ESA Content Filters for Email Messages with Multiple Attachments

Document ID: 117821

Contributed by Enrico Werner, Cisco TAC Engineer.
Jul 01, 2014

Contents

Introduction

This document describes how the negative content filter conditions work for email messages that contain multiple attachments on the Cisco Email Security Appliance (ESA).

Problem

You use a content filter that allows certain types of email attachments, while other types of attachments should be marked for quarantine. When an email message arrives that has multiple attachments, one that should be allowed and another that should be marked for quarantine, the filter identifies the entire message as *allowed*.

Here is the content filter that is used:

```
if attachment filename != (list of attachments), then quarantine
```

This condition and action functions as intended if the email message has a single attachment, but it does not function properly for messages that contain multiple, different attachments.

Example Scenario

These are the types of attachments that are allowed:

- ***rar***
- ***pdf***
- ***jpg***

All other attachments should be sent to quarantine, as specified by the filter condition and action.

Filter Condition

Here is the filter condition that is used:

```
if attachment filename != (rar|pdf|jpg)
```

Filter Action

Here is the filter action that is used:

`quarantine`

The expectation typically is that if the email message contains a ***pdf*** attachment and a ***txt*** attachment, then it should be quarantined due to the ***txt*** attachment because it is not in the list of allowed attachments. However, this content filter does not function as intended because it matches the ***pdf*** attachment in the message and directly permits it, even though it has a ***txt*** attachment.

Solution

It is not possible to quarantine the email with the ***txt*** attachment for these reasons:

- The attachment conditions are for ***all*** of the attachments that are included in a message.
- The negative ***!=*** comparison verifies whether ***any*** of the attachments match.

As described, if ***any*** of the attachments are allowed, such as when they match the ***!=***, then the entire message is treated as *allowed*. There is no way around this; it is simply the way that these conditions work.

The only other solution is to invert the logic and block specific attachments, not just any attachment that is not white−listed.

Updated: Jul 01, 2014 Document ID: 117821