工作用消息过滤器

目录

简介

此条款在最佳实践和实施去关于消息过滤器在电子邮件安全工具(ESA)。消息过滤器允许描述如何的特殊规则的创建处理符合特定情况的消息，当他们由ESA接收并且处理。

先决条件

- ESA过滤器操作基本的了解
- 与命令行界面(CLI)的熟悉在ESA

使用消息过滤器优点

有使用在内容过滤器的消息过滤器两个主要优点：

1. 应用对往workqueue的开始处的消息处理渠道的他们。由于此，我们能通过过滤消息潜在节约很大数量的资源，在使用前所有主要扫描引擎(IE ：反垃圾邮件、防病毒、AMP等等)。
2. 他们将采取在流入的行动，并且流出流量，而对于内容过滤您将需要创建一流入的和一个流出的。

并且，有不是可用配置使用内容过滤器可以通过消息过滤器仅执行的少量情况。

示例：如果有需求定义根据ESA的Sendergroup的情况，该选项是仅可用的在消息过滤器。

> **Note**:非最终消息过滤器操作是渐增的。如果消息匹配每个过滤器指定一不同的操作的多个过滤器，则所有操作被累计并且被强制执行。然而，如果消息匹配指定同一操作的多个过滤器，前期操作被改写，并且最终过滤器操作被强制执行。

消息过滤器的操作

当AsyncOS处理消息过滤器时， AsyncOS扫描的内容，处理的顺序和采取的行动根据几个要素：

- 亦称他们配置的消息过滤器按顺序处理(由上至下首先持续)
- 当到达过滤器的时候，消息过滤器在消息内容将处理。
- 当您匹配常规表示时，您配置“分数”相符匹配必须发生的次数，在过滤器操作采取前。这允许您“斟酌”对不同的期限的答复。
- 在连接消息过滤器的情况的主要替代项是：**(并且/或者/IF/)**

创建消息过滤器

```
partha.cisco.com> filters


Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]>
```

首先，我们发出从CLI的命令**过滤器**输入消息过滤器配置模式。然后选项是：

- **新**：此选项是开始一个新的过滤器的创建。此选择由过滤器名称然后语法跟随。
- **删除**：此选项是删除一个现有过滤器根据需要。在发出此命令以后，您可以进入序号过滤器名称删除
- **导入**：您能导入在设备目录保存的过滤器的涉及的文件。
- **出口**：此选项准许导出过滤器的涉及的文件，导入到另一个目的地
- **移动**：此选项准许根据首选修改过滤器的命令
- **SET** ：此选项允许我们更改一个过滤器的状态从激活的到非激活和反过来也是一样地
- **列表**：此选项将显示所有已创建过滤器现在ESA
- **详细信息**：此选项允许我们发现过滤器的组件创建，例如定义的条件和操作。
- **LOGCONFIG** ：此选项显示为有作为存档定义的操作的消息过滤器创建的日志文件名称(`文件夹名称")
- **ROLLOVERNOW** ：此选项准许变成所有日志现在创建的归结于在消息过滤器定义的存档操作的文件夹

过滤器在ESA所有模式可以创建例如**集群**、**组**或者**计算机**模式。

的设置首选标准ESA将应用过滤器对电子邮件和下面：

第1首选：计算机模式

第2首选：组模式

第3首选：集群模式

对于创建消息过滤器，我们需要语法的组合定义情况和操作：

示例：

```
if (recv-listener == 'InboundMail' or recv-int == 'notmain')

{

skip-filters();

}

else

{

quarantine("Policy");

}
```

.
上述过滤器表示，如果接收的监听程序是'InboundMail'或接收接口是'notmain'然后操作将是跳过剩余的消息过滤器。

如果条件不配比，则请检疫对策略。这在以后定义。

有用提示

通常，用于消息过滤器的语法也许获得混乱，但是同样的一个容易参考点可能是内容过滤器。

我们能创建有我们在消息过滤器想要的情况和操作的内容过滤器。在我们提交过滤器后，在Next页我们将看到3选项卡在过滤器顶部区分即：

- 说明
- 规则
- 策略

当我们点击选项卡**规则**，那将显示我们语法过滤器用途和同样可以用于创建消息过滤器。那是简单方法根据我们的需求缩小过滤器情况的语法。

用于消息过滤器的常规表示

- **Carat (^)** ：包含脱字号符号(^)的规则只匹配字符串的开始处。

示例：^I上午将匹配我是工程师

- **美元的符号($)** ：包含美元的符号字符($)的规则只匹配字符串的末端

示例：.com $将匹配google.com以及yahoo.com

- **期限字符(。)** ：包含期限字符的规则(。)匹配所有字符(除了新的一行)。

示例：常规表示**^... admin$**匹配字符串macadmin以及字符串不是sunadmin，但是win32admin。

- **星号(*)方针**：包含星号(*)的规则匹配“上一个方针的零或更多匹配”。特别是，期限的顺序和星号(。*)匹配字符所有顺序(不包含新的一行)。

示例：常规表示**^P.*Piper$**匹配所有这些字符串：PPiper，彼得吹笛者， P.Piper

- **斜线特殊字符(\)** ：斜线字符特殊字符。因而顺序\。只匹配一个字面值期限，顺序\ $只匹配一个字面值美元的符号，并且顺序\ ^只匹配一个字面值脱字号符号。

示例：常规表示**^ik \ \ .ac \ \ .uk$**只匹配字符串ik.ac.uk

- **案例感觉迟钝((？i))** ：标记(？指示常规表示的其余的i)在不区分大小写模式应该对待。

示例：常规表示**(？我) cisco**匹配Cisco、CISCO以及cisco

- **或者(|)** ：“或”操作员。如果A和B是常规表达，表达式“A|B”将匹配匹配“A”或“B.”的所有字符串

示例： 表达式**“foo|柱状图”将**匹配**foo或**不是**柱状图**，但是foobar。

相关信息

[Cisco电子邮件安全工具-最终用户指南]