使用邮件过滤器实施邮件策略

邮件网关采用了一系列内容扫描和邮件过滤技术，可帮助您实施公司策略，并对进出企业网络的特定邮件加以处理。

本章介绍多种可用于策略实施的强大功能：内容扫描引擎、邮件过滤器、附件过滤器和内容词典。

本章包含以下部分：

概述

利用邮件过滤器，可以创建规定在邮件网关接收邮件时对邮件作何处理的特殊规则。邮件过滤器规定应区别对待每一类邮件。思科邮件过滤器还可以扫描邮件内容中是否存在指定词语，通过这种方式实施公司邮件策略。本章包含以下各节：

- **邮件过滤器的要素**。利用邮件过滤器，可创建规定在收到邮件时对邮件作何处理的特殊规则。过滤器规则根据邮件或附件内容、有关网络的信息、邮件信封、邮件信头或邮件正文识别邮件。过滤操作可生成通知，也可以丢弃、退回、存档、密件抄送或修改邮件。有关详细信息，请参阅邮件过滤器的要素, on page 2。
- **处理邮件过滤器**。AsyncOS 处理邮件过滤器时，AsyncOS 扫描的内容、处理顺序以及执行的操作取决于多种因素，其中包括邮件过滤器顺序、任何可能改变邮件内容的预处理、邮件的MIME结构、为内容匹配配置的阈值得分以及查询结构。有关详细信息，请参阅邮件过滤器处理, on page 4。

- **邮件过滤器规则**。每个过滤器都有一个规则，用于定义过滤器可对其执行操作的邮件集合。可以在创建邮件过滤器时定义这些规则。有关详细信息，请参阅邮件过滤器规则, on page 2。
- **邮件过滤器操作**。每个过滤器都有在规则求出 true 值时对邮件执行的操作。可以执行的操作分为两类：最终操作（如传送、丢弃或退回邮件）和允许邮件进一步处理的非最终操作（如删除或插入信头）。有关详细信息，请参阅邮件过滤器操作, on page 2。
- **附件扫描邮件过滤器**。附件扫描邮件过滤器可删除邮件中不符合公司策略的附件，同时继续传送原始邮件。可以根据附件的特定文件类型、指纹或内容过滤附件。使用图像分析器，您还可以扫描图像附件。图像分析器使用测量图像属性的算法来确定不适当内容的可能性。这些算法可以检测图像中的形状和颜色面板。分析器可以识别图像中的形状类型以及任何肤色相对于图像中其他颜色的百分比，以帮助识别不适当的内容。肤色颜色百分比较高的图像更有可能是不适当的内容。这些算法不会以任何方式进行区分。有关详细信息，请参阅附件扫描, on page 86。
- **使用 CLI 管理邮件过滤器**。CLI 支持将命令与邮件过滤器搭配使用。例如，您可能需要显示、重新排序、导入或导出邮件过滤器列表。有关详细信息，请参阅使用 CLI 管理邮件过滤器, on page 97。
- **邮件过滤器示例**。本节介绍一些真实的过滤器示例及其相关的简要说明。有关详细信息，请参阅 邮件过滤器示例, on page 112。

邮件过滤器的要素

利用邮件过滤器，可创建规定在收到邮件时对邮件作何处理的特殊规则。邮件过滤器包括邮件过滤器规则和邮件过滤操作。

相关主题

- 邮件过滤器规则, on page 2
- 邮件过滤器操作, on page 2
- 邮件过滤器示例语法, on page 3

邮件过滤器规则

邮件过滤器规则决定过滤器将应用于的邮件。可以使用逻辑连接符 AND、OR 和 NOT 组合规则来创建更复杂的测试。此外，还可以使用括号组合规则表达式。

邮件过滤器操作

邮件过滤器的目的是对所选邮件执行操作。

操作分为两类：

- 最终操作（例如，传送、删除以及退回）会结束邮件处理，并且不允许通过后续过滤器对邮件做更多处理。
- 非最终操作，允许对邮件做进一步处理。

Note 非最终邮件过滤器操作可以累积。如果邮件与多个过滤器匹配，且每个过滤器都指定了不同的操作，那么这些操作会累积，并一并实施。但是，如果邮件与指定相同操作的多个过滤器匹配，那么前面的操作将被覆盖，只执行最终过滤器操作。

相关主题

- “过滤器操作”摘要表, on page 55
- 操作变量, on page 64
- 匹配内容可视性, on page 66
- 邮件过滤器操作说明和示例, on page 67

