What kind of actions can I apply to an email message using message filters?

TAC   **Document ID: 118100**

Contributed by John Yu and Robert Sherwin, Cisco TAC Engineers.

Jul 29, 2014

Contents

Introduction

This document describes actions that can be applied to messages as they are processed through message filters on the Email Security Appliance (ESA).

What kind of actions can I apply to an email message using message filters?

Message filters allow you to create special rules describing how to handle messages as they are received by the ESA. A message filter specifies that a certain kind of email message should be given special treatment. Message filters also allow you to enforce corporate email policy by scanning the content of messages for words you specify.

Message filters support two types of actions: non−final and final.

- Non−final actions performs an action which permits the message to be processed further.
- Final action ends the processing of a message, and permits no further proccessing through subsequent filters.

Non−final message filter actions are cumulative. If a message matches multiple filters where each filter specifies a different action, then all actions are accumulated and enforced. However, if a message matches multiple filters specifying the same action, the prior actions are overridden and the final filter action is enforced.

Note: Message filters are similar to mail policy content filters, but are configured via the CLI only. Message filter are able to take certain actions that are not available to content filters. Message filters are applied on the ESA only.

Tip: Please see the "Using Message Filters to Enforce Email Policies" chapter of the AsyncOS User Guide for complete and detailed information, including message filter examples.

Non−Final Actions

- Alter source host: ***alt−src−host***
- Alter recipient: ***alt−rcpt−to***
- Alter mailhost: ***alt−mailhost***
- Notify: ***notify***
- Notify Copy: ***notify−copy***
- Blind carbon copy: ***bcc***
- Blind carbon copy with scan: ***bcc−scan***
- Archive: ***log***
- Quarantine: ***quarantine (quarantine_name)***
- Duplicate (Quarantine): ***duplicate−quarantine(quarantine_name)***
- Remove headers: ***strip−header***
- Insert headers: ***insert−header***
- Edit header text: ***edit−header−text***
- Edit body text: ***edit−body−txt()***
- Convert HTML: ***html−convert()***
- Assign bounce profile: ***bounce−profile***
- Bypass Anti−Spam System: ***skip−spamcheck***
- Bypass Anti−Virus System: ***skip−viruscheck***
- Bypass Outbreak Filter Scanning: ***skip−vofcheck***
- Drop Attachments by Name: ***drop−attachments−by−name***
- Drop Attachments by Type: ***drop−attachments−by−type***
- Drop Attachments by File Type: ***drop−attachments−by−filetype***
- Drop Attachments by MIME Type: ***drop−attachments−by−mimetype***
- Drop Attachments by Size: ***drop−attachments−by−size***
- Drop Attachments by Content: ***drop−attachments−where−contains***
- Drop Attachments by Dictionary Match: ***drop−attachments−where−dictionary−match***
- Add Footer: ***add−footer(footer−name)***
- Add Heading: ***add−heading(heading−name)***
- Encrypt on Delivery: ***encrypt−deferred***
- Add Message Tag: ***tag−message(tag−name)***
- Add Log Entry: ***log−entry***

Note: For URL specific message filters, use a separate action to handle the case in which the reputation service does not provide a score for a URL.

- Replace URL with text, based on URL reputation: ***url−reputation−replace*** *or* ***url−no−reputation−replace***
- Defang URL based on URL reputation: ***url−reputation−defang*** *or* ***url−no−reputation−defang***
- Redirect URL to a Cisco security proxy, based on URL reputation: ***url−reputation−proxy−redirect*** *or* ***url−no−reputation−proxy−redirect***
- Replace URL with text, based on URL Category: ***url−category−replace***
- Defang URL based on URL category: ***url−category−defang***
- Redirect URL to Cisco security proxy, based on URL category: ***url−category−proxy−redirect***
- No Operation: ***no−op***

Final Actions

- Skip Remaining Message Filters: ***skip−filters***
- Drop message: ***drop***
- Bounce message: ***bounce***
- Encrypt and Deliver Now: ***encrypt***

Related Information

- *Cisco Email Security Appliance − End−User Guides*
- *Technical Support & Documentation − Cisco Systems*