ESA Message Filter Action Descriptions

Document ID: 117857

Contributed by Tomki Camp and Enrico Werner, Cisco TAC Engineers.
Jun 26, 2014

Contents

Introduction

This document describes the differences between the drop−attachments−by−name, −type, −filetype, and −mimetype message filter actions on the Cisco Email Security Appliance (ESA).

Message Filter Action Overview

Messages that are sent using MIME can have labels assigned to various body parts, which are often called attachments. These labels can (and do) conflict with each other in the information they provide. In addition, a body part might have its own characteristics. For example, a user might take a JPEG image, attach it to a mail message, give it a MIME type of ***text/html***, and mark it with a MIME filename of ***jan.mp3***. All of these labels conflict with the reality of what the attachment is.

For example, consider this message header:

```
Boundary_(ID_n6BU1raweF+4UwCeweFmVQ)
Content−type: application/msword; name="eval form.doc"
Content−transfer−encoding: BASE64
Content−disposition: attachment; filename="eval form.doc"
Content−description: eval form.doc
```

In this case, the MIME filenames and MIME types are all consistent and might or might not match the actual format of the body part (attachment). However, in this header, there are inconsistencies:

```
Boundary_(ID_n6BU1raweF+4UwCeweFmVQ)
Content−type: image/jpeg; name="eval form.doc"
Content−transfer−encoding: BASE64
Content−disposition: attachment; filename="evaluation.zip"
Content−description:  These are the latest warez, d00d.
```

For well−formed messages, implementing policy is fairly easy. But in the case of someone either intentionally or unintentionally trying to bypass policy, additional flexibility is required.

Network managers often want to drop attachments of a particular type, such as all MP3 files. However, implementing this policy means that you have to decide which of the labels you want to pay attention to (if any of them). AsyncOS gives you the flexibility to look at the MIME type (such as *text/html*), the MIME filename (such as *jan.mp3*), and to actually *fingerprint* the attachment in order to try and determine what the true format is. When implementing your policy using message filters or content filters, you might want to use one or more of these labels.

Message Filter Action Descriptions

Here are the message filter action descriptions:

- ***drop−attachments−by−name*** − Checks the filenames of each attachment in a message to see if it matches the given regular expression. The filename is taken from the MIME headers. This comparison is case−sensitive. If one of the message attachments matches the filename, this rule returns ***true***. If an attachment is an archive, the IronPort C−Series appliance will harvest the file names from inside the archive and apply ***scanconfig*** rules (by default, MIME types of video/*, audio/* and image/* are not scanned, and nothing over 5 MB is scanned) accordingly.

- ***drop−attachments−by−type*** − Drops all attachments on messages that have a MIME type, determined by either the given MIME type or the file extension. Archive file attachments (zip, tar) will be dropped if they contain a file that matches.

- ***drop−attachments−by−filetype*** − Examines attachments based on the fingerprint of the file, and not just the three−letter filename extension. This is similar to the UNIX file command. In addition to individual file types that can be specified, the group expressions Compressed, Document, Executable, Image, and Media include all file types of the general type. For example, the *Executable* group includes .exe, .java .msi .pif, .dll, .scr, and.com files. Please refer to the AsyncOS User Guide for a complete list of file types that can be specified.

- ***drop−attachments−by−mimetype*** − Drops all attachments on messages that have a given MIME type. This action does not attempt to ascertain the MIME type by file extension, so it also does not examine the contents of the archives.

Updated: Jun 26, 2014 Document ID: 117857