Defining Which Hosts Are Allowed to Connect Using the Host Access Table

This chapter contains the following sections:

Overview of Defining Which Hosts Are Allowed to Connect

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 Host Access Table (HAT).

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

To control incoming connections from remote hosts, you define the following information:

- **Remote hosts.** Define the way in which a remote host attempts to connect to the listener. You group remote host definitions into *sender groups* . For example, you can define multiple remote hosts in a sender group by IP address and partial hostname. You can also define remote hosts by their IP Reputation score. For more information, see Defining Remote Hosts into Sender Groups, on page 2.
- **Access rules.** You can define whether the defined remote hosts in the sender group are allowed to connect to the listener and under what conditions. You define access rules using *mail flow policies* . For example, you can define that a particular sender group is allowed to connect to the listener, but only allow a maximum number of messages per connection. For more information, see Defining Access Rules for Email Senders Using Mail Flow Policies, on page 7

Define which hosts are allowed to connect to the listener on the Mail Policies > HAT Overview page.

When a listener receives a TCP connection, it compares the source IP address against the configured sender groups. It evaluates the sender groups in the order listed on the HAT Overview page. When it finds a match, it applies the configured mail flow policy to the connection. If you have configured multiple conditions within a sender group, that sender group is matched if any of the conditions match.

When you create a listener, AsyncOS creates predefined sender groups and mail flow polices for the listener. You can edit the predefined sender groups and mail flow policies, and create new sender groups and mail flow policies. For more information, see Understanding Predefined Sender Groups and Mail Flow Policies, on page 10.

You can export all information stored in a Host Access Table to a file, and you can import Host Access Table information stored in a file into the email gateway for a listener, overriding all configured Host Access Table information. For more information, see Working with the Host Access Table Configuration, on page 21.

Related Topics

- Default HAT Entries, on page 2

Default HAT Entries

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

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

In the HAT Overview, the default entry is named "ALL." You can edit the default entry by clicking the mail flow policy for the ALL sender group on the Mail Policies > HAT Overview page.

Note By rejecting all hosts other than the ones you specify, the `listenerconfig` and `systemsetup` commands prevent you from unintentionally configuring your system as an "open relay." An open relay (sometimes called an "insecure relay" or a "third party" relay) is an SMTP email server that allows third-party relay of email messages. By processing email that is neither for nor from a local user, an open relay makes it possible for an unscrupulous sender to route large volumes of spam through your gateway.

Defining Remote Hosts into Sender Groups

You can define the way in which remote hosts attempt to connect to a listener. You group remote host definitions into sender groups. A sender group is a list of remote hosts defined for the purpose of handling email from those senders in the same way.

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

For more information on the list of acceptable addresses in sender groups, see Sender Group Syntax, on page 3.

When an SMTP server attempts an SMTP connection with the email gateway, the listener evaluates the sender groups in order and assigns the connection to a sender group when it matches *any* criterion in the sender group, such as IP reputation score, domain, or IP address.

Note The system acquires and verifies the validity of the remote host's IP address by performing a double DNS lookup. This consists of a reverse DNS (PTR) lookup on the IP address of the connecting host, followed by a forward DNS (A) lookup on the results of the PTR lookup. The system then checks that the results of the A lookup match the results of the PTR lookup. If the results do not match, or if an A record does not exist, the system only uses the IP address to match entries in the HAT.

Define sender groups on the Mail Policies > HAT Overview page.

Related Topics

- Sender Group Syntax, on page 3
- Sender Groups Defined by Network Owners, Domains, and IP Addresses, on page 4
- Defining Sender Groups by IP Reputation Score, on page 6
- Sender Groups Defined by Querying DNS Lists, on page 7

Sender Group Syntax

Table 1: Defining Remote Hosts in the HAT: Sender Group Syntax

Syntax	Meaning
`n:n:n:n:n:n:n:n`	IPv6 address; does not need to include leading zeroes.
`n:n:n:n:n:n:n:n-n:n:n:n:n:n:n:n` `n:n:n-n:n:n:n:n`	Range of IPv6 addresses; does not need to include leading zeroes.
`n.n.n.n`	Full (complete) IPv4 Address

`n.n.n.`
`n.n.n.`
`n.n.`
`n.n.`
`n.`
	Partial IPv4 address

`n.n.n.n-n.`
`n.n.n.n-n.`
`n.n.n-n.`
`n.n-n.`
`n.n-n`
`n-n.`
`n-n`
	Range of IPv4 addresses

Syntax	Meaning
`yourhost.example.com`	A fully-qualified domain name
`.partialhost`	Everything within the partialhost domain

`n/c`
`n.n/c`
`n.n.n/c`
`n.n.n.n/c`
	IPv4 CIDR address block

`n:n:n:n:n:n:n:n/c`	IPv6 CIDR address block; does not need to include leading zeroes
`SBRS[n:n]SBRS[none]`	IP Reputation Score. For more information, see Defining Sender Groups by IP Reputation Score, on page 6.
`SBO:n`	Network Owner Identification Number. For more information, see Defining Sender Groups by IP Reputation Score, on page 6.
`dnslist[dnsserver.domain]`	DNS List query. For more information, see Sender Groups Defined by Querying DNS Lists, on page 7.
ALL	Special keyword that matches ALL addresses. This applies only to the ALL sender group, and is always included (but not listed).

Sender Groups Defined by Network Owners, Domains, and IP Addresses

Since the SMTP protocol has no built-in method for authenticating senders of email, senders of unsolicited bulk email have been successful at employing a number of tactics for hiding their identity. Examples include spoofing the Envelope Sender address on a message, using a forged HELO address, or simply rotating through different domain names. This leaves many mail administrators asking themselves the fundamental question, “Who is sending me all of this email?” To answer this question, the IP Reputation Service has developed a unique hierarchy for aggregating identity-based information based on the IP address of the connecting host — the one thing that is almost impossible for a sender to forge in a message.

An **IP Address** is defined as the IP address of the sending mail host. The email gateway supports both Internet Protocol version 4 (IPv4) and version 6 (IPv6) addresses.

A **Domain** is defined as an entity that uses hostnames with a given second-level domain name (for example, yahoo.com), as determined by a reverse (PTR) lookup on the IP address.

A **Network Owner** is defined as an entity (usually a company) that controls a block of IP addresses, as determined based on IP address space assignments from global registries such as ARIN (the American Registry for Internet Numbers) and other sources.

An **Organization** is defined as an entity that most closely controls a particular group of mail gateways within a network owner’s IP block, as determined by SenderBase. An Organization may be the same as the Network Owner, a division within that Network Owner, or a customer of that Network Owner.

Related Topics

- Setting Policies Based on the HAT, on page 5

Setting Policies Based on the HAT

The following table lists some examples of network owners and organizations.

