Understand Parameters Related to Mail Flow Policies and Destination Controls

Contents

Introduction

This document describes a couple of configuration aspects of the Email Security Appliance (ESA) on how to Throttle/Rate-Limit Senders and Delivery. The features that will be described in the article are Mail Flow Policies and Destination Controls.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding of Mail Flow Policies and Destination Controls
- Familiarity with the usage of these features in the ESA's config

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Advantages of Mail Flow Policies and Destination Controls

There is one very important function that both these features have, and that's Rate Limiting/Throttling. This aspect helps the admin have control on which traffic should be free-flowing and which to be allowed with restrictions.

Mail Flow Policies

These are the policies that apply to the Sender Groups of the ESA, on the basis of which email traffic modulation is done.

Mail Flow Policies always applies to traffic which is Incoming to the ESA irrespective of the email being an Inbound or Outbound one.

The Mail Flow Policies works in the backend with regards to the selected Connection Behavior for that policy. The different Connection Behavior available in ESAs are:

1. Accept
2. Reject
3. Relay
4. TCP Refuse
5. Continue

Accept: Connection is accepted, and email acceptance is then further restricted by listener settings, including the Recipient Access Table (for public listeners). This connection behavior treats an email as Inbound one

Reject: The client attempting to connect gets a 4XX or 5XX SMTP status code. No email is accepted. This is mainly used for Blacklisting senders

Relay: Connection is accepted. Receiving for any recipient is allowed and is not constrained by the Recipient Access Table. This treats an email as an Outbound one

TCP Refuse: Connection is refused at the TCP level.

Continue: The mapping in the HAT is ignored, and processing of the HAT continues. If the incoming connection matches a later entry that is not CONTINUE, that entry is used instead. The CONTINUE rule is used to facilitate the editing of the HAT in the GUI.

Components of a Mail Flow Policy

Max. Messages Per Connection: The maximum number of messages that can be sent through this listener per connection from a remote host. Each ICID depicts one connection

Max. Recipients Per Message: The maximum number of recipients per message that will be accepted from this host that's processed using this Mail Flow Policy

Max. Message Size: The maximum size of a message that will be accepted by this listener tagged to the Mail Flow Policy. The smallest possible maximum message size is 1 kilobyte.

Max. Concurrent Connections From a Single IP: The maximum number of concurrent connections allowed to connect to this listener from a single IP address.

Custom SMTP Banner Code: The SMTP code returned when a connection is established with this listener.

Custom SMTP Banner Text: The SMTP banner text returned when a connection is established with this listener. You can use some variables in this field.

Override SMTP Banner Hostname: By default, the appliance will include the hostname associated with the interface of the listener when displaying the SMTP banner to remote hosts (for example, 220-hostname ESMTP). You may choose to override this banner by entering a different hostname here. Additionally, you may leave the hostname field blank to choose *not* to display a hostname in the banner.

Mail Flow Limits

Max. Recipients Per Hour: The maximum number of recipients per hour this listener will receive from a remote host. The number of recipients per sender IP address is tracked globally. Each listener tracks its own rate limiting threshold, however, because all listeners validate against a single counter, it is more likely that the rate limit will be exceeded if the same IP address (sender) is connecting to multiple listeners. You can use some variables in this field.

Max. Recipients Per Hour Code: The SMTP code returned when a host exceeds the maximum number of recipients per hour defined for this listener.

Max. Recipients Per Hour Text: The SMTP banner text returned when a host exceeds the maximum number of recipients per hour defined for this listener.

Rate Limit for Envelope Senders

Max. Recipients Per Time Interval: The maximum number of recipients during a specified time period that this listener will receive from a unique envelope sender, based on the mail-from address. The number of recipients is tracked globally. Each listener tracks its own rate limiting threshold; however, because all listeners validate against a single counter, it is more likely that the rate limit will be exceeded if messages from the same mail-from address are received by multiple listeners.

Sender Rate Limit Error Code: The SMTP code returned when an envelope exceeds the maximum number of recipients for the time interval defined for this listener.

Sender Rate Limit Error Text: The SMTP banner text returned when an envelope sender exceeds the maximum number of recipients for the time interval defined for this listener.

Exceptions: If you want certain envelope senders to be exempt from the defined rate limit, select an address list that contains the envelope senders.

The address list is defined from Mail Policies à Address List (Full email addresses, Domains, IP

Addresses can be used for exemptions)

Use SenderBase for Flow Control: Enable “lookups” to the SenderBase Reputation Service for this listener.

Group by Similarity of IP Addresses: Used to track and rate limit incoming mail on a per-IP address basis while managing entries in a listener’s Host Access Table (HAT) in large CIDR blocks. You define a range of significant bits (from 0 to 32) by which to group similar IP addresses for the purposes of rate-limiting, while still maintaining an individual counter for each IP address within that range.

NOTE: Requires “Use SenderBase” to be disabled.

Directory Harvest Attack Prevention (DHAP)

Max. Invalid Recipients Per Hour: The maximum number of invalid recipients per hour this listener will receive from a remote host. This threshold represents the total number of RAT rejections and SMTP call-ahead server rejections combined with the total number of messages to invalid LDAP recipients dropped in the SMTP conversation or bounced in the work queue (as configured in the LDAP accept settings on the associated listener).

Drop Connection if DHAP threshold is Reached within an SMTP Conversation:

The appliance will drop a connection to a host if the threshold of invalid recipients is reached.

Max. Invalid Recipients Per Hour Code: Specify the code to use when dropping connections. The default code is 550.

Max. Invalid Recipients Per Hour Text: Specify the text to use for dropped connections. The default text is “Too many invalid recipients.