邮件过滤器示例语法

过滤器规范的字面意思是：

如果邮件与规则匹配，则按顺序执行操作。如存在 else 子句，则在邮件与规则不匹配时执行 else 子句中的操作。

为过滤器指定名称有助于您在激活、停用或删除过滤器时更轻松地管理过滤器。

邮件过滤器使用以下语法：

语法示例	目的
expedite：	过滤器名称
if (recv-listener == 'InboundMail' or recv-int == 'notmain')	规则说明

`{`
`  alt-src-host('outbound1');`
`skip-filters();`
`}`
	操作规范

`else`
`{`
`  alt-src-host('outbound2');`
`}`
	可选备用操作说明

注意，可以忽略所有备用操作：

语法示例	目的
expedite2:	过滤器名称
`if ((not (recv-listener == 'InboundMail')) and` (not (recv-int == 'notmain')))	规则说明

语法示例	目的

{
alt-src-host('outbound2');
skip-filters();
}
 	
	操作规范

您可以在一个文本文件中按顺序逐个添加多个过滤器。

必须将过滤器中的值包含在单引号或双引号中。值两端的单引号或双引号必须成对出现，例如，表达式 `notify('customercare@example.com')` 和 `notify("customercare@example.com")` 均有效，而表达式 `notify("customercare@example.com')` 会导致语法错误。

以“#”字符开头的行被视为注释并被忽略，但不会被 AsyncOS 保留，因为可通过 `filters -> detail` 查看过滤器进行验证。

邮件过滤器处理

处理邮件过滤器时，AsyncOS 扫描的内容、处理的顺序以及执行的操作取决于以下因素：

- **邮件过滤器顺序**。邮件过滤器在列表中按顺序排列。处理邮件时，AsyncOS 会按照过滤器在列表中的顺序应用每个邮件过滤器。如果执行了最终操作，则不再对邮件执行进一步处理。有关详细信息，请参阅邮件过滤器顺序, on page 5。
- **处理之前**。对 AsyncOS 邮件执行的操作可能会在评估邮件过滤器之前添加或删除信头。处理过程中，AsyncOS 会处理作用于邮件信头的邮件过滤器进程。有关详细信息，请参阅邮件信头规则和求值, on page 5。
- **邮件的 MIME 结构**。邮件的 MIME 结构决定了邮件的哪个部分可视为“正文”，哪些部分视为“附件”。许多邮件过滤器配置为仅对邮件的正文或邮件的附件部分执行操作。有关详细信息，请参阅邮件正文与邮件附件, on page 5。
- **为正则表达式配置的阈值得分**。匹配正则表达式时，应配置“得分”来汇总过滤器执行操作之前匹配必须发生的次数。这允许您对不同条件的响应进行“加权”。有关详细信息，请参阅内容扫描中的匹配阈值, on page 6。
- **查询的结构**。对邮件过滤器中的 AND 或 OR 测试求值时，AsyncOS 不会对不必要的测试求值。此外，请注意，系统不会按照从左到右的顺序对测试求值。相反，在对 AND 和 OR 测试求值时，系统会优先对成本最低的测试求值。有关详细信息，请参阅邮件过滤器中的 AND 和 OR 测试, on page 8。

相关主题

- 邮件过滤器顺序, on page 5
- 邮件信头规则和求值, on page 5
- 邮件正文与邮件附件, on page 5
- 内容扫描中的匹配阈值, on page 6
- 邮件过滤器中的 AND 和 OR 测试, on page 8

邮件过滤器顺序

邮件过滤器在列表中按顺序排列，并按在列表中的位置编号。处理邮件时，系统按关联数字顺序应用邮件过滤器。因此，如果过滤器 9 已经在邮件上执行了最终操作（如退回），过滤器 30 不会有机会修改邮件的源主机。过滤器在列表中的位置可以通过系统用户界面更改。通过文件导入的过滤器根据其在导入文件中的相对顺序排列。

执行最终操作后，不再对邮件执行进一步操作。

尽管邮件可能符合某一过滤器规则，过滤器可能会出于任何以下原因不对邮件执行操作：

- 过滤器处于非活动状态。
- 过滤器无效。
- 过滤器被对邮件执行最终操作的上一个过滤器取代。

邮件信头规则和求值

应用信头规则时，过滤器将对“已处理”信头求值，而非原始邮件信头。因此：

- 如果信头由之前的处理操作添加，现在可通过任何后续信头规则进行匹配。
- 如果信头被之前的处理操作删除，不再通过任何后续信头规则进行匹配。
- 如果信头被之前的处理操作修改，则任何后续信头规则将对修改后的信头求值，而不是原始信头。

