ESA邮件过滤器操作说明

目录

简介

本文档介绍思科邮件安全设备(ESA)上的丢弃附件（按名称）、-type、-filetype和 — mimetype邮件过滤器操作之间的区别。

邮件过滤器操作概述

使用MIME发送的邮件可以将标签分配到各种正文部分，这些部分通常称为附件。 这些标签在提供的信息中可能（并且确实）相互冲突。此外，车身部件可能具有自己的特性。 例如，用户可以获取JPEG图像，将其附加到邮件中，为其提供MIME类**型的**text/html，并使用MIME文件名**jan.mp3进行标记**。所有这些标签都与附件的真实性相冲突。

例如，请考虑以下消息报头：

```
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
```

在这种情况下，MIME文件名和MIME类型都是一致的，可能或可能与正文部分（附件）的实际格式不匹配。但是，在此报头中存在不一致：

```
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.
```

对于格式良好的信息而言，实施政策相当容易。但是，如果有人有意或无意尝试绕过策略，则需要额外的灵活性。

网络管理员通常希望删除特定类型的附件，例如所有MP3文件。但是，实施此策略意味着您必须确定要注意的标签（如果有）。 AsyncOS让您能够灵活地查看MIME类型(如*text/html*)、MIME文件名(如*jan.mp3*)，并实际为附件*指纹*，以便尝试确定真正的格式。当使用邮件过滤器或内容过滤器实施策略时，您可能希望使用一个或多个这些标签。

邮件过滤器操作说明

以下是邮件过滤器操作说明：

- **drop-attachments-by-name** — 检查邮件中每个附件的文件名，以查看其是否与给定的正则表达式匹配。文件名取自MIME报头。此比较区分大小写。如果其中一个邮件附件与文件名匹配，则此规则返回**true**。如果附件是存档文件，则IronPort C系列设备将从存档文件内部获取文件名并应用**scanconfig**规则（默认情况下，不扫描视频/*、音频/*和图像/*的MIME类型，并且不扫描超过5 MB的任何内容）。

- **drop-attachments-by-type** — 删除具有MIME类型的邮件上的所有附件，由给定MIME类型或文件扩展名确定。 如果存档文件附件(zip、tar)包含匹配的文件，则会将其删除。

- **drop-attachments-by-filetype** — 根据文件的指纹检查附件，而不仅是三字母文件扩展名。这类似于UNIX file命令。除了可以指定的单个文件类型外，组表达式“压缩”、“文档”、“可执行文件”、“图像”和“媒体”还包含通用类型的所有文件类型。例如，可执*行程*序组包括.exe、.java .msi .pif、.dll、.scr和.com文件。有关可指定的文件类型的完整列表，请参阅《AsyncOS用户指南》。

- **drop-attachments-by-mimetype** — 删除具有给定MIME类型的邮件上的所有附件。此操作不会尝试按文件扩展名确定MIME类型，因此也不会检查存档的内容。