Mail Policies

This chapter contains the following sections:

- Overview of Mail Policies, on page 1
- How to Enforce Mail Policies on a Per-User Basis, on page 2
- Handling Incoming and Outgoing Messages Differently, on page 3
- Matching Users to a Mail Policy, on page 3
- Message Splintering, on page 6
- Configuring Mail Policies, on page 7
- Setting Priority for Message Headers, on page 12

Overview of Mail Policies

The email gateway enforces your organization's policies for messages sent to and from your users through the use of mail policies. These are sets of rules that specify the types of suspect, sensitive, or malicious content that your organization may not want entering or leaving your network. This content may include:

- spam
- legitimate marketing messages
- graymail
- viruses
- phishing and other targeted mail attacks
- confidential corporate data
- personally identifiable information

You can create multiple policies that satisfy the disparate security needs of the different user groups within your organization. The email gateway uses the rules defined in these policies to scan each message and, if necessary, perform an action to protect your user. For example, policies can prevent the delivery of suspected spam messages to executives while allowing their delivery to IT staff but with a modified subject to warn them of the content, or drop dangerous executable attachments for all users except those in the System Administrator group.

How to Enforce Mail Policies on a Per-User Basis

Procedure

	Command or Action	Purpose
Step 1	Enable the content-scanning features that you want the email gateway to use for incoming or outgoing messages.	The features you can enable and configure one or more of the following: • Anti-Virus • File Reputation Filtering and File Analysis (incoming messages only) • Managing Spam and Graymail • Graymail Detection and Safe Unsubscribe. See Managing Spam and Graymail. • Outbreak Filters • Data Loss Prevention (outgoing messages only) • Content Filters • Integrating Secure Email Gateway with Threat Defense
Step 2	(Optional) Create content filters for actions to take on messages that contain specific data.	See Content Filters
Step 3	(Optional) Define an LDAP group query in order to specify users to whom the mail policy rules apply.	See Using Group LDAP Queries to Determine if a Recipient is a Group Member.
Step 4	(Optional) Define the default mail policies for incoming or outgoing messages.	See Configuring the Default Mail Policy for Incoming or Outgoing Messages , on page 7.
Step 5	Define the group of users for whom you want to set up user-specific mail policies.	Create an incoming or outgoing mail policy. See Configuring Mail Policies, on page 7 for more information.
Step 6	Configure the content security features and the content filter actions the email gateway takes on messages.	Configure the different content security features for the mail policy. • Content Filters: Applying the Content Filter to Messages for a Certain User Group • Anti-Virus: Configuring Virus Scanning Actions for Users • File Reputation Filtering and File Analysis: File Reputation Filtering and File Analysis • Anti-Spam: Defining Anti-Spam Policies • Graymail Detection and Safe Unsubscribe: Configuring the Incoming Mail Policy for

	Command or Action	Purpose
		Graymail Detection and Safe Unsubscribing • Outbreak Filters: The Outbreak Filters Feature and the Outbreak Quarantine • Data Loss Prevention: Using Outgoing Mail Policies to Assign DLP Policies to Senders and Recipients. • Threat Defense Connector: How to Configure Email Gateway to use Threat Defense Connector

Handling Incoming and Outgoing Messages Differently

The email gateway uses two different sets of mail policies for message content security:

- *Incoming mail policies* for messages are messages received from connections that match an ACCEPT HAT policy in any listener.
- *Outgoing mail policies* for messages are messages from connections that match a RELAY HAT policy in any listener. This includes any connection that was authenticated with SMTP AUTH.

Having separate sets of policies allow you to define different security rules for messages sent to your users and messages sent from your users. You manage these policies using the **Mail Policies > Incoming Mail Policies** or **Outgoing Mail Policies** pages in the GUI, or the policyconfig command in the CLI.

Note Some features can be applied only to incoming or to outgoing mail policies. For example, Data Loss Prevention scanning can only be performed on outgoing messages. Advanced Malware Protection (File Reputation scanning and File Analysis) is available in Incoming Mail Policies and Outgoing Mail Policies.

In certain installations, "internal" mail being routed through the Cisco appliance may be considered *outgoing* , even if all the recipients are addressed to internal addresses. For example, by default for C170 and C190 appliances, the system setup wizard will configure only one physical Ethernet port with one listener for receiving inbound email and relaying outbound email.