此行为在邮件过滤器和内容过滤器上的表现相同。

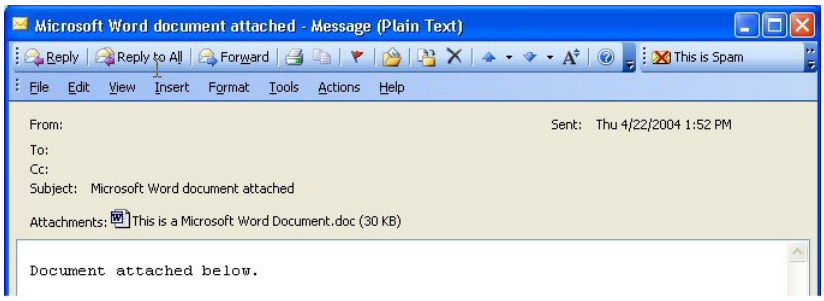
邮件正文与邮件附件

邮件消息由多个要素构成。尽管 RFC 将邮件信头后面的任何内容均视为多部分的“邮件正文”，很多用户对邮件的“正文”和“附件”仍有不同的定义。使用名为 *body*-variable 或 `attachment`-*variable* 的任意思科邮件过滤器时，邮件网关将按照很多 MUA 呈现这类内容的方式，尝试区分大部分用户眼中的“正文”和“附件”。

在编写 *body*-variable 或 `attachment`-*variable* 邮件过滤器规则时，邮件信头后面的任何内容均视为邮件正文，这部分的内容被视为正文中 MIME 部分的首要文本内容。这类内容后面的任何要素（即任何额外的 MIME 部分）被视为附件。AsyncOS 会对邮件的不同 MIME 部分评估，确定文件中被视为附件的部分。

例如，下图展示了一封 Microsoft Outlook MUA 中的邮件，词句“`Document attached below.`”显示为纯文本邮件正文，而文档“`This is a Microsoft Word document.doc`”显示为附件。由于很多用户对邮件有这样的认识（而不是第一部分是纯文本、第二部分是一个二进制文件的多部分邮件），思科在邮件过滤器中使用术语“附件”创建规则，区分邮件的 .doc 文件部分（即第二个 MIME 部分）和“正文”部分（第一个纯文本部分），尽管根据 RFCS 1521 和 1522 中的规定，邮件正文包括所有 MIME 部分。

Figure 1: 含“附件”的邮件



由于邮件网关对多部分邮件的正文和附件部分做了这样的区分，要使用 body-*variable* 或 `attachment-`*variable* 邮件过滤器规则实现预期行为，必须注意以下事项：

- 如果邮件包含一个文本部分，即邮件的信头格式是“Content-Type: text/plain”或“Content-Type: text/html”，邮件网关会将整封邮件视为正文。如果内容类型是其他类型，邮件网关会将其视为单独的附件。
- 邮件正文中包含某些编码文件（例如，使用 uuencode 编码的文件）。在这种情况下，编码文件会被视为附件，并被提取和扫描，而剩余文本则被视为文本正文。
- 单个非文本部分始终被视为附件。例如，只含 .zip 文件的邮件被视为附件。

内容扫描中的匹配阈值

添加搜索邮件正文或附件中模式的过滤器规则时，可以指定找到模式的最小次数阈值当 AsyncOS 扫描邮件时，它会将在邮件和附件中找到的匹配数“得分”加总。如果未达到最小阈值，则正则表达式不会求值为 True。您可以为以下过滤器规则指定此阈值：

- 正文包含 (body-contains)
- 仅正文包含 （only-body-contains）
- 附件包含 (attachment-contains)
- 每个附件均包含 (every-attachment-contains)
- 每个附件均包含 (every-attachment-contains)
- 附件字典匹配 (attachment-dictionary-match)

您还可以为 `drop-attachments-where-contains` 操作指定阈值。

Note 不能为扫描信头或信封收件人和发件人的过滤器规则指定阈值。

相关主题

- 阈值语法, on page 7
- 邮件正文和附件的阈值评分, on page 7
- 多部分/备用 MIME 部分的阈值评分, on page 7
- 内容词典的阈值评分, on page 8

阈值语法

要为最小匹配次数指定阈值，请指定得出 true 值的模式和最小匹配数：

```
if(<filter rule>('<pattern>',<minimum threshold>)){
```

例如，要指定 body-contains 过滤器规则必须至少找到值“公司机密”两次，请使用以下语法：

```
if(body-contains('Company Confidential',2)){
```

