ESA消息过滤器操作说明

目录

简介

本文描述丢弃附件由NAME之间的差异，型， -文件类型，和- mimetype在思科的消息过滤器操作给安全工具(ESA)发电子邮件。

消息过滤器操作概述

传送使用MIME的信息能有标签分配到多种身体局部，经常呼叫附件。 他们提供的这些标签能(和)彼此相冲突在信息。另外，身体局部也许有其自己的特性。 例如，用户也许采取JPEG镜像，附加它到邮件消息，给它**文本/html的**MIME类型和标记它用**jan.mp3** MIME文件名。所有这些标签相冲突以什么的实际情况附件是。

例如，请考虑此信息标题：

```
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类型全部一致，并且也许或者也许不匹配身体局部(附件)的实际格式。 然而，在此报头，有不一致：

```
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.
```

对于合格的消息，实现策略是非常容易的。但是一旦尝试的某人有意或无意绕过策略，另外的灵活性要求。

网络管理器经常要丢弃一种特定类型的附件，例如所有MP3文件。然而，实现此策略意味着您必须决定哪些标签您希望注意(如果任何一个)。AsyncOS提供您灵活性查看MIME类型(例如*文本/html*)，MIME文件名(例如*jan.mp3*)和实际上*指*纹附件为了尝试和确定什么真的格式是。当实现您的策略使用消息过滤或内容过滤器时，您也许要使用一个或很多这些标签。

消息过滤器操作说明

这是消息过滤器操作说明：

- **丢弃附件由NAME** -检查每个附件文件名在消息的发现是否匹配给的常规表示。文件名从MIME报头被采取。此比较区分大小写。如果其中一个消息附件匹配文件名，**真**此规则的回归。如果附件是存档， IronPort C系列设备从存档里边将收获文件名并且相应地运用**scanconfig**规则(默认情况下， video/*的MIME类型， audio/*和image/*没有被扫描，并且什么都在5 MB没有被扫描)。

- **丢弃附件由类型**-丢弃在有一个MIME类型的消息的所有附件，取决于二者之一给的MIME类型或文件扩展。 归档文件附件(邮政编码， tar)将丢弃，如果他们包含配比的文件。

- **丢弃附件由文件类型**-检查根据文件和不仅三个字母文件名扩展的指纹的附件。这类似于file命令的UNIX。除可以指定的单个文件类型之外，组表达式被压缩的，文档、可执行、镜像和梅迪亚包括普通类型的所有文件类型。例如，*可执行的*组包括.exe， .java .msi .pif， .dll， .scr， and.com文件。请参考可以指定文件类型的完整列表的AsyncOS用户指南。

- **丢弃附件由mimetype** -丢弃在有一个给的MIME类型的消息的所有附件。此操作不尝试由文件扩展确定MIME类型，因此也不检查存档的内容。