Matching Users to a Mail Policy

As messages are received by the email gateway, the email gateway attempts to match each message recipient and sender to a mail policy in the Incoming or Outgoing Mail Policies table, depending on whether it is an incoming or outgoing message.

Matches are based on the recipient's address, the sender's address, or both:

- *Recipient address* matches the Envelope Recipient address

  When matching recipient addresses, the recipient addresses entered are the final addresses after processing by preceding parts of the email pipeline. For example, if enabled, the default domain, LDAP routing or

masquerading, alias table, domain map, and message filters features can rewrite the Envelope Recipient address and may affect whether the message matches a mail policy.

- *Sender address* matches:
  - Envelope Sender (RFC821 MAIL FROM address)
  - Address found in the RFC822 From: header
  - Address found in the RFC822 Reply-To: header

Addresses may be matched on either a full email address, user, domain, or partial domain, and addresses may also match LDAP group membership.

Related Topics

- First Match Wins, on page 4
- Examples of Policy Matching, on page 4

First Match Wins

Each user (sender or recipient) is evaluated for each mail policy defined the appropriate mail policy table in a top-down fashion.

For each user, the first matching policy wins. If a user does not match any specific policy, user will automatically match the default policy of the table.

If a match is made based on a sender address, all remaining recipients of a message will match that policy. (This is because there can be only one sender per message.)

The envelope sender and the envelope recipeint have a higher priority over the sender header when you match a message to a mail policy. If you configure a mail policy to match a specific user, the messages are automatically classified into the mail policy based on the envelope sender and the envelope recipient.

Examples of Policy Matching

The following examples help show how the policy tables are matched in a top-down fashion.

Given the following Incoming Mail Email Security Policy table shown in the following table, incoming messages will match different policies.

Table 1: Policy Matching Example

Order	Policy Name	Users	
		Sender	Recipient
1	special_people	ANY	joe@example.com ann@example.com
2	from_lawyers	@lawfirm.com	ANY
3	acquired_domains	ANY	@newdomain.com @anotherexample.com

Order	Policy Name	Users	
4	engineering	ANY	PublicLDAP.ldapgroup: engineers
5	sales_team	ANY	jim@john@larry@
6	Default Policy	ANY	ANY

Related Topics

- Example 1, on page 5
- Example 2, on page 5
- Example 3, on page 5

Example 1

A message from sender `bill@lawfirm.com` sent to recipient `jim@example.com` matches:

- Policy #2 when the user description matches the sender (`@lawfirm.com`) and the recipient (ANY).
- Policy #2 when the envelope sender is `bill@lawfirm.com`.
- Policy #5 when the header sender is `bill@lawfirm.com` but the enveloper sender does not match `@lawfirm.com`.

Example 2

Sender `joe@yahoo.com` sends an incoming message with three recipients: `john@example.com`, `jane@newdomain.com`, and `bill@example.com` :

- The message for recipient `jane@newdomain.com` will receive the anti-spam, anti-virus, outbreak filters, and content filters defined in policy #3.
- The message for recipient `john@example.com` will receive the settings defined in policy #5.
- Because the recipient `bill@example.com` does not match the engineering LDAP query, the message will receive the settings defined by the default policy.

This example shows how messages with multiple recipients can incur *message splintering* . See Message Splintering, on page 6 for more information.

Example 3

Sender `bill@lawfirm.com` (`bill@lawfirm.com` is used for envelope sender) sends a message to recipients `ann@example.com` and `larry@example.com` :

- The recipient `ann@example.com` will receive the anti-spam, anti-virus, outbreak filters, and content filters defined in policy #1.
- The recipient `larry@example.com` will receive the anti-spam, anti-virus, outbreak filters, and content filters defined in policy #2, because the sender (`@lawfirm.com`) and the recipient (`ANY`) matches.

Message Splintering

Intelligent message splintering is the mechanism that allows for differing recipient-based content security rules to be applied independently to message with multiple recipients.

Each recipient is evaluated for each policy in the appropriate mail policy table (Incoming or Outgoing) in a top-down fashion.

