Working with Message Filters

Contents

[Introduction](#)
[Prerequisites](#)
[Advantages of Using Message Filters](#)
[Related Information](#)

Introduction

This article goes over best practices and implementation regarding Message Filters on the Email Security Appliance (ESA). Message filters allow the creation of special rules describing how to handle messages that meet specific conditions as they are received and processed by the ESA.

Prerequisites

- Basic understanding of ESA filter operation
- Familiarity with the Command Line Interface (CLI) on the ESA

Advantages of Using Message Filters

There are two major advantages of using Message Filters over Content Filters :

1. They are applied to messages towards the beginning of the workqueue processing pipeline. Due to this, we can potentially save a large number of resources by filtering messages before any major scanning engines are utilized (ie: Anti-Spam, Anti-Virus, AMP, Etc.).
2. They will take action on both Incoming and Outgoing traffic, whereas for Content Filters you would need to create one for Incoming and one for Outgoing.

Also, there are few conditions that aren't available to be configured using Content Filters which can be done only via Message Filters.

Example: If there is a requirement to define conditions based on ESA's Sendergroup, that option is available only in Message Filters.

> **Note**: 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.

Operations of Message Filters

When AsyncOS processes message filters, the content that AsyncOS scans, the order of the processing, and the actions taken are based on several factors:

- Message Filters are processed in the order they are configured (Top to Bottom aKa First to

Last)

- A Message filter will be processed on the message content at the time when it reaches the filter.
- When you match a regular expression, you configure a “score” to tally up the number of times a match must occur before a filter action is taken. This allows you to “weigh” the responses to different terms.
- The major alternates in linking conditions of a Message Filter are : **(AND / OR / IF / ELSE)**

Creating Message Filters

```
partha.cisco.com> filters


Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]>
```

First, we issue the command **filters** from the CLI to enter the configuration mode of Message Filters. Then the options are :

- **NEW**: This option is to begin the creation of a new filter. This option selection is followed by Filter name and then the syntax.
- **DELETE**: This option is to delete an existing filter as per need. After issuing this command, you may enter the filter name of sequence number to delete
- **IMPORT**: You can import a filters’ related file saved in the appliance directory.
- **EXPORT**: This option allows to export the filters’ related file, to be imported to another destination
- **MOVE**: This option allows to modify a filter’s order as per preference
- **SET**: This option allows us to change the status of a filter from Active to Inactive and vice-versa
- **LIST**: This option will display all the created filters present in the ESA
- **DETAIL**: This option allows us to see the components of the filter created, such as the conditions and the actions defined.

- **LOGCONFIG**: This option displays the logfile names created for message filters that had actions defined as an archive (‘folder name”)

- **ROLLOVERNOW**: This option allows to roll over all the logs present in the folders that are created due to the archive action defined in message filters

Filters can be created in all modes of ESA such as **Cluster**, **Group** or **Machine** mode.

The criteria of config preference in which the ESA will apply the filters to the emails will be as beneath :

1st Preference: Machine mode

2nd Preference: Group Mode

3rd Preference: Cluster mode

For creating of Message Filters, we need a combination of syntax to define conditions and actions :

Example:

```
if (recv-listener == 'InboundMail' or recv-int == 'notmain')

{

skip-filters();

}

else

{

quarantine(“Policy”);

}

.
```

The above filter depicts that if the receiving listener is 'InboundMail' OR the receiving interface is 'notmain' then the action will be to skip any remaining message filters.

If the conditions don’t match, then quarantine to Policy. This is defined after else.

Helpful Tips

At times, the syntax to be used in Message Filters may get confusing, but an easy reference point for the same could be Content Filters.

We can create a Content Filter with conditions and actions that we want in the Message Filter. After we submit the filter, in the next page we will see 3 tabs at the top of the filters section namely:

- Description

- Rules
- Policies

When we click on the tab **Rules**, that will show us the syntax that the filter uses and the same can be used to create Message Filters. That's the simplest way to narrow down the syntax for filter conditions as per our requirement.

Regular Expression Used in Message Filters

- **Carat (^)**: rules containing the caret symbol (^) only match the beginning of the string.

Example: **^I'm** will match I'm an engineer

- **Dollar sign ($):** Rules containing the dollar sign character ($) only match the end of the string

Example: **.com$** will match google.com as well as yahoo.com

- **Period character (.):** Rules containing a period character (.) match any character (except a new line).

Example: The regular expression **^...admin$** matches the string macadmin as well as the string sunadmin but not win32admin.

- **Asterisk (*) directive:** Rules containing an asterisk (*) match "zero or more matches of the previous directive." In particular, the sequence of a period and an asterisk (.*) matches any sequence of characters (not containing a new line).

Example: The regular expression **^P.*Piper$** matches all of these strings: PPiper, Peter Piper, P.Piper

- **Backslash special characters (\)**: The backslash character *escapes* special characters. Thus the sequence \. only matches a literal period, the sequence \$ only matches a literal dollar sign, and the sequence \^ only matches a literal caret symbol.

Example: The regular expression **^ik\\.ac\\.uk$** only matches the string ik.ac.uk

- **Case-insensitivity ((?i))**: The token (?i) that indicates the rest of the regular expression should be treated in case-insensitive mode.

Example: The regular expression **(?i)cisco** matches Cisco, CISCO as well as cisco

- **Or (|):** The "or" operator. If A and B are regular expressions, the expression "A|B" will match any string that matches either "A" or "B."

Example: The expression **"foo|bar"** will match either **foo or bar**, but not foobar.

Related Information

[Cisco Email Security Appliance - End-User Guides]