默认情况下，在保存内容扫描过滤器时，AsyncOS 会编译过滤器，并默认为其分配阈值 1（如果您未分配值）。

您可以为内容词典中的值指定最小模式匹配数量。有关内容词典的详细信息，请参阅“文本资源”一章。

邮件正文和附件的阈值评分

邮件可能包含多个部分。为搜索邮件正文或附件中模式的过滤器规则时指定阈值时，AsyncOS 通过计算邮件部分和附件的匹配数量确定阈值“得分”。AsyncOS 将汇总邮件所有部分的匹配，确定匹配是否达到阈值，除非邮件过滤器指定特定 MIME 部分（例如 `attachment-contains` 过滤器规则）。例如，您设置了阈值为 2 的 `body-contains` 邮件过滤器。您收到一封正文包含一个匹配、附件包含一个匹配的邮件。对此邮件评分时，AsyncOS 会对两个匹配求和，做出邮件达到阈值得分的判断。

同样，如果您有多个附件，AsyncOS 会汇总每个附件的得分来计算匹配的得分。例如，您设置了阈值为 3 的 `attachment-contains` 过滤器规则。您收到一封包含两个附件的邮件，并且每个附件包含两个匹配，那么 AsyncOS 对此邮件的评分为四，并做出已达到阈值得分的判断。

多部分/备用 MIME 部分的阈值评分

为避免重复计数，如果同样的内容有两种不同的表示（纯文本和 HTML），AsyncOS 不会汇总重复部分中的匹配。相反，它会比较每个部分的匹配，并选择最大值。之后，AsyncOS 会将此值与多部分邮件其他部分的得分相加得出总得分。

例如，您配置了 `body-contains` 过滤器规则，并将阈值设为 4。您收到包含纯文本、HTML 和两个附件的邮件。邮件的结构如下：

```
multipart/mixed

        multipart/alternative

                text/plain

                text/html

        application/octet-stream

        application/octet-stream
```

`body-contains` 过滤器规则将通过首先对邮件的 text/plain 和 text/html 部分评分来确定此邮件的得分。然后比较这些得分的结果，并从结果中选择最高分。接下来，将此结果与每个附件的得分相加得出最终得分。假设该邮件有以下数量的匹配：

```
multipart/mixed

        multipart/alternative

                text/plain (2 matches)

                text/html (2 matches)

        application/octet-stream (1 match)

        application/octet-stream
```

因为，AsyncOS 比较 text/plain 和 text/html 部分的匹配，返回得分 3，而该得分未达到触发过滤器规则的最小阈值。

内容词典的阈值评分

使用内容词典时，您可以对术语进行“加权”，这样可以使某些术语更轻易地触发过滤器操作。例如，您可能希望不要对术语“银行”触发邮件过滤器。但是，如果术语“银行”与术语“账号”结合，并附有美国银联转帐号，您可能希望触发过滤器操作。为此，您可以使用加权词典，增加某些术语组合的重要性。当邮件过滤器使用内容词典计算过滤器规则的匹配得分时，过滤器将使用这些权重确定最终得分。例如，假设您创建了包含以下内容和权重的内容词典：

Table 1: 内容词典示例

术语/智能标识符	加权
美国银联转帐号	3
账户	2
银行	1

将此内容词典与 `dictionary-match` 或 `attachment-dictionary-match` 邮件过滤器规则结合使用时，AsyncOS 会将术语的权重与邮件中每个匹配术语匹配次数的总“得分”相加。例如，如果术语“帐号”在邮件正文中出现三次，AsyncOS 会在总得分中加 6。如果邮件过滤器的阈值设为 6，AsyncOS 将做出已达到阈值得分的判断。或者，如果每个术语在邮件中出现一次，总值将为 6，此得分会触发过滤器操作。

邮件过滤器中的 **AND** 和 **OR** 测试

对邮件过滤器中的 AND 或 OR 测试求值时，AsyncOS 不会对不必要的测试求值。因此，例如 AND 测试的一端为 False，系统不会对另一端求值。请注意，系统不会按照从左到右的顺序对测试求值。相反，在对 AND 和 OR 测试求值时，系统会优先对成本最低的测试求值。例如，在以下过滤器中，

系统会始终优先处理 remote-ip 测试，因为该测试的成本比 rcpt-to-group 测试成本低（LDAP 测试成本通常较高）：

```
andTestFilter:

if (remote-ip == "192.168.100.100" AND rcpt-to-group == "GROUP")

  { ... }
```

