriate, while keeping Anti-Spam and Anti-Virus scanning enabled as required.DHAP limits invalid recipient enumeration attempts during the Simple Mail Transfer Protocol (SMTP) conversation.
4. If you drop mail based on reputation for non-relayed traffic, add a message filter that applies equivalent handling to relayed mail where required. Example:

```
Drop_Low_Reputation_Relayed_Mail:
if reputation <= -2.0
{ drop(); }
```

Verify

- In **Monitor > Overview**, confirm internal servers no longer appear as untrusted external senders.
- In message tracking/mail logs, confirm the expected sender group is applied (for example, an internal relays sender group).



Note: If mail is re-injected (for example, inter-subscriber mail is re-processed through inbound policy), exempt thereinjectionn interface in the filter as needed.Reinjectionn sends a message back through policy evaluation, so filters can match the same message again unless the interface is excluded.

DNS

Symptoms

- DNS resolver selection or split: DNS configuration causes delivery failures, slowSMTP transactions, or failed reputationDNS-based checks.

Environment

- Applies to deployments that require public DNS resolution, internal-onlyDNS resolution, or split-horizonDNS for internal domains and services.

Symptoms

- Message tracking shows DNSlookup failures/timeouts for MX, AAA,PTRR, or reputation-related queries.
- Mail delivery is delayed due to repeatedDNS retries.

Cause

- ESA is configured to use resolvers that cannot resolve required public records, required internal records, or both.
- Split-horizonDNS, which returns different answers for the same domain based on the source network, is required but not implemented for internal domains or services.

Resolution

Configure Domain Name System (DNS) resolution based on where the ESA resolves records: the public Internet, internal-only domains, or both:

1. Use public recursive resolvers when the ESA primarily needs public DNS records and policy allows it.

2. Use internalDNS or split-horizon DNS when the ESA must resolve internal-only zones, internal mail exchange MXX) records, Lightweight Directory Access Protocol LDAPP) records, or other private services.

3. Public DNS is appropriate when the appliance mainly resolves Internet mail records and no internal-only zones or policy restrictions apply.

Use InternalDNS or splitDNS when Required

- Internal-only domains
- InternalMXX records
- Split-horizonDNS (different answers for the same domain based on the source network)
- Compliance or security policy requires internal recursive resolvers
- PrivateDNS zones required for routing
- PrivateDNS zones required for Lightweight Directory Access Protocol LDAPP)
- PrivateDNS zones required for internal services used by the ESA

Verify

- Confirm the ESA can resolve required public and internalhostnamess (as applicable) and that mail delivery and reputationDNS-based checks succeed in message tracking.

Message and Content Filters

The most common error is to add matching conditions in filters when they are not required.

- **Blank conditions:** Leave the condition blank when the filter must run for every message in a given mail policy.
- **Evaluation behavior:** In asyncOS message filters, a blank condition evaluates to *true*, so the filter runs on every message that reaches it.
- **Scope:** Control scope by attaching the filter to the appropriate Incoming or Outgoing Mail Policy.
- **Order:** Message filters evaluate message attributes and actions in sequence. Content filters are typically scoped by the mail policy that calls them.

Examples:

- Using the **rcpt-to** condition in a message filter is usually unnecessary when the goal is to target a specific user or group. Prefer a recipient-based Incoming Mail Policy and apply the content filter to that policy when the requirement maps cleanly to recipients or recipient groups. Reserve **rcpt-to** conditions for exceptions where policy matching cannot express the requirement.
- Testing for the presence of an attachment before dropping it is usually redundant when the intent is to block a specific attachment type. Configure the filter to drop the targeted attachment type directly; use an attachment-presence test only when different actions are required depending on whether an attachment exists.
- Use **deliver()** only when the message must bypass remaining filters. The **deliver()** action stops further filter processing and then delivers the message; to deliver mail without skipping remaining filters, do not configure an explicit **deliver()** action (implicit delivery applies).

Open Relay Prevention

Symptom/Impact

- Third-party relay tests report that the appliance accepts malformed or dangerous recipient addresses.
- Publicblocklists list the sendingIPP because SMTP address parsing allows patterns commonly used to validate open relays.

Cause

- Simple Mail Transfer Protocol SMTP address parsing and character handling allow invalid address

formats (for example, double **@** signs) or address literals, which are IP addresses written directly in the address instead of a domain name.

Resolution

Some services test whether the Message Transfer Agent (MTA) accepts malformed addresses that can indicate an open relay condition. Configure strict parsing and rejection behavior so the ESA rejects these addresses during the SMTP conversation.

- Add a dedicated HAT sender group for relay-test sources preceding **ALLOWLIST** for reporting. Configure no rate limiting and no Directory Harvest Attack Prevention DHAP) if appropriate, while keeping Anti-Spam and Anti-Virus enabled as required.
- Enable **Strict Address Parsing** (Loose is the default) to prevent double **@** signs in addresses.
- Reject (do not strip) invalid characters to prevent acceptance of malformed addresses.
- Reject (do not accept) address literals, and enter these characters: ***%!****?**

Verify

- Run an external relay test and confirm the ESA rejects malformed recipient addresses during the SMTP conversation.
- Use message tracking to confirm the relay-test sender group is matched and that mail is processed with the intended scanning settings.

Related Information

- Get Technical Support and Documentation
- ReviewAsyncOSS forESA User Guides
- Email Security Appliance ESA) installation and configuration guides (HAT, mail policies, and message filters)