Table 2: Example of Network Owners and Organizations

Example Type	Network Owner	Organization
Network Service Provider	Level 3 Communications	Macromedia Inc. AllOutDeals.com GreatOffers.com
Email Service Provider	GE	GE Appliances GE Capital GE Mortgage
Commercial Sender	The Motley Fool	The Motley Fool

As network owners can range dramatically in size, the appropriate entity to base your mail flow policy on is the organization. The IP Reputation Service has a unique understanding of the source of the email down to the organization level, which the email gateway leverages to automatically apply policies based on the organization. In the example above, if a user specified "Level 3 Communications" as a sender group in the Host Access Table (HAT), SenderBase will enforce policies based on the individual organizations controlled by that network owner.

For example, in the table above, if a user enters a limit of 10 recipients per hour for Level 3, the email gateway will allow up to 10 recipients per hour for Macromedia Inc., Alloutdeals.com *and* Greatoffers.com (a total of 30 recipients per hour for the Level 3 network owner). The advantage of this approach is that if one of these organizations begins spamming, the other organizations controlled by Level 3 will not be impacted. Contrast this to the example of "The Motley Fool" network owner. If a user sets rate limiting to 10 recipients per hour, the Motley Fool network owner will receive a total limit of 10 recipients per hour.

The Mail Flow Monitor feature is a way of defining the sender and providing you with monitoring tools to create mail flow policy decisions about the sender. To create mail flow policy decisions about a given sender, ask these questions:

- **Which IP addresses are controlled by this sender?**

  The first piece of information that the Mail Flow Monitor feature uses to control the inbound email processing is the answer to this question. The answer is derived by querying the IP Reputation Service. The IP Reputation Service provides information about the relative size of the sender (either the network owner or the SenderBase organization). Answering this question assumes the following:

  - Larger organizations tend to control more IP addresses, and send more legitimate email.

- **Depending on its size, how should the overall number of connections be allotted for this sender?**

  - Larger organizations tend to control more IP addresses, and send more legitimate email. Therefore, they should be allotted more connections to your email gateway.
  - The sources of high-volume email are often ISPs, NSPs, companies that manage outsourced email delivery, or sources of unsolicited bulk email. ISPs, NSPS, and companies that manage outsourced email delivery are examples of organizations that control many IP addresses, and should be allotted more connections to your email gateway. Senders of unsolicited bulk email usually do not control

many IP addresses; rather, they send large volumes of mail through a few number of IP addresses. They should be allotted fewer connections to your email gateway.

The Mail Flow Monitor feature uses its differentiation between network owners and SenderBase organizations to determine how to allot connections per sender, based on logic in SenderBase. See the "Using Email Security Monitor" chapter for more information on using the Mail Flow Monitor feature.

Defining Sender Groups by IP Reputation Score

The email gateway can query the IPReputation Service to determine a 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. The scale of the score ranges from -10.0 to +10.0, as described in the following table.

Table 3: Definition of the IP Reputation Score

Score	Meaning
-10.0	Most likely to be a source of spam
0	Neutral, or not enough information to make a recommendation
+10.0	Most likely to be a trustworthy sender
none	No data available for this sender (typically a source of spam)

Using the IP Reputation Score, you configure the email gateway to apply mail flow policies to senders based on their trustworthiness. For example, all senders with a score less than -7.5 could be rejected. This is most easily accomplished via the GUI; see Creating a Sender Group for Message Handling , on page 13. However, if you are modifying an exported HAT in a text file, the syntax for including IP Reputation Scores is described in the following table.

Table 4: Syntax for IP Reputation Scores

`SBRS[ n n`	IP Reputation Score. Senders are identified by querying the IP Reputation Service, and the scores are defined between the ranges.
SBRS[none]	Specify no IP (very new domains may not have IP Reputation Scores yet).

Note Network owners added to a HAT via the GUI use the syntax `SBO:n`, where *n* is the network owner's unique identification number in the IP Reputation Service.

Use the **Network > Listeners** page or `listenerconfig -> setup` command in the CLI to enable a listener to query the IP Reputation Service. You can also define the timeout value that the email gateway should wait when querying the IP Reputation Service. Then, you can configure different policies to use look ups to the IP Reputation Service by using the values in the Mail Policies Pages in the GUI or the `listenerconfig -> edit -> hostaccess` commands in the CLI.

Note You can also create message filters to specify "thresholds" for IP Reputation Scores to further act upon messages processed by the system. For more information, see "IP Reputation Rule," "Bypass Anti-Spam System Action," and "Bypass Anti-Virus System Action" in the anti-spam and anti-virus chapters.

Sender Groups Defined by Querying DNS Lists

You also have the ability in a listener's HAT to define a sender group as matching a query to a specific DNS List sever. The query is performed via DNS at the time of the remote client's connection. The ability to query a remote list also exists currently as a message filter rule (see "DNS List Rule" in the chapter on "Using Message Filters to Enforce Email Policies"), but only once the message content has been received in full.

This mechanism allows you to configure a sender within a group that queries a DNS List so that you can adjust your mail flow policies accordingly. For example, you could reject connections or limit the behavior of the connecting domain.

Note Some DNS Lists use variable responses (for example, "127.0.0.1" versus "127.0.0.2" versus "127.0.0.3") to indicate various facts about the IP address being queried against. If you use the message filter DNS List rule (see "DNS List Rule" in the chapter on "Using Message Filters to Enforce Email Policies"), you can compare the result of the query against different values. However, specifying a DNS List server to be queried in the HAT only supports a Boolean operation for simplicity (that is, does the IP address appear in the list or not)

Note Be sure to include brackets in the query in the CLI. Brackets are not necessary when specifying a DNS List query in the GUI. Use the dnslistconfig command in the CLI to test a query, configure general settings for DNL queries, or flush the current DNS list cache.

Note that this mechanism can be used to identify "good" connections as well as "bad" connections. For example, a query to query.bondedsender.org will match on connecting hosts who have posted a financial bond with Cisco Systems' Bonded Sender™ program to ensure the integrity of their email campaign. You could modify the default ALLOWED_LIST sender group to query the Bonded Sender program's DNS servers (which lists these legitimate email senders who have willingly posted bonds) and adjust the mail flow policy accordingly.

Defining Access Rules for Email Senders Using Mail Flow Policies

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 the following types of parameters in the mail flow policy:

- Connection parameters, such as maximum number of messages per connection.
- Rate limiting parameters, such as maximum number of recipients per hour.

- Modify custom SMTP codes and responses communicated during the SMTP conversation.
- Enable spam detection.
- Enable virus protection.
- Encryption, such as using TLS to encrypt the SMTP connection.
- Authentication parameters, such as using DKIM to verify incoming mail.

Ultimately, mail flow policies perform one of the following actions on connections from remote hosts:

- **ACCEPT.** Connection is accepted, and email acceptance is then further restricted by listener settings, including the Recipient Access Table (for public listeners).
- **REJECT.** Connection is initially accepted, but the client attempting to connect gets a 4XX or 5XX SMTP status code. No email is accepted.