由于先执行成本最低的测试，改变测试项的顺序不会产生影响。如果您要确保测试的执行顺序，请使用嵌套的 if 语句。这也是尽可能避免高成本测试的最佳方法：

```
expensiveAvoid:

if (<simple tests>)

  { if (<expensive test>)

    { <action> }

  }
```

在稍微复杂的情况下，可考虑：

```
if (test1 AND test2 AND test3) { ... }
```

系统从左到右对表达式分组，使其变成：

```
if ((test1 AND test2) AND test3) { ... }
```

这意味着系统要做的第一件事是对比 (test1 AND test2) 和 test3 的成本，首先对第二个 AND 求值。如果这三个测试的成本相同，则首先执行 test3，因为 (test1 AND test2) 的成本是其两倍。

邮件过滤器规则

每个过滤器都有定义过滤器适用邮件对象的规则。首先定义过滤器规则，然后定义规则返回 true 值时对邮件执行的过滤操作。

相关主题

- 过滤器规则摘要表, on page 9
- 规则中的正则表达式, on page 19
- 智能标识符, on page 22
- 邮件过滤器操作说明和示例, on page 67

过滤器规则摘要表

下表 汇总了可以在邮件过滤器中使用的规则。

Table 2: 邮件过滤器规则

规则	语法	说明
主题信头	`subject`	主题信头是否匹配某一文本模式？请参阅Subject 规则, on page 26。
正文大小	`body-size`	正文大小是否在某一范围内？请参阅正文大小规则, on page 29。
信封发件人	`mail-from`	信封发件人（即，<MAIL FROM>）是否与指定模式匹配？请参阅信封发件人规则, on page 28。
组中的信封发件人	`mail-from-group`	信封发件人（即，<MAIL FROM>）是否在指定的 LDAP 组中？请参阅组中的信封发件人规则, on page 28。
发件人组	`sendergroup`	与侦听程序主机访问表 (HAT) 中的哪个发件人组匹配？请参阅发件人组规则, on page 28。
信封收件人	`rcpt-to`	信封收件人（即 Envelope To <RCPT TO>）是否与指定模式匹配？请参阅信封收件人规则, on page 27。 **Note** `rcpt-to` 规则基于邮件。如果一个邮件有多个收件人，那么一个收件人与指定操作规则匹配，即可将指定操作应用至发送给所有收件人的邮件。

规则	语法	说明
组中的信封发件人	`rcpt-to-group`	信封收件人（即 Envelope To <RCPT TO>）是否在指定的 LDAP 组中？请参阅组中的信封收件人规则, on page 27。 **Note** `rcpt-to-group` 规则基于邮件。如果邮件具有多个收件人，只须在组中找到一个收件人便可使指定的操作影响发送给所有收件人的邮件。
远程 IP	`remote-ip`	邮件是否来自与指定 IP 地址或 IP 地址范围匹配的远程主机？请参阅远程 IP 规则, on page 30。
接收接口	`recv-int`	邮件是否通过指定的接收接口接收？请参阅。接收 IP 接口规则, on page 30
接收侦听程序	`recv-listener`	邮件是否通过指定的侦听程序接收？请参阅接收侦听程序规则, on page 30。
日期	`date`	当前时间在特定日期时间之前还是之后？请参阅日期规则, on page 30。
信头	`header(<string>)`	邮件是否包含指定的信头？信头的值是否与某一文本模式匹配？请参阅信头规则, on page 31。
MS	`random(<integer>)`	随机数是否在某一范围内？请参阅随机规则, on page 31。
收件人计数	`rcpt-count`	邮件将发给多少收件人？请参阅收件人计数规则, on page 32。
地址计数	`addr-count()`	收件人的累积数量是多少？ 此过滤器与 rcpt-count 过滤器规则的不同之处在于，它的作用对象是邮件正文信头，不是信封收件人。请参阅地址计数规则, on page 32。