Security Features

Spam / AMP / Virus / Sender Domain Reputation Verification / Outbreak Filters / Advanced Phishing Protection / Graymail / Content & Message Filters : The Security Engines / Scanning and filters’ related scanning can be enabled or disabled from here

Encryption and Authentication: We can modify settings as Off, Prefer, or Require Transport Layer Security (TLS) in SMTP conversations for this listener.

The Verify Client Certificate option directs the Email Security appliance to establish a TLS connection to the user’s mail application if the client certificate is valid.

For the TLS Preferred, the appliance still allows a non-TLS connection if the user doesn’t have a certificate, but rejects a connection if the user has an invalid certificate.

For the TLS Required setting, selecting this option requires the user to have a valid certificate in order for the appliance to allow the connection.

SMTP Authentication: Allows, disallow, or requires SMTP Authentication from remote hosts

connecting to the listener

If Both TLS and SMTP Authentication are enabled : Require TLS To Offer SMTP Authentication

Domain Key/DKIM Signing: Enable Domain Keys or DKIM signing on this listener

DKIM Verification : Enable DKIM verification.

S/MIME Decryption/Verification: Enable S/MIME decryption or verification.

Signature After Processing: Choose whether to retain or remove the digital signature from the messages after S/MIME verification.

S/MIME Public Key Harvesting: Enable S/MIME public key harvesting.

Harvest Certificates on Verification Failure : Choose whether to harvest public keys if the verification of the incoming signed messages fail.

Store Updated Certificate: Choose whether to harvest updated public keys

SPF/SIDF Verification: Enable SPF/SIDF signing on this listener.

Conformance Level : Set the SPF/SIDF conformance level. You can choose from SPF, SIDF or SIDF Compatible

Downgrade PRA verification result if 'Resent-Sender:' or 'Resent-From:' were used: If you choose a conformance level of SIDF compatible, configure whether you want to downgrade Pass result of the PRA Identity verification to None if there are Resent-Sender: or Resent-From: headers present in the message

HELO Test: Configure whether you want to perform a test against the HELO identity (Use this for SPF and SIDF Compatible conformance levels)

DMARC Verification: Enable DMARC verification on this listener

Use DMARC Verification Profile: Select the DMARC verification profile that you want to use on this listener. The same is created from Mail Policies --> DMARC --> Add Profile

DMARC Feedback Reports: Enable sending of DMARC aggregate feedback reports.

Bounce Verification

Consider Untagged Bounces to be Valid: Applies only if bounce verification tagging is enabled. By default, the appliance considers untagged bounces invalid and either rejects the bounce or adds a custom header, depending on the Bounce Verification settings. If you choose to consider untagged bounces to be valid, the appliance accepts the bounce message.

Sender Verification

Envelope Sender DNS Verification:

Senders can be unverified for different reasons. Unverified senders are classified into the following categories:

- Connecting host PTR record does not exist in the 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).

We can enable or disable the Sender Verification feature.

Use Sender Verification Exception Table: We can use the sender verification domain exception table to allow exemptions. We can only have one exception table, but can be enable per mail flow policy.

The Exception table can be created from Mail Policies --> Sender Verification Exception Table --> Add Sender Verification Exception

Destination Controls

This is a feature that controls the email deliveries. All emails that finish processing via the ESAs, and are about to exit the ESAs for further deliveries can be controlled by the Destination Controls feature.

The **Default** Destination Controls profile applies to all deliveries. Just in case, there's a need for domain-specific delivery controls then we have to create customized Destination Controls profile.

Components of a Destination Controls Profile

Limits

Concurrent connections : Number of simultaneous connections (DCIDs) to remote hosts the appliance will attempt to open for completing delivery.

Maximum Messages Per Connection: Number of messages the ESA will send to a destination domain over a connection (DCID) before the appliance initiates a new connection.

Recipients: Number of recipients the appliance will send to a given remote host in a given time period.

Apply limits: This aspects helps decide on how to apply the limits we have specified on a per-destination and per MGA hostname basis.

TLS Support

This helps to decide whether TLS connections to remote hosts will be set to None / Preferred / Required

DANE Support: If you configure DANE as 'Opportunistic' and the remote host does not support DANE, opportunistic TLS is preferred for encrypting SMTP conversations.

If you configure DANE as 'Mandatory' and the remote host does not support DANE, no connection

is established to the destination host.

If you configure DANE as 'Mandatory' or 'Opportunistic' and the remote host supports DANE, it is preferred for encrypting SMTP conversations.

NOTE: DANE will not be enforced for domains that have SMTP Routes configured.

Bounce Verification

This helps to decide whether or not to perform envelope sender address tagging (prvs-xxxxxx-xxxx) via Bounce Verification.

Bounce Verification can be configured from Mail Policies --> Bounce Verification --> Add New Key

Bounce Profile

The bounce profile can be used by the appliance for a given remote host. It decides how long will an email be retained in the Delivery Queue of the ESA if there are delivery issues, prior to Hard Bouncing an email

The bounce profile is set via the Network --> Bounce Profiles

Global Settings

Certificate: This is the aspect where we define the certificates that are to be used when establishing SSL/TLS connections while initiating email deliveries to the next hop. It's always recommended to use a Certificate Authority (CA) signed certificate in this aspect.

Send an alert when a required TLS connection fails: We can specify whether the appliance sends an alert if the TLS negotiation fails when delivering messages to a domain that requires a TLS connection. The alert message contains the name of the destination domain for the failed TLS negotiation. The appliance sends the alert message to all recipients set to receive **Warning** severity level alerts for **System alert** types.

We can manage alert recipients via the System Administration --> Alerts