Note You can also configure AsyncOS to perform this rejection at the message recipient level (RCPT TO), rather than at the start of the SMTP conversation. Rejecting messages in this way delays the message rejection and bounces the message, allowing AsyncOS to retain more detailed information about the rejected messages. This setting is configured from the CLI `listenerconfig > setup` command. For more information, see Listening for Connection Requests by Creating a Listener Using CLI.

- **TCPREFUSE.** Connection is refused at the TCP level.
- **RELAY.** Connection is accepted. Receiving for any recipient is allowed and is not constrained by the Recipient Access Table.
- **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. For more information, see Creating a Sender Group for Message Handling , on page 13.

Related Topics

- HAT Variable Syntax, on page 8

HAT Variable Syntax

The following table defines a set of variables that can also be used in conjunction with the custom SMTP and Rate Limiting banners defined for a mail flow policy. Variable names are case-insensitive. (That is, $group is equivalent to $Group .)

Table 5: HAT Variable Syntax

Variable	Definition
$Group	Replaced by the name of the sender group that was matched in the HAT. If the sender group has no name, “None” is displayed.

Variable	Definition
$Hostname	Replaced by the remote hostname if and only if is has been validated by the email gateway. If the reverse DNS lookup of the IP address is successful but returns no hostname, then “None” is displayed. If the reverse DNS lookup fails (for example, if the DNS server cannot be reached, or no DNS server has been configured) then “Unknown” is displayed.
$OrgID	Replaced by the SenderBase Organization ID (an integer value). If the email gateway cannot obtain a SenderBase Organization ID, or if the IP Reputation Service did not return a value, “None” is displayed.
$RemoteIP	Replaced by the IP address of the remote client.
$HATEntry	Replaced by the entry in the HAT that the remote client matched.

Related Topics

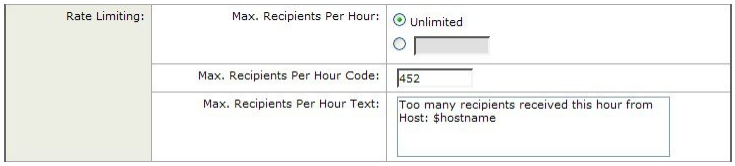
- Using HAT Variables, on page 9
- Testing HAT Variables, on page 10

Using HAT Variables

Note These variables can be used with the `smtp_banner_text` and `max_rcpts_per_hour_text` advanced HAT parameters described in the “Configuring the Gateway to Receive Email” chapter.

Using these variables, you could edit the custom SMTP banner response text for accepted connections in the $TRUSTED policy in the GUI:

Figure 1: Using HAT Variables



Or like this, in the CLI:

```
Would you like to specify a custom SMTP response?  [Y]> y


Enter the SMTP code to use in the response. 220 is the standard code.

[220]> 200


Enter your custom SMTP response.  Press Enter on a blank line to finish.
```

```
You've connected from the hostname: $Hostname, IP address of: $RemoteIP, matched the group:
 $Group,
$HATEntry and the SenderBase Organization: $OrgID.
```

Testing HAT Variables

To test these variables, add the IP address of a known, trusted machine to the $ALLOWED_LIST sender group of a listener on the email gateway. Then, connect from that machine via telnet. You can see the variable substitution in the SMTP response. For example:

```
# telnet
IP_address_of_Email_Security_Appliance port


220 hostname
 ESMTP


200 You've connected from the hostname: hostname
, IP address of: IP-address_of_connecting_machine
, matched the group: ALLOWED_LIST, 10.1.1.1 the SenderBase Organization: OrgID
.
```

Understanding Predefined Sender Groups and Mail Flow Policies

The following table lists the predefined sender groups and mail flow policies that are configured when a public listener is created.

Table 6: Predefined Sender Groups and Mail Flow Policies for Public Listeners

Predefined Sender Group	Description	Default Configured Mail Flow Policy
ALLOWED_LIST	Add senders you trust to the Allowed_list sender group. The $TRUSTED mail flow policy is configured so that email from senders you trust has no rate limiting enabled, and the content from those senders is not scanned by the Anti-Spam or Anti-Virus software.	$TRUSTED
BLOCKED_LIST	Senders in the Blocked_list sender group are rejected (by the parameters set in the $BLOCKED mail flow policy). Adding senders to this group rejects connections from those hosts by returning a 5XX SMTP response in the SMTP HELO command.	$BLOCKED

Predefined Sender Group	Description	Default Configured Mail Flow Policy
SUSPECTLIST	The Suspectlist sender group contains a mail flow policy that throttles, or slows, the rate of incoming mail. If senders are suspicious, you can add them to the Suspectlist sender group, where the mail flow policy dictates that: • Rate limiting limits the maximum number of messages per session, the maximum number of recipients per message, the maximum message size, and the maximum number of concurrent connections you are willing to accept from a remote host. • The maximum recipients per hour from the remote host is set to 20 recipients per hour. Note that this setting is the maximum throttling available. You can increase the number of recipients to receive per hour if this parameter is too aggressive. • The content of messages will be scanned by the anti-spam scanning engine and the anti-virus scanning engine (if you have these feature enabled for the system). • The SenderBase Reputation Service will be queried for more information about the sender.	$THROTTLED
UNKNOWNLIST	The Unknownlist sender group may be useful if you are undecided about the mail flow policy you should use for a given sender. The mail flow policy for this group dictates that mail is accepted for senders in this group, but the Anti-Spam software (if enabled for the system), the anti-virus scanning engine, and the IP Reputation Service should all be used to gain more information about the sender and the message content. Rate limits for senders in this group are also enabled with default values. For more information on virus scanning engines, see Virus Scanning. For more information on the IP Reputation Service, see IP Reputation Service.	$ACCEPTED
ALL	Default sender group that applies to all other senders. For more information, see Default HAT Entries, on page 2.	$ACCEPTED

The following table lists the predefined sender groups and mail flow policies that are configured when a private listener is created.

Table 7: Predefined Sender Groups and Mail Flow Policies for Private Listeners

Predefined Sender Group	Description	Default Configured Mail Flow Policy
RELAYLIST	Add senders you know should be allowed to relay to the Relaylist sender group. The $RELAYED mail flow policy is configured so that email from senders you are allowing to relay has no rate limiting, and the content from those senders is not scanned by the anti-spam scanning engine or anti-virus software. **Note** The RELAYLIST sender group includes the systems allowed to relay email when the System Setup Wizard was run.	$RELAYED
ALL	Default sender group that applies to all other senders. For more information, see Default HAT Entries, on page 2.	$BLOCKED

Note When you run the System Setup Wizard on an email gateway model that has only two Ethernet ports, you are prompted to create only one listener. It creates a public listener that also includes a $RELAYED mail flow policy that is used to relay mail for internal systems. For email gateway models that have more than two Ethernet ports, the RELAYLIST sender group and $RELAYED mail flow policy only appear on private listeners.

Handling Messages from a Group of Senders in the Same Manner

Use the Mail Policies > HAT Overview and Mail Flow Policy pages to configure how the listener handles messages from senders. Do this by creating, editing, and deleting sender groups and mail flow policies.