规则	语法	说明
SPF 状态	`spf-status`	什么是SPF验证状态？此过滤器规则允许查询不同的SPF验证结果。可以为每个 SPF/SIDF 有效返回值指定不同的操作。请参阅SPF-Status 规则, on page 38。
SPF 通过	`spf-passed`	是否通过 SPF/SIDF 验证？此过滤器规则将 SPF/SIDF 结果表示为布尔值。请参阅SPF-Passed 规则, on page 40。
S/MIME 网关邮件	`smime-gateway`	邮件是否已经过S/MIME签名、加密或签名并加密？请参阅S/MIME 网关邮件规则, on page 40
S/MIME 网关已验证	`smime-gateway-verified`	S/MIME 邮件是否已成功通过验证，解密或已成功解密并验证？请参阅S/MIME 网关验证规则, on page 40。
图像判定	`image-verdict`	什么是图像扫描判定？此过滤器规则可查询不同的图像分析判定结果。请参阅图像分析, on page 89。
工作队列计数	`workqueue-count`	工作队列计数等于、小于还是大于指定值？请参阅工作队列计数规则, on page 40。
正文扫描	`body-contains(<regular expression>)`	邮件是否包含与指定模式匹配的文本或附件？模式是否出现了为阈值指定的最少次数？ 引擎扫描传送状态部分和关联附件。 请参阅正文扫描 , on page 33。
正文扫描	`only-body-contains (<regular expression>)`	邮件正文是否包含与指定模式匹配的文本？模式是否出现了为阈值指定的最少次数？附件不进行扫描。请参阅正文扫描规则, on page 33。
加密检测	`encrypted`	邮件是否加密？请参阅加密检测规则, on page 34。

规则	语法	说明
附件文件名	`attachment-filename`	邮件是否包含文件名与指定模式匹配的附件？请参阅附件文件名规则, on page 35。
附件类型	`attachment-type`	邮件是否包含特定 MIME 类型的附件？请参阅附件类型规则, on page 34。
附件文件类型	`attachment-filetype`	邮件是否包含文件类型根据指纹与特定模式匹配的附件（类似于 UNIX `file` 命令）？如果附件是 Excel 或 Word 文档，您还可以搜索以下类型的嵌入文件：exe、dll、bmp、tiff、pcx、gif、jpeg、png 以及 Photoshop 图像。 必须用引号将文件类型引起，创建的过滤器才有效。使用单引号或双引号均可。例如，要搜索 .exe 附件，请使用以下语法： `if (attachment-filetype == "exe")` 有关详细信息，请参阅附件文件名和存档文件中的单个压缩文件, on page 35。
附件MIME类型	`attachment-mimetype`	邮件是否包含特定 MIME 类型的附件？该规则与 `attachment-type` 规则类似，不同之处在于该规则会评估 MIME 附件指定的 MIME 类型。（如果没有明确指明文件类型，则邮件网关不会尝试根据其扩展名来“猜测”文件的类型。）请参阅附件扫描邮件过滤器示例, on page 93。
附件文件散列列表	`attachment-hashlist-match`	邮件是否包含与文件散列列表中的特定文件 SHA-256 值匹配的附件？请参阅丢弃与文件 SHA-256 过滤器匹配的邮件附件, on page 119和如果附件与文件 SHA-256 过滤器匹配，则丢弃邮件, on page 119。

规则	语法	说明
受保护的附件	`attachment-protected`	邮件是否包含受密码保护的附件？请参阅隔离受保护的附件, on page 96。
未受保护的附件	`attachment-unprotected`	如果扫描引擎检测到未受保护的附件，附件未受保护过滤条件将返回 true。如果扫描引擎可以读取附件，文件则被视为未受保护。如果其中一个所含文件未受保护，压缩文件则视为未受保护。 **注意** - 附件未受保护过滤条件与附件受保护过滤条件不相互排斥。扫描同一附件时，可能会出现两个过滤条件均返回 true 的情况。例如，当压缩文件同时包含受保护和未受保护的文件时，可能会出现这种情况。 请参阅检测未受保护的附件, on page 96。
附件扫描	`attachment-contains (<regular expression>)`	邮件是否包含文本或另一个附件与指定模式匹配的附件？模式是否出现了为阈值指定的最少次数？ 此规则类似于 `body-contains()` 规则，只是它会尝试避免扫描邮件的整个“正文”。也即，只扫描用户视为附件的部分。请参阅附件扫描邮件过滤器示例, on page 93。
附件扫描	`attachment-binary-contains (<regular expression>)`	邮件是否包含二进制数据与指定模式匹配的附件？ 此规则与 `attachment-contains()` 规则相似，但只在二进制数据中搜索模式。

