# Differences Between Message Filters and Content Filters on the ESA

**Document ID: 117825**

Contributed by Tomki Camp and Enrico Werner, Cisco TAC Engineers.
Jun 23, 2014

## Contents



## Introduction

This document describes the differences between Message Filters and Content Filters in the Cisco Email Security Appliance (ESA), and it describes which filter is better for which type of action.

## Differences Between Message Filters and Content Filters

Message Filters and Content Filters use the same scripting language and regular−expression matching.

### Content Filters

Content Filters support a subset of the rules and actions used by Message Filters. Content Filters include all of the rules and actions needed in order to identify and act upon the content of a message, and they are easy to configure in the GUI.

### Message Filters

Message Filters are more flexible and give access to the metadata of a message, such as the receiving listener, the sender IP, the SenderBase reputation score of the sender, the number of recipients in the message, the size of the message or attachments. A subset of the metadata is available in Content Filters as well. Message Filters are applied as the ***first*** Policy processing step in the ESA email pipeline. When a Message Filter is applied, its actions apply to all recipients of the message. This means that, if the action is Drop, then no recipient receives the message, even if the rule that matched the message matched only one recipient.

### Actions for All Recipients

Content Filters are applied as the ***last*** Policy processing step in the email pipeline, after messages have been ***splintered*** into separate copies depending on the Mail Policies (and therefore different recipient groups) defined in your configuration.  Because of this, Content Filters can be applied to a more finely−grained group of senders or recipients. If you perform an action on all recipients, it is therefore more efficient to do so in a Message Filter before message splintering takes place. This is especially true in the case of content scanning (body−contains or attachment−contains rule), or if the action is to drop or bounce a message, which would then avoid anti−spam and anti−virus scanning on a message destined for non−delivery.