Each policy that matches a message creates a new message with those recipients. This process is defined as *message splintering* :

- If some recipients match different policies, the recipients are grouped according to the policies they matched, the message is split into a number of messages equal to the number of policies that matched, and the recipients are set to each appropriate "splinter."
- If all recipients match the same policy, the message is not splintered. Conversely, a maximum splintering scenario would be one in which a single message is splintered for each message recipient.
- Each message splinter is then processed by anti-spam, anti-virus, Advanced Malware Protection (incoming messages only), DLP scanning (outgoing messages only), Outbreak Filters, and content filters independently in the email pipeline.

The following table illustrates the point at which messages are splintered in the email pipeline.

<table>
<tr><td rowspan="9">Work Queue</td><td>Message Filters
<code>(filters)</code></td><td rowspan="9">Email Security Manager Scanning (Per Recipient)</td><td>↓ Message for all recipients</td></tr>
<tr><td>Anti-Spam
<code>(antispamconfig, antispamupdate)</code></td><td rowspan="8">Messages are splintered immediately after message filter processing but before anti-spam processing:
Message for all recipients matching policy 1
Message for all recipients matching policy 2
Message for all other recipients (matching the default policy)
Note
DLP scanning is only performed on outgoing messages.</td></tr>
<tr><td>Anti-Virus
<code>(antivirusconfig, antivirusupdate)</code></td></tr>
<tr><td>File Reputation and Analysis (Advanced Malware Protection)
<code>(ampconfig)</code></td></tr>
<tr><td>Graymail Management</td></tr>
<tr><td>Content Filters
<code>(policyconfig -> filters)</code></td></tr>
<tr><td>Outbreak Filters
<code>(outbreakconfig, outbreakflush, outbreakstatus, outbreakupdate)</code></td></tr>
<tr><td>Data Loss Prevention
<code>(policyconfig)</code></td></tr>
</table>

Note New MIDs (message IDs) are created for each message splinter (for example, MID 1 becomes MID 2 and MID 3). For more information, see the "Logging" chapter. In addition, the `trace` function shows which policies cause a message to be split.

Policy matching and message splintering in Email Security Manager policies obviously affect how you manage the message processing available on the email gateway.

Related Topics

- Managed Exceptions, on page 7

Managed Exceptions

Because the iterative processing of each splinter message impacts performance, Cisco recommends configuring your content security rules on a *managed exception* basis. In other words, evaluate your organization's needs and try to configure the feature so that the majority of messages will be handled by the default mail policy and the minority of messages will be handled by a few additional "exception" policies. In this manner, message splintering will be minimized and you are less likely to impact system performance from the processing of each splinter message in the work queue.

Configuring Mail Policies

Mail policies map different user groups to specific security settings, such as Anti-Spam or Anti-Virus.

Related Topics

- Configuring the Default Mail Policy for Incoming or Outgoing Messages , on page 7
- Creating a Mail Policy for a Group of Senders and Recipients, on page 8
- Finding Which Policies Apply to a Sender or Recipient, on page 11

Configuring the Default Mail Policy for Incoming or Outgoing Messages

The default mail policies apply to messages that are not covered by any other mail policy. If no other policies are configured, the default policies apply to all messages.

Before You Begin

Understand how you can define the individual security services for the mail policy. See How to Enforce Mail Policies on a Per-User Basis, on page 2.

Procedure

Step 1 Depending on your requirements, choose one of the following:

- **Mail Policies > Incoming Mail Policies**
- **Mail Policies > Outgoing Mail Policies.**

Step 2 Click the link for the security service you want to configure for the Default mail policy.

Note
For default security service settings, the first setting on the page defines whether the service is enabled for the policy. You can click "Disable" to disable the service altogether.

Step 3 Configure the settings for the security service.

Step 4 Click **Submit**.

Step 5 Submit and commit your changes.

Creating a Mail Policy for a Group of Senders and Recipients

Before You Begin

- Understand how you can define the individual security services for the mail policy. See How to Enforce Mail Policies on a Per-User Basis, on page 2.
- Remember that each recipient is evaluated for each policy in the appropriate table (incoming or outgoing) in a top-down fashion. See First Match Wins, on page 4 for more information.
- (Optional) Define the delegated administrators who will be responsible for managing the mail policy. Delegated administrators can edit a policy's Anti-Spam, Anti-Virus, Advanced Malware Protection, and Outbreak Filters settings and enable or disable content filters for the policy. Only operators and administrators can modify a mail policy's name or its senders, recipients, or groups. Custom user roles that have full access to mail policies are automatically assigned to mail policies.