规则	语法	说明
附件扫描	`every-attachment-contains (<regular expression>)`	此邮件的所有附件是否包含与指定模式匹配的文本？文本必须存在于所有附件，执行的操作实际上是对每个附件的“`attachment-contains()`”操作执行逻辑 AND 运算。正文不进行扫描。模式是否出现了为阈值指定的最少次数？ 请参阅附件扫描邮件过滤器示例, on page 93。
附件大小	`attachment-size`	邮件是否包含大小在某一范围内的附件？该规则与 `body - size` 规则类似，但会尝试避免扫描邮件的整个“正文”。也即，只扫描用户视为附件的部分。在执行任何解码之前先评估大小。请参阅附件扫描邮件过滤器示例, on page 93。
公共阻止列表	`dnslist(<query server>)`	发件人的 IP 地址是否出现在公共阻止列表服务器上 (RBL)？请参阅DNS 列表规则, on page 35。
IP 信誉	`reputation`	什么是发件人的 IP 信誉得分？请参阅IP 信誉规则, on page 36。
无 IP 信誉	`no-reputation`	用于测试 IP 信誉得分是否为“无”(None)。请参阅IP 信誉规则, on page 36。
字典	`dictionary-match (<dictionary_name>)`	邮件正文是否包含 *dictionary_name* 内容词典中的任何正则表达式或术语？模式是否出现了为阈值指定的最少次数？请参阅词典规则, on page 37。
附件词典匹配	`attachment-dictionary-match (<dictionary_name>)`	附件是否包含 *dictionary_name* 内容词典中的任何正则表达式？模式是否出现了为阈值指定的最少次数？请参阅词典规则, on page 37。

规则	语法	说明
主题词典匹配	`subject-dictionary-match (<dictionary_name>)`	主题信头是否包含 *dictionary name* 内容词典中的任何正则表达式或术语？请参阅词典规则, on page 37。
信头词典匹配	`header-dictionary-match (<dictionary_name>, <header>)`	指定的信头（不区分大小写）中是否包含 *dictionary name* 内容词典中的任何正则达式或术语？请参阅词典规则, on page 37。
正文词典匹配	`body-dictionary-match (<dictionary_name>)`	如果词典术语与邮件正文中的内容匹配，此过滤条件会返回 true。过滤器会在不被视为附件的 MIME 部分搜索术语，并在达到用户定义的阈值（默认阈值值为 1）时返回 true。请参阅词典规则, on page 37。
信封收件人词典匹配	`rcpt-to-dictionary-match (<dictionary_name>)`	信封收件人是否包含 *dictionary name* 内容词典中的任何正则表达式或术语？请参阅词典规则, on page 37。
信封发件人词典匹配	`mail-from-dictionary-match (<dictionary_name>)`	信封发件人是否包含 *dictionary name* 内容词典中的任何正则表达式或术语？请参阅词典规则, on page 37。
SMTP 身份验证的用户匹配	`smtp-auth-id-matches (<target>[, <sieve-char>])`	信封发件人的地址和邮件信头中的地址是否与发件人的已验证 SMTP 用户 ID 匹配？请参阅SMTP 身份验证用户匹配规则, on page 41。
正确	`true`	匹配所有邮件。请参阅True 规则, on page 26。
有效	`valid`	如果邮件包含不可分析/无效的 MIME 部分，则返回 False，反之返回 True。请参阅Valid 规则, on page 26。
已签名	`signed`	邮件是否已签名？请参阅已签名规则, on page 43。

规则	语法	说明
签名证书	`signed-certificate (<field> [<operator> <regular expression>])`	邮件签署人或X.509证书颁发者是否与某一模式匹配？请参阅签名证书规则, on page 43。
信头重复	`header-repeats (<target>, <threshold> [, <direction>])`	如果在给定的时间内出现特定数量满足下列条件的邮件，返回 `true`： • 在上一小时检测到主题信头相同的邮件。 • 在上一小时检测到来自同一信封发件人的邮件。 请参阅信头重复规则, on page 45。
URL 信誉	`url-reputation url-no-reputation`	邮件中任何 URL 的信誉得分是否在指定范围内？ URL 的信誉得分是否不存在？ 请参阅URL 信誉规则 , on page 47和将邮件网关配置为使用外部威胁源。
URL 类别	`url-category`	邮件中任何 URL 的类别是否与指定类别匹配？ 请参阅 URL 类别规则 , on page 48。
损坏的附件	`attachment-corrupt`	此邮件是否具有已损坏的附件？ 请参阅损坏的附件规则, on page 48。
邮件语言	`message-language`	邮件（主题和正文）是否为其中一种所选语言？ 请参阅邮件语言规则, on page 48。
宏检测	`macro-detection-rule ([ ‘file_type-1', 'file_type-2', …,'file_type-n'])`	传入或传出邮件是否包含启用宏的附件？ 请参阅 宏检测规则, on page 49