Related Topics

- Creating a Sender Group for Message Handling , on page 13
- Adding a Sender to an Existing Sender Group, on page 14
- Rearranging the Order of the Rules to Perform for Incoming Connections, on page 14
- Searching for Senders, on page 15
- Defining Access Rules for Email Senders Using Mail Flow Policies, on page 7
- Defining Default Values for Mail Flow Policies, on page 20

Creating a Sender Group for Message Handling

Procedure

Step 1 Navigate to the **Mail Policies > HAT Overview** page.

Step 2 Choose the listener to edit in the Listener field.

Step 3 Click **Add Sender Group**.

Step 4 Type the name of the sender group.

Step 5 Select the order in which to place it in the list of sender groups.

Step 6 (Optional) Enter a comment, for example information about this sender group or its settings.

Step 7 Select a mail flow policy to which to apply this sender group.

Note If you do not know the mail flow policy you would like to apply to this group (or if no mail flow policies exist yet), then use the default "CONTINUE (no policy)" mail flow policy.

Step 8 (Optional) Select a DNS list.

Step 9 (Optional) Include senders for which IP Reputation Score has no information. This is referred to as "none" and generally denotes a suspect.

Step 10 (Optional) Enter a DNS list.

Step 11 (Optional) Configure host DNS verification settings.

For more information, see Implementing More Stringent Throttling Settings for Unverified Senders, on page 29 .

Step 12 Click **Submit** to create the sender group.

Step 13 Click on the newly created sender group.

Step 14 Click **Add Sender** to add senders to the sender group.

- **Add sender IP address** .Select **IP Addresses**, add an IPv4 address, IPv6 address, or a hostname, and submit the changes.

  A sender can include a range of IP addresses and partial hostnames.

- **Add sender's country of origin**. Select **Geolocation**, select the country, and submit the changes.

Step 15 Submit and commit your changes.

What to do next

Related Topics

- Editing IP Reputation Filtering Score Thresholds for a Listener

Adding a Sender to an Existing Sender Group

Procedure

Step 1 From a domain, IP, or network owner profile page, click the Add to Sender Group link.

Step 2 Choose the sender group from the list defined for each listener.

Step 3 Submit and commit your changes.

Note When you add a domain to a sender group, two actual domains are listed in the GUI. For example, if you were adding the domain `example.net` , on the Add to Sender Group page, both `example.net` and `.example.net` are added. The second entry ensures that any host in the subdomain of `example.net` will be added to the sender group. For more information, see Sender Group Syntax, on page 3.

If one or more of the senders you are adding to a sender group is a duplicate of a sender that is already present in that sender group, the duplicate senders will not be added and you will see a confirmation message.

Step 4 Click **Save** to add the sender and return to the Incoming Mail Overview page.

What to do next

Related Topics

- Protecting Email Gateway-Generated Messages From the Spam Filter
- How to Configure the Email Gateway to Scan Messages for Spam

Rearranging the Order of the Rules to Perform for Incoming Connections

If you add a sender group to a listener, you may need to edit the sender group order.

The HAT is read from top to bottom for each host that attempts to connect to the listener. If a rule matches a connecting host, the action is taken for that connection immediately.

Procedure

Step 1 Navigate to the **Mail Policies > HAT Overview** page.

Step 2 Choose the listener to edit in the Listener field.

Step 3 Click **Edit Order.**

Step 4 Type the new order for existing rows of sender groups in the HAT.

Cisco recommends maintaining the default order: RELAYLIST (certain hardware models only), followed by ALLOWED_LIST, BLOCKED_LIST, SUSPECTLIST, and UNKNOWNLIST.

Step 5 Submit and commit your changes.

Searching for Senders

You can find senders by entering text in the Find Senders field at the top of the HAT Overview page. Enter the text to search with and click Find.

Defining Rules for Incoming Messages Using a Mail Flow Policy

Consider the following rules and guidelines before creating a mail flow policy:

- Defaults for the policy are "greyed out" while the "Use Default" radio button is selected. To overwrite the default values, enable the feature or setting by selecting the "On" radio button and making changes to the now accessible values. To define default values, see Defining Default Values for Mail Flow Policies, on page 20.
- Some parameters depend on certain pre-configurations. (For example, the Directory Harvest Attack prevention setting requires that you have configured an LDAP Acceptance Query.)

Procedure

Step 1 Navigate to the **Mail Policies > Mail Flow Policies** page.

Step 2 Click **Add Policy**.

Step 3 Enter the information described in the following table.

Table 8: Mail Flow Policy Parameters

Parameter	Description
Connections	
Maximum message size	The maximum size of a message that will be accepted by this listener. The smallest possible maximum message size is 1 kilobyte.
Maximum concurrent connections from a single IP	The maximum number of concurrent connections allowed to connect to this listener from a single IP address.
Maximum messages per connection	The maximum number of messages that can be sent through this listener per connection from a remote host.
Maximum recipients per message	That maximum number of recipients per message that will be accepted from this host.
SMTP Banner	
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. **Note** You can use some variables in this field. For more information, see HAT Variable Syntax, on page 8.

Parameter	Description
Custom SMTP Reject Banner Code	The SMTP code returned when a connection is rejected by this listener.
Custom SMTP Reject Banner Text	The SMTP banner text returned when a connection is rejected by this listener.
Override SMTP Banner Host Name	By default, the email gateway 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.
Rate Limit for Hosts	
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. **Note** You can use some variables in this field. For more information, see HAT Variable Syntax, on page 8.
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 Exceeded Text	The SMTP banner text returned when a host exceeds the maximum number of recipients per hour defined for this listener.
Rate Limit for Sender	
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 not 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. Select whether to use the default maximum recipients, accept unlimited recipients, or specify another maximum number of recipients. Use the Default Mail Flow Policy settings to specify the maximum number of recipients and the time interval that will be used by the other mail flow policies by default. The time interval can only be specified using the Default Mail Flow Policy.
Sender Rate Limit Exceeded 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 Exceeded 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.

Parameter	Description
Exceptions	If you want certain envelope senders to be exempt from the defined rate limit, select an address list that contains the envelope senders. See Using a List of Sender Addresses for Incoming Connection Rules, on page 22for more information.
Flow Control	
Use SenderBase for Flow Control	Enable "look ups" to the IP Reputation Service for this listener.
Group by Similarity of IP Addresses: (significant bits 0-32)	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. Requires "Use SenderBase" to be disabled. For more information about HAT significant bits, see Configuring Routing and Delivery Features.
Directory Harvest Attack Prevention (DHAP)	
Directory Harvest Attack Prevention: Maximum 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). For more information on configuring DHAP for LDAP accept queries, see Working with LDAP Queries.
Directory Harvest Attack Prevention: Drop Connection if DHAP threshold is Reached within an SMTP Conversation	The email gateway 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."
Drop Connection if DHAP threshold is reached within an SMTP Conversation	Enable to drop connections if the DHAP threshold is reached within an SMTP conversation.
Max. Invalid Recipients Per Hour Code	Specify the code to use when dropping connections due to DHAP within an SMTP conversation. The default code is 550.

