Troubleshoot Common HAT/RAT Errors on ESA

Contents

Introduction

This document describes a high-level overview, configuration guidance, and troubleshooting techniques to diagnose common issues for the Host Access Table (HAT) and Recipient Access Table (RAT) on the Email Security Appliance (ESA).

Overview

HAT

For every configured listener, you must define a set of rules that control incoming connections from remote hosts. For example, you can define remote hosts and whether or not they can connect to the listener. AsyncOS allows you to define which hosts are allowed to connect to the listener using the HAT.

The HAT maintains a set of rules that control incoming connections from remote hosts for a listener. Every configured listener has its own independent HAT. You can configure HATs for both public and private listeners.

By default, the HAT is defined to take different actions depending on the listener type:

- Public listener: The HAT is set up to accept emails from all hosts.
- Private listener: The HAT is configured to relay email from the host(s) you specify, and reject all other hosts.

A HAT rule consists of a Sender Group, SenderBase Reputation Score (SBRS), External Threat Feed Sources applied, and Mail Flow Policy.

Sender Group

A sender group is a list of senders identified by one or more of these:

- IP Address (IPv4 or IPv6)
- IP Range
- Specific host or domain name
- IP Reputation Service 'organization' classification
- IP Reputation Score (IPRS) range (or lack of score)
- DNS list query response

SenderBase Reputation Score

The appliance can query the IP reputation service to determine an IP reputation score. The IP reputation score is a numeric value assigned to an IP address, domain, or organization based on information from the IP reputation service.

External Threat Feed (ETF) Sources Applied

The ETFs framework allows the ESA to consume external threat information in STIX format communicated over the TAXII protocol.

The ability to consume external threat information helps an organization to:

- Proactively respond to cyber threats such as malware, ransomware, phishing attacks, and targeted attacks.
- Subscribe to local and third-party threat intelligence sources.
- Improve efficacy.

You need a valid feature key to utilize ETF on your ESA. For information on how to obtain a feature key, contact your Cisco Sales Representative and/or Cisco Global Licensing Operations.

Mail Flow Policy

Mail Flow Policies allow you to control or limit the flow of email messages from a sender to the listener during the SMTP conversation. You control SMTP conversations by defining these types of parameters in the Mail Flow Policy:

- Connection parameters (for example, maximum number of messages per connection)
- Rate limiting parameters (for example, maximum number of recipients per hour)
- Custom SMTP codes and responses are communicated during the SMTP conversation
- Enable/disable Anti-Spam detection
- Enable/disable Anti-Virus protection
- Encryption (for example, TLS)
- Authentication and verification (for example, DMARC, DKIM, and SPF)

RAT

AsyncOS uses the RAT for each public listener to manage the acceptance or rejection of recipient addresses. Recipient addresses include these:

- Domains
- Email addresses
- Groups of email addresses

By default, the RAT rejects all recipients to prevent the creation of an open relay.

Common Implementation Scenarios

Blocking a Sender Manually

In order to block a specific sender by sender IP address, add a manual entry for the IP address under the blocklist sender group and ensure that the action is set to 'Reject' or 'TCP Refuse'. For configuration instructions, refer to: Block a Sender IP Manually on ESA.

Adding Groups/Ranges of IP Addresses into the HAT

Adjacent IP addresses can be grouped as subnets such as 192.0.2.0/24, IP address ranges such as 192.0.2.10-20, or partial IP addresses such as 192.0.2. and added to the table. In order to add multiple nonadjacent IP addresses, observe these steps:

From the GUI:

1. Navigate to **Mail Policies > HAT Overview** (if necessary, choose the appropriate cluster level).
2. Choose the **Sender Group** to modify and choose **Add Sender**.
3. In the **Sender** field, enter the applicable IP ranges (for example, 192.0.2.0/24), an optional comment, and choose **Submit**.
4. Click **Commit Changes** to save.

From the CLI:

1. Run the command sequence:

   <#root>

   listenerconfig >> EDIT

2. Enter the name or number of the listener to edit.
3. Run the command sequence and then enter the sender group number or name to edit:

   HOSTACCESS >> EDIT >> 1

4. Choose **new** and enter a comma-separated list of senders to add.
5. When complete, run **commit** to save the changes.

Troubleshooting

Sender Matching Incorrect Sender Group

Verify the mail logs on the ESA or message tracking on the Security Management Appliance (SMA), and check for these entries in the Incoming Connection ID (ICID):

```
ICID 476946 ACCEPT SG WhiteList match nx.example SBRS None country United States
```

Reason: Connecting Host DNS Verification is enabled on the sender group, and connecting host PTR record does not exist in DNS is selected.

```
ICID 476946 ACCEPT SG WhiteList match not.double.verified.example SBRS None country United States
```

Reason: Connecting Host DNS Verification is enabled on the sender group, and connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A) is chosen.

```
ICID 476946 ACCEPT SG WhiteList match serv.fail.example SBRS None country United States
```

Reason: Connecting Host DNS Verification is enabled on the sender group, and connecting host PTR record lookup fails due to temporary DNS failure is selected.

Incorrect Sender Group Host Configuration

A sender group is a list of senders identified by:

- IP Address (IPv4 or IPv6)
- IP Range
- Specific host or domain name
- IP Reputation Service 'organization' classification
- IP Reputation Score (IPRS) range (or lack of score)
- DNS List query response

Sample of misconfigured addresses under Sender Group: ESA Sender Group Matching Partial Hostnames.

Do HAT/RAT rejections count against 'Stopped by Reputation Filtering'?

Yes, messages rejected by a sender group with the reject action in the Mail Flow Policy are counted in the 'Stopped by Reputation Filtering' report counter.

Note: This counter can include HAT policy rejections and SBRS-based rejections. Verify the rejection reason in the mail logs to distinguish the source.

Verifying Rejects by RAT Table

This is example log output from the mail logs on an ESA:

```
Thu Sep 18 09:10:14 2014 Info: MID 48445 ICID 15970 To: <user@example.com> "Rejected by RAT"
```

Reason: The specific domain is not allowed under the RAT in the ESA configuration.

How to log additional sender/recipient information for rejected connections?

By default, a rejected connection logs only the sender MTA IP address in the mail logs, and does not log the envelope sender or envelope recipient. If additional logging is required for troubleshooting, delayed HAT reject can be enabled on AsyncOS.

⚠ **Caution**: Cisco recommends that you do not enable this feature permanently because it requires additional resources.

More details can be found here: HAT Delayed Rejection FAQ.

Related Information

- Cisco Email Security Appliance - End-User Guides
- Cisco Technical Support & Downloads