Procedure

Step 1 Choose **Mail Policies > Incoming Mail Policies** or **Mail Policies > Outgoing Mail Policies.**

Step 2 Click **Add Policy**.

Step 3 Enter a name for the mail policy.

Step 4 (Optional) Click the Editable by (Roles) link and select the custom user roles for the delegated administrators who will be responsible for managing the mail policy.

Step 5 Define users for the policy. For instructions to define users, see Defining Senders and Recipients for Mail Policies, on page 9.

Step 6 Click **Submit**.

Step 7 Click the link for the content security service you want to configure for the mail policy.

Step 8 From the drop-down list, select the option to customize the settings for the policy instead of using the default settings.

Step 9 Customize the security service settings.

Step 10 Submit and commit your changes.

What to do next

Related Topics

- Defining Senders and Recipients for Mail Policies, on page 9

- How to Configure the Email Gateway to Scan Messages for Spam

Defining Senders and Recipients for Mail Policies

You can define senders and recipients to whom the policy applies in the following ways:

- Full email address: `user@example.com`
- Partial email address: `user@`
- All users in a domain: `@example.com`
- All users in a partial domain: `@.example.com`
- By matching an LDAP Query

Note Entries for users are case-insensitive in both the GUI and CLI in AsyncOS. For example, if you enter the recipient `Joe@` for a user, a message sent to `joe@example.com` will match.

While defining senders and recipients for mail policies, keep in mind that:

- You must specify at least one sender and recipient.
- You can set the policy to match if,
  - The message is from any sender, one or more of the specified senders, or none of the specified senders.
  - The message is sent to any recipient, one or more of the specified recipients, or all of the specified recipients and none of the specified recipients.

Procedure

Step 1 Under **Users** section, click **Add User**.

Step 2 Define the senders for the policy. Choose one of the following options:

- **Any Sender**. The policy is matched if the message is from any sender.
- **Following Senders**. The policy is matched if the message is from one or more of the specified senders. Select this option and enter sender details in the text box or choose an LDAP group query.
- **Following Senders are Not**. The policy is matched if the message is not from none of the specified senders. Select this option and enter sender details in the text box or choose an LDAP group query.

To understand how sender conditions are set while choosing the above fields, see Examples, on page 10.

Step 3 Define the recipients for the policy. Choose one of the following options:

- **Any Recipient**. The policy is matched if the message is sent to any recipient.
- **Following Recipients**. The policy is matched if the message is sent to the specified recipients. Select this option, enter the recipient details in the text box or choose an LDAP group query.

You can choose whether policy is matched if the message is sent to one or more of the specified recipients or all of the specified recipients. Choose one of the following options from the drop-down list: **If one more conditions match** or **Only if all conditions match**.

- **Following Recipients are Not**. The policy is matched if the message is sent to none of the specified recipients. Select this option, enter the recipient details in the text box or choose an LDAP group query.

Note
You can configure this option only if you have selected **Following Recipients** and chosen **Only if all conditions match** from the drop-down list.

To understand how recipient conditions are set while choosing the above fields, see Examples, on page 10.

Step 4 Click **Submit**.

Step 5 Review the selected conditions on the **Users** section.

What to do next

Related Topics

- Creating a Mail Policy for a Group of Senders and Recipients, on page 8
- Examples, on page 10

Examples

The following table describes how conditions are set when you choose various options on the Add User page.