Parameter	Description
Max. Invalid Recipients Per Hour Text:	Specify the text to use when dropping connections due to DHAP within an SMTP conversation.
Spam Detection	
Anti-spam scanning	Enable anti-spam scanning on this listener.
Virus Detection	
Anti-virus scanning	Enable the anti-virus scanning on this listener.
Sender Domain Reputation Verification	
Sender Domain Reputation Verification	Enable sender domain reputation verification.
Encryption and Authentication	
TLS	Deny, Prefer, or Require Transport Layer Security (TLS) in SMTP conversations for this listener. If you select Preferred, you can make TLS mandatory for envelope senders from a specific domain or with a specific email address by selecting an Address List that specifies those domains and email addresses. When an envelope sender matching a domain or address in this list tries to send a message over a connection that does not use TLS, the email gateway rejects the connection and the sender will have to try again using TLS. The Verify Client Certificate option directs the email gateway to establish a TLS connection to the user's mail application if the client certificate is valid. If you select this option for the TLS Preferred setting, the email gateway 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 email gateway to allow the connection. For information on creating an address list, see Using a List of Sender Addresses for Incoming Connection Rules, on page 22. For information on using client certificates for TLS connections, see Establishing a TLS Connection from the Email Gateway.
SMTP Authentication	Allows, disallow, or requires SMTP Authentication from remote hosts connecting to the listener. SMTP Authentication is described in detail in the "LDAP Queries" chapter.
If Both TLS and SMTP Authentication are enabled:	Require TLS to offer SMTP Authentication.

Parameter	Description
Domain Key/ DKIM Signing	Enable Domain Keys or DKIM signing on this listener (ACCEPT and RELAY only).
DKIM Verification	Enable DKIM verification.
S/MIME Decryption and Verification	
S/MIME Decryption/Verification	• Enable S/MIME decryption or verification. • Choose whether to retain or remove the digital signature from the messages after S/MIME verification. For triple wrapped messages, only the inner signature is retained or removed.
S/MIME Public Key Harvesting	
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 Verification	Enable SPF/SIDF signing on this listener. For more information, see Email Authentication.
Conformance Level	Set the SPF/SIDF conformance level. You can choose from SPF, SIDF or SIDF Compatible. For details, see Email Authentication.
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. You may choose this option for security purposes.
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	Enable DMARC verification on this listener. For more information, see DMARC Verification.
Use DMARC Verification Profile	Select the DMARC verification profile that you want to use on this listener.

Parameter	Description
DMARC Feedback Reports	Enable sending of DMARC aggregate feedback reports. For more information about DMARC aggregate feedback report, see DMARC Aggregate Reports. **Note** DMARC specification requires the feedback report messages to be DMARC compliant. Make sure that these messages are DKIM signed or you must publish appropriate SPF records.
Untagged Bounces	
Consider Untagged Bounces to be Valid	Applies only if bounce verification tagging (discussed in the "Configuring Routing and Delivery Features" chapter) 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 email gateway accepts the bounce message.
Envelope Sender DNS Verification	
	See Verifying Senders, on page 25.
Exception Table	
Use Exception Table	Use the sender verification domain exception table. You can only have one exception table, but you can enable it per mail flow policy. See Sender Verification Exception Table, on page 27 for more information.

Note If anti-spam or anti-virus scanning is enabled globally in the HAT, messages are flagged for anti-spam or anti-virus scanning as they are accepted by the email gateway. If anti-spam or anti-virus scanning is disabled after the message is accepted, the message will still be subject to scanning when it leaves the work queue.

Step 4 Submit and commit your changes.

Defining Default Values for Mail Flow Policies

Procedure

Step 1 Click **Mail Policies > Mail Flow Policies**.

Step 2 Choose the listener to edit in the Listener field.

Step 3 Click the **Default Policy Parameters** link below the configured mail flow policies.

Step 4 Define the default values that all mail flow policies for this listener use.

For more information on the properties, see Defining Rules for Incoming Messages Using a Mail Flow Policy, on page 15.

Step 5 Submit and commit your changes.

Working with the Host Access Table Configuration

You can export all information stored in a Host Access Table to a file, and you can import Host Access Table information stored in a file into the email gateway for a listener, overwriting all existing Host Access Table information.

Related Topics

- Exporting the Host Access Table Configuration to an External File, on page 21
- Importing the Host Access Table Configuration from an External File, on page 21

Exporting the Host Access Table Configuration to an External File

Procedure

Step 1 Navigate to the Mail Policies > HAT Overview page.
Step 2 Choose the listener to edit in the Listener menu.
Step 3 Click **Export HAT.**
Step 4 Enter a file name for the exported HAT. This is the name of the file that will be created in the configuration directory on the email gateway.
Step 5 Submit and commit your changes.

Importing the Host Access Table Configuration from an External File

When you import a HAT, all of the existing HAT entries are removed from the current HAT.

Procedure

Step 1 Navigate to the Mail Policies > HAT Overview page.
Step 2 Choose the listener to edit in the Listener menu.
Step 3 Click **Import HAT.**
Step 4 Select a file from the list.

Note The file to import must be in the configuration directory on the email gateway.

Step 5 Click **Submit**. You will see a warning message, asking you to confirm that you wish to remove all of the existing HAT entries.
Step 6 Click **Import**.
Step 7 Commit your changes.

You can place “comments” in the file. Lines that begin with a ‘#’ character are considered comments and are ignored by AsyncOS. For example:

```
# File exported by the GUI at 20060530T215438
$BLOCKED
    REJECT {}
[ ... ]
```

Using a List of Sender Addresses for Incoming Connection Rules

Mail flow policies allow you to use of an address list for certain settings that apply to a group of envelope senders, such as rate limiting exemptions and mandatory TLS connections. An address list can consist of email addresses, domains, partial domains, and IP addresses. You can use the **Mail Policies > Address Lists** page in the GUI or the `addresslistconfig` command in the CLI to create an address list. The Address Lists page displays all address lists on the email gateway, along with any mail flow policies that use an address list.

Procedure

Step 1 Select **Mail Policies > Address Lists**.

Step 2 Click **Add Address List**.

Step 3 Enter a name for the address list.

Step 4 Enter a description of the address list.

Step 5 (Optional) To enforce using full email addresses in the address list, select **Full Email Addresses only**.

Step 6 Choose any one of the following options to create an address list:

- Select **Full Email Addresses only** if you want to enforce using full email addresses in the address list.
- Select **Domains only** if you want to enforce using domains in the address list.
- Select **IP Addresses only** if you want to enforce using IP addresses in the address list.

Step 7 Enter the addresses you want to include. You can use the following formats:

- Full email address: `user@example.com`
- Partial email address: `user@`

  Note If you have selected **Allow only full Email Addresses**, you cannot use partial email addresses.

- IP address in their email address: `@[1.2.3.4]`
- All users in a domain: `@example.com`
- All users in a partial domain: `@.example.com`

Note that domains and IP addresses must start with a `@` character.

Separate email addresses with a comma. If you separate the addresses using a new line, AsyncOS automatically converts your entries into a comma-separated list.

Step 8 Submit and commit your changes.

SenderBase Settings and Mail Flow Policies

In order to classify connections to the email gateway and apply mail flow policies (which may or may not contain rate limiting), a listener uses the following methodology:

Classification -> Sender Group -> Mail Flow Policy -> Rate Limiting

For more information, see Sender Groups Defined by Network Owners, Domains, and IP Addresses, on page 4.

The "Classification" stage uses the sending host's IP address to classify an inbound SMTP session (received on a public listener) into a Sender Group. The Mail Flow Policy associated with that Sender Group may have parameters for rate limiting enabled. (Rate limiting limits the maximum number of messages per session, the maximum number of recipients per message, the maximum message size, and/or the maximum number of concurrent connections you are willing to accept from a remote host.)

Normally, in this process, recipients are counted against each sender in the corresponding named sender group. If mail is received from several senders in the same hour, the total recipients for all senders is compared against the limit.

There are some exceptions to this counting methodology:

- If the classification is done by Network Owner, then the IP Reputation Service will automatically divide a large block of addresses into smaller blocks.

Counting of recipients and recipient rate limiting is done separately for each of these smaller blocks (usually, but not always, the equivalent of a /24 CIDR block).

- If the HAT Significant Bits feature is used. In this case, a large block of addresses may be divided into smaller blocks by applying the significant bits parameter associated with the policy.

Note that this parameter relates to the **Mail Flow Policy -> Rate Limiting** phase. It is not the same as the "bits" field in the "network/bits" CIDR notation that may be used to classify IP addresses in a Sender Group.

By default, IP Reputation Service and IP Profiling support are *enabled* for public listeners and *disabled* for private listeners.

Related Topics

- HAT Significant Bits Feature, on page 23

HAT Significant Bits Feature

Beginning with the 3.8.3 release of AsyncOS, you can track and rate limit incoming mail on a per-IP address basis while managing sender group entries in a listener's Host Access Table (HAT) in large CIDR blocks. For example, if an incoming connection matched against the host "10.1.1.0/24," a counter could still be generated for each individual address within that range, rather than aggregating all traffic into one large counter.

Note In order for the significant bits HAT policy option to take effect, you *must* not enable "User SenderBase" in the Flow Control options for the HAT (or, for the CLI, answer **no** to the question for enabling the SenderBase Information Service in the `listenerconfig -> setup` command: "Would you like to enable Reputation Filters and IP Profiling support?"). That is, the Hat Significant Bits feature and enabling SenderBase IP Profiling support are mutually exclusive.

In most cases, you can use this feature to define sender groups *broadly* — that is, large groups of IP addresses such as "10.1.1.0/24" or "10.1.0.0/16" — while applying mail flow rate limiting *narrowly* to smaller groups of IP addresses.

The HAT Significant Bits feature corresponds to these components of the system:

- HAT Configuration , on page 24
- Significant Bits HAT Policy Option , on page 24
- Injection Control Periodicity , on page 24

HAT Configuration

There are two parts of HAT configuration: sender groups and mail flow policies. Sender group configuration defines how a sender's IP address is "classified" (put in a sender group). Mail flow policy configuration defines how the SMTP session from that IP address is controlled. When using this feature, an IP address may be "classified in a CIDR block" (e.g. 10.1.1.0/24) sender group while being controlled as an individual host (/32). This is done via the "signficant_bits" policy configuration setting.

Significant Bits HAT Policy Option

The HAT syntax allows for the signficant_bits configuration option. This feature appears in the GUI in the Mail Policies > Mail Flow Policies page.

When the option to use SenderBase for flow control is set to "OFF" or Directory Harvest Attack Prevention is enabled, the "significant bits" value is applied to the connecting sender's IP address, and the resulting CIDR notation is used as the token for matching defined sender groups within the HAT. Any rightmost bits that are covered by the CIDR block are "zeroed out" when constructing the string. Thus, if a connection from the IP address 1.2.3.4 is made and matches on a policy with the significant_bits option set to 24, the resultant CIDR block would be 1.2.3.0/24. So by using this feature, the HAT sender group entry (for example, 10.1.1.0/24) can have a different number of network significant bits (24) from the significant bits entry in the policy assigned to that group (32, in the example).

For more information on `listenerconfig` command, see the CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway.

Injection Control Periodicity

A global configuration option exists to allow you to adjust when the injection control counters are reset. For very busy systems maintaining counters for a very large number of different IP addresses, configuring the counters to be reset more frequently (for example, every 15 minutes instead of every 60 minutes) will ensure that the data does not grow to an unmanageable size and impact system performance.

The current default value is 3600 seconds (1 hour).You can specify periods ranging from as little as 1 minute (60 seconds) to as long as 4 hours (14,400 seconds).

Adjust this period via the GUI, using the global settings (for more information, see Configuring Global Settings for Listeners).

You can also adjust this period using the `listenerconfig -> setup` command in the CLI. For more information on `listenerconfig` command, see the CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway.

Verifying Senders

Spam and unwanted mail is frequently sent by senders whose domains or IP addresses cannot be resolved by DNS. DNS verification means that you can get reliable information about senders and process mail accordingly. Sender verification prior to the SMTP conversation (connection filtering based on DNS lookups of the sender's IP address) also helps reduce the amount of junk email processed through the mail pipeline on the email gateway.

Mail from unverified senders is not automatically discarded. Instead, AsyncOS provides sender verification settings that allow you to determine how the email gateway handles mail from unverified senders: you can configure your email gateway to automatically block all mail from unverified senders prior to the SMTP conversation or throttle unverified senders, for example.

The sender verification feature consists of the following components:

- **Verification of the connecting host.** This occurs prior to the SMTP conversation. For more information, see Sender Verification: Host, on page 25.
- **Verification of the domain portion of the envelope sender.** This occurs during the SMTP conversation. For more information, see Sender Verification: Envelope Sender, on page 26.

Related Topics

- Sender Verification: Host, on page 25
- Sender Verification: Envelope Sender, on page 26
- Implementing Sender Verification — Example Settings, on page 28
- Testing Your Settings for Messages from Unverified Senders, on page 31
- Sender Verification and Logging, on page 32

Sender Verification: Host

Senders can be unverified for different reasons. For example, the DNS server could be "down" or not responding, or the domain may not exist. Host DNS verification settings for sender groups allow you to classify unverified senders prior to the SMTP conversation and include different types of unverified senders in your various sender groups.