Sender			Recipient			Condition
Any Sender	**Following Senders**	**Following Senders are Not**	**Any Recipient**	**Following Recipients**	**Following Recipients are Not**	
Selected	-	-	-	Selected (Default) **Only if all conditions match** option is selected Values: `user1@`, `user2@`	-	**Sender**: Any **Recipient**: `user1@[AND]user2@`

-	Selected
	Values:
	`u1@a.com`,
	`u2@a.com`
		-	-	Selected
				(Default) **Only if all conditions match** option is selected
				Values:
				`u1@b.com`,
				`u2@b.com`
					Selected
					Values:
					`u3@b.com`,
					`u4@b.com`
						Sender:
						`u1@a.com[OR]u2@a.com`
						Recipient:
						`[u1@b.com[AND]u2@b.com]`
						`[AND]`
						`[[NOT]`
						`[u3@b.com[AND]u4@b.com]]`

-	-	Selected
		Values:
		`u1@a.com,`
		`u2@a.com`
			-	Selected
				If one or more conditions match option is also selected
				Values:
				`u1@b.com,`
				`u2@b.com`
					-	**Sender**:
						`[NOT] [u1@a.com[OR]u2@a.com]`
						Recipient:
						`u1@b.com [OR] u2@b.com`

Related Topics

- Defining Senders and Recipients for Mail Policies, on page 9

Finding Which Policies Apply to a Sender or Recipient

Use the Find Policies section at the top of the Mail Policies page to search for users already defined in incoming or outgoing mail policies.

For example, type bob@example.com and click the Find Policies button to display results showing which policies contain defined users that will match the policy.

Click the name of the policy to edit the users for that policy.

Note that the default policy will always be shown when you search for any user, because, by definition, if a sender or recipient does not match any other configured policies, it will *always* match the default policy.

Related Topics

- Managed Exceptions, on page 7

Managed Exceptions

Using the steps shown in the two examples above, you can begin to create and configure policies on a *managed exception* basis. In other words, after evaluating your organization's needs you can configure policies so that the majority of messages will be handled by the default policy. You can then create additional "exception" policies for specific users or user groups, managing the differing policies as needed. In this manner, message splintering will be minimized and you are less likely to impact system performance from the processing of each splinter message in the work queue.

You can define policies based on your organizations' or users' tolerance for spam, viruses, and policy enforcement. The following table outlines several example policies. "Aggressive" policies are designed to minimize the amount of spam and viruses that reach end-users mailboxes. "Conservative" policies are tailored to avoid false positives and prevent users from missing messages, regardless of policies.

Table 2: Aggressive and Conservative Email Security Manager Settings

	Aggressive Settings	Conservative Settings
Anti-Spam	Positively identified spam: Drop Suspected spam: Quarantine Marketing mail: Deliver and prepend " `[Marketing]` " to the subject messages	Positively identified spam: Quarantine Suspected spam: Deliver and prepend " `[Suspected Spam]` " to the subject of messages Marketing mail: Disabled
Anti-Virus	Repaired messages: Deliver Encrypted messages: Drop Unscannable messages: Drop Infectious messages: Drop	Repaired messages: Deliver Encrypted messages: Quarantine Unscannable messages: Quarantine Infectious messages: Drop
Advanced Malware Protection **(File Reputation Filtering and File Analysis)**	Unscanned attachments: Drop Messages with Malware Attachments: Drop Messages with pending File Analysis: Quarantine	Unscanned attachments: Deliver and prepend " `[WARNING: ATTACHMENT UNSCANNED]` " to the subject of messages. Messages with Malware Attachments: Drop Messages with pending File Analysis: Deliver and prepend " `[WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]` " to the subject of messages.
Virus Filters	Enabled, no specific filename extensions or domains allowed to bypass Enable message modification for all messages	Enabled with specific filename extensions or domains allowed to bypass Enable message modification for unsigned messages

Setting Priority for Message Headers

You can set the priority for a message header to match the incoming and outgoing messages in your email gateway.

Important You can set the priority in which the email gateway checks for message headers in the incoming and outgoing messages. The email gateway first checks for the message header with the highest priority for all the mail policies. If there is no header match in any of the mail policies, the email gateway looks for the next message header in the priority list for all the mail policies. If none of the message headers match in any of the mail policies, the default mail policy settings are used.

Procedure

Step 1 Go to **Mail Policies** > **Mail Policy Settings**.

By default, the Envelope Sender header is set to a priority 1. You can click on the Envelope Sender link to change the priority.

Step 2 Click **Add Priority** and check the appropriate header name (for example, Header “From’”) check box to add a new priority.

Step 3 Click **Submit** and commit your changes.