The email gateway attempts to verify the sending domain of the connecting host via DNS for incoming mail. This verification is performed prior to the SMTP conversation. The system acquires and verifies the validity of the remote host's IP address (that is, the domain) by performing a *double DNS lookup* . A double DNS lookup is defined as a reverse DNS (PTR) lookup on the IP address of the connecting host, followed by a forward DNS (A) lookup on the results of the PTR lookup. The email gateway then checks that the results of the A lookup match the results of the PTR lookup. If the PTR or A lookups fail, or the results do not match, the system uses only the IP address to match entries in the HAT and the sender is considered as not verified.

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).

Using the sender group "Connecting Host DNS Verification" settings, you can specify a behavior for unverified senders (see Throttling Messages from Unverified Senders Using the SUSPECTLIST Sender Group, on page 29).

You can enable host DNS verification in the sender group settings for any sender group; however, keep in mind that adding host DNS verification settings to a sender group means *including* unverified senders in that group. That means that spam and other unwanted mail will be included. Therefore, you should only enable these settings on sender groups that are used to reject or throttle senders. Enabling host DNS verification on the ALLOWED_LIST sender group, for example, would mean that mail from unverified senders would receive the same treatment as mail from your trusted senders in your ALLOWED_LIST (including bypassing anti-spam/anti-virus checking, rate limiting, etc., depending on how the mail flow policy is configured).

Sender Verification: Envelope Sender

With envelope sender verification, the domain portion of the envelope sender is DNS verified. (Does the envelope sender domain resolve? Is there an A or MX record in DNS for the envelope sender domain?) A domain does not resolve if an attempt to look it up in the DNS encounters a temporary error condition such as a timeout or DNS server failure. On the other hand, a domain does not exist if an attempt to look it up returns a definitive "domain does not exist" status. This verification takes place during the SMTP conversation whereas host DNS verification occurs before the conversation begins — it applies to the IP address of connecting SMTP server.

In more detail: AsyncOS performs an MX record query for the domain of the sender address. AsyncOS then performs an A record lookup based on the result of the MX record lookup. If the DNS server returns "NXDOMAIN" (there is no record for this domain), AsyncOS treats that domain as non-existent. This falls into the category of "Envelope Senders whose domain does not exist." NXDOMAIN can mean that the root name servers are not providing any authoritative name servers for this domain.

Note Sender verification rejects a domain with no MX record if the DNS response is "NOERROR."

However, if the DNS server returns "SERVFAIL," it is categorized as "Envelope Senders whose domain does not resolve." SERVFAIL means that the domain does exist but DNS is having transient problems looking up the record.

A common technique for spammers or other illegitimate senders of mail is to forge the MAIL FROM information (in the envelope sender) so that mail from unverified senders that is accepted will be processed. This can lead to problems as bounce messages sent to the MAIL FROM address are undeliverable. Using envelope sender verification, you can configure your email gateway to reject mail with malformed (but not blank) MAIL FROMs.

For each mail flow policy, you can:

- Enable envelope sender DNS verification.
- Offer custom SMTP code and response for malformed envelope sender. Malformed envelope senders are blocked if you have enabled envelope sender DNS verification.
- Offer custom response for envelope sender domains which do not resolve.
- Offer custom response for envelope sender domains which do not exist in DNS.

You can use the sender verification exception table to storeSender Verification Exception Table, on page 27 a list of domains or addresses from which mail will be automatically allowed or rejected (see). The sender

verification exception table can be enabled independently of Envelope Sender verification. So, for example, you can still reject special addresses or domains specified in the exception table without enabling envelope sender verification. You can also always allow mail from internal or test domains, even if they would not otherwise be verified.

Though most spam is from unverifiable senders, there are reasons why you might want to accept mail from an unverified sender. For example, not all legitimate email can be verified through DNS lookups — a temporary DNS server problem can stop a sender from being verified.

When mail from unverified senders is attempted, the sender verification exception table and mail flow policy envelope sender DNS verification settings are used to classify envelope senders during the SMTP conversation. For example, you may accept and throttle mail from sending domains that are not verified because they do not exist in DNS. Once that mail is accepted, messages with malformed MAIL FROMs are rejected with a customizable SMTP code and response. This occurs during the SMTP conversation.

You can enable envelope sender DNS verification (including the domain exception table) in the mail flow policy settings for any mail flow policy via the GUI or the CLI (`listenerconfig -> edit -> hostaccess -> < policy >`).

Related Topics

- Partial Domains, Default Domains, and Malformed MAIL FROMs, on page 27
- Custom SMTP Code and Response, on page 27
- Sender Verification: Envelope Sender, on page 26

Partial Domains, Default Domains, and Malformed MAIL FROMs

If you enable envelope sender verification or disable allowing partial domains in SMTP Address Parsing options for a listener (see the SMTP Address Parsing Options section in the “Configuring the Gateway to Receive Email” chapter), the default domain settings for that listener will no longer be used.

These features are mutually exclusive.

Custom SMTP Code and Response

You can specify the SMTP code and response message for messages with malformed envelope senders, for envelope senders which do not exist in DNS, and for envelope senders which do not resolve via DNS queries (DNS server might be down, etc.).

In the SMTP response, you can include a variable, `$EnvelopeSender` , which is expanded to the value of the envelope sender when the custom response is sent.

While typically a “Domain does not exist” result is permanent, it is possible for this to be a transient condition. To handle such cases, “conservative” users may wish to change the error code from the default 5XX to a 4XX code.

Sender Verification Exception Table

The sender verification exception table is a list of domains or email addresses that will either be automatically allowed or rejected during the SMTP conversation. You can also specify an optional SMTP code and reject response for rejected domains. There is only one sender verification exception table per email gateway and it is enabled per mail flow policy.

The sender verification exception table can be used to list obviously fake but correctly formatted domains or email addresses from which you want to reject mail. For example, the correctly formatted MAIL FROM:

`pres@whitehouse.gov` could be listed in the sender verification exception table and set to be automatically rejected. You can also list domains that you want to automatically allow, such as internal or test domains. This is similar to envelope recipient (SMTP RCPT TO command) processing which occurs in the Recipient Access Table (RAT).

The sender verification exception table is defined in the GUI via the Mail Policies > Exception Table page (or the CLI, via the `exceptionconfig` command) and then is enabled on a per-policy basis via the GUI (see Defining Messages to Send to Unverified Senders Using the ACCEPTED Mail Flow Policy, on page 30) or the CLI (see the *CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*.

Entries in the sender verification exception table have the following syntax:

See Excluding Unverified Senders from Sender Verification Rules Based on Sender's Email Address, on page 30 for more information about modifying the exception table.

Implementing Sender Verification — Example Settings

This section provides an example of a typical conservative implementation of host and envelope sender verification.

For this example, when implementing host sender verification, mail from connecting hosts for which reverse DNS lookup does not match is throttled via the existing SUSPECTLIST sender group and THROTTLED mail flow policy.

A new sender group (UNVERIFIED) and a new mail flow policy (THROTTLEMORE) are created. Mail from connecting hosts which are not verified will be throttled (using the UNVERIFIED sender group and the more aggressive THROTTLEMORE mail flow policy) prior to the SMTP conversation.

Envelope sender verification is enabled for the ACCEPTED mail flow policy.

The following table shows the suggested settings for implementing sender verification:

Table 9: Sender Verification: Suggested Settings

Sender Group	Policy	Include
UNVERIFIED SUSPECTLIST	THROTTLEMORE THROTTLED	Prior to SMTP conversation: Connecting host PTR record does not exist in the DNS. Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A).
	ACCEPTED	Envelope Sender Verification during SMTP conversation: - Malformed MAIL FROM: - Envelope sender does not exist in DNS. - Envelope sender DNS does not resolve.

Related Topics

- Throttling Messages from Unverified Senders Using the SUSPECTLIST Sender Group, on page 29
- Implementing More Stringent Throttling Settings for Unverified Senders, on page 29

- Defining Messages to Send to Unverified Senders Using the ACCEPTED Mail Flow Policy, on page 30
- Excluding Unverified Senders from Sender Verification Rules Based on Sender's Email Address, on page 30
- Searching for Addresses within the Sender Verification Exception Table, on page 30

Throttling Messages from Unverified Senders Using the SUSPECTLIST Sender Group

Procedure

Step 1 Select **Mail Policies > HAT Overview**.

Step 2 Click **SUSPECTLIST** in the list of sender groups.

Step 3 Click **Edit Settings.**

Step 4 Select the THROTTLED policy from the list.

Step 5 Check the "Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A)" checkbox under Connecting Host DNS Verification.

Step 6 Submit and commit your changes.

Now, senders for which reverse DNS lookups fail will match the SUSPECTLIST sender group and will receive the default action from the THROTTLED mail flow policy.

Implementing More Stringent Throttling Settings for Unverified Senders

Procedure

Step 1 Create a new mail flow policy (for this example, it is named THROTTLEMORE) and configure it with more stringent throttling settings.

a) On the Mail Flow Policies page, click **Add Policy**
b) Enter a name for the mail flow policy, and select Accept as the Connection Behavior.
c) Configure the policy to throttle mail.
d) Submit and commit your changes.

Step 2 Create a new sender group (for this example, it is named UNVERIFIED) and configure it to use the THROTTLEMORE policy:

a) On the HAT Overview page, click **Add Sender Group**
b) Select the THROTTLEMORE policy from the list.
c) Check the "Connecting host PTR record does not exist in DNS" checkbox under Connecting Host DNS Verification.
d) Submit and commit your changes.

Defining Messages to Send to Unverified Senders Using the ACCEPTED Mail Flow Policy

Procedure

Step 1 Select **Mail Policies > Mail Flow Policies**.

Step 2 On the Mail Flow Policies page, click on the ACCEPTED mail flow policy.

Step 3 Scroll down to the **Sender Verification** section.

Step 4 In the **Envelope Sender DNS Verification** section, do the following:

- Select **On** to enable envelope sender DNS verification for this mail flow policy.
- You may also define custom SMTP code and responses.

Step 5 In the **Use Domain Exception Table** section, select **On** to enable the domain exception table.

Step 6 Submit and commit your changes.

Excluding Unverified Senders from Sender Verification Rules Based on Sender's Email Address

Procedure

Step 1 Select **Mail Policies > Exception Table**.

Note The exception table applies globally to all mail flow policies with "Use Exception Table" enabled.

Step 2 Click **Add Domain Exception** on the Mail Policies > Exception Table page.

Step 3 Enter an email address. You can enter a specific address (pres@whitehouse.gov), a name (user@), a domain (@example.com or @.example.com), or an address with a bracketed IP address (user@[192.168.23.1]).

Step 4 Specify whether to allow or reject messages from the address. When rejecting mail, you can also specify an SMTP code and custom response.

Step 5 Submit and commit your changes.

Searching for Addresses within the Sender Verification Exception Table

Procedure

Step 1 Enter the email address in the Find Domain Exception section of the Exception Table page.

Step 2 Click **Find**.

If the address matches any of the entries in the table, the first matching entry is displayed.

Testing Your Settings for Messages from Unverified Senders

Now that you have configured sender verification settings, you can verify the behavior of your email gateway.

Note that testing DNS-related settings is beyond the scope of this document.

Related Topics

- Sending a Test Message with a Malformed MAIL FROM Sender Address, on page 31
- Sending a Message from an Address That is Excluded from Sender Verification Rules, on page 31

Sending a Test Message with a Malformed MAIL FROM Sender Address

While it may be difficult to test the various DNS-related settings for your THROTTLED policy, you can test the malformed MAIL FROM setting.

Procedure

Step 1 Open a Telnet session to your email gateway.

Step 2 Use SMTP commands to send a test message with a malformed MAIL FROM (something like "admin" without a domain).

Note If you have configured your email gateway to use a default domain or to specifically allow partial domains when sending or receiving email or if you have enabled address parsing (see the "Configuring the Gateway to Receive Email" chapter) you may not be able to create, send, and receive an email with a missing or malformed domain.

Step 3 Verify that the message is rejected.

```
# telnet IP_address_of_Email_Security_Appliance port
220 hostname ESMTP
helo example.com
250 hostname
mail from: admin
553 #5.5.4 Domain required for sender address
```

Note that the SMTP code and response is the one you configured for the envelope sender verification settings for the THROTTLED mail flow policy.

Sending a Message from an Address That is Excluded from Sender Verification Rules

To confirm that mail from the email address listed in the sender verification exception table is not subject to envelope sender verification:

Procedure

Step 1 Add the following address to the exception table with an "Allow" behavior: admin@zzzaaazzz.com

Step 2 Commit your changes.

Step 3 Open a Telnet session to your email gateway.

Step 4 Use SMTP commands to send a test message from the email address you entered in the sender verification exception table (admin@zzzaaazzz.com).

Step 5 Verify that the message is accepted.

```
# telnet IP_address_of_Email_Security_Appliance port
220 hostname ESMTP
helo example.com
250 hostname
mail from: admin@zzzaaazzz.com
250 sender <admin@zzzaaazzz.com> ok
```

If you remove that email address from the sender verification exception table, mail from that sender will be rejected because the domain portion of the envelope sender is not DNS verified.

Sender Verification and Logging

The following log entries provide an example of Sender Verification verdicts.

Related Topics

- Envelope Sender Verification, on page 32

Envelope Sender Verification

Malformed Envelope Senders:

```
Thu Aug 10 10:14:10 2006 Info: ICID 3248 Address: <user> sender rejected, envelope sender
 domain missing
```

Domain does not exist (NXDOMAIN):

```
Wed Aug  9 15:39:47 2006 Info: ICID 1424 Address: <user@domain.com> sender rejected, envelope
 sender domain does not exist
```

Domain does not resolve (SERVFAIL):

```
Wed Aug  9 15:44:27 2006 Info: ICID 1425 Address: <user@domain.com> sender rejected, envelope
 sender domain could not be resolved
```