规则	语法	说明
伪造邮件检测	`forged-email-detection ("<dictionary_name>", <threshold>)`	是否为伪造邮件的发件人邮箱？此规则检查邮件的“发件人:”信头是否与内容字典中的任何用户相似。 请参阅伪造邮件检测规则, on page 50。
重复边界验证	`duplicate_boundaries`	邮件是否包含重复的 MIME 边界？ 请参阅重复边界验证规则, on page 51。
格式错误的 MIME 信头检测	`malformed-header`	邮件是否包含格式错误的MIME信头？ 请参阅格式不正确的MIME信头检测规则, on page 51。
地理位置	`geolocation-rule (['country_name-1', 'country_name-2', 'country_name-n'])`	传入邮件是否来自选定的国家/地区？ **Note** 在使用地理定位邮件过滤器规则之前，请启用设备上的反垃圾邮件引擎。 请参阅地理位置规则, on page 52。

域信誉	`Sender Domain Reputation:`
	` - sdr-reputation`
	`  (< ‘sdr_verdict_range'>,`
	`  < ‘domain_exception`
	`  _list'>)`
	` - sdr-age (< ‘unit'>,`
	`  < ‘operator'>`
	`  < ‘actual value’ >)`
	` - sdr-unscannable`
	`  (<'domain_exception`
	`  _list'>)`
	
	`External Threat Feeds:`
	` domain-external-`
	` threat-feeds`
	` (<'external_threat_`
	` feed_source_name'>,`
	` <'header'> , <'domain`
	`_exception_list'>)`
		发件人域是否与指定的条件匹配？
		• 发件人域信誉
		• 外部威胁源
		请参阅ETF 的域信誉规则, on page 52或SDR 的域信誉规则, on page 53。
		有关详细信息，请参阅将邮件网关配置为使用外部威胁源或发件人域信誉过滤。

系统会按顺序对进入邮件网关的每封邮件应用所有邮件过滤器，除非指定终止对邮件进一步处理的最终操作。（请参阅邮件过滤器操作, on page 2。）此外，还可以对所有邮件应用过滤器，并使用逻辑连接符（AND、OR 以及 NOT）组合规则。

规则中的正则表达式

定义规则的多个基本测试使用正则表达式匹配。正则表达式可以很复杂。在邮件过滤器规则中使用正则表达式时，可参考下表：

Table 3: 规则中的正则表达式

正则表达式 (`abc`)	如果正则表达式中的命令序列与字符串的任何部分匹配，则视为过滤器规则中的正则表达式与字符串匹配。 例如，正则表达式 Georg 与字符串 `George Of The Jungle`、字符串 `Georgy Porgy`、字符串 La Meson Georgette 以及 `Georg` 均匹配。
插入符 (^) 美元符号 (`$`)	包含美元符号字符 ($) 的规则只与字符串结尾匹配，包含插入符字符 (^) 的规则只与字符串的开头部分匹配。 例如，正则表达式 `^Georg$` 只与字符串 `Georg` 匹配。 搜索空信头会返回 "^$"
字母、空格和 `@` 符号	包含字符、空格、以及 at 符号 (@) 的规则只与自身匹配。 例如，正则表达式 `^George@admin$` 只与字符串 `George@admin` 匹配。
句点字符 (.)	包含句点字符 (.) 的规则匹配任何字符（新行除外）。 例如，正则表达式 `^...admin$` 与字符串 `macadmin` 以及字符串 `sunadmin` 匹配，但与 `win32admin` 不匹配。
星号 (*) 指令	包含星号 (*) 的规则与“上一命令的零个或多个匹配”匹配。尤其是，句点和星号序列 (.*) 将与任何字符序列（不包含换行符）匹配。 例如，正则表达式 `^P.*Piper$` 匹配下列所有字符串：`PPiper`、Peter Piper、P.Piper 和 `Penelope Penny Piper`。
反斜线特殊字符 (\)	反斜线字符对特殊字符进行转义。因此，序列 `\.` 仅与句点的字母表达匹配，序列 `\$` 仅与美元符号的字母表达匹配，序列 `\^` 仅与克拉符号的字母表达匹配。例如，正则表达式 `^ik\.ac\.uk$` 仅与字符串 `ik.ac.uk` 匹配。 **重要说明：**反斜线也是解析器的特殊转义字符。因此，如果要在正则表达式中使用反斜线，必须使用两个反斜线，以便在解析后仅保留一个“真正的”反斜线，然后将其传递给正则表达式系统。因此，如果您希望与上述示例域匹配，需要输入 `^ik\\.ac\\.uk$`。

不区分大小写 `(?i)`	符号 (?i) 表示正则表达式剩余部分应做不区分大小写处理。将此令牌放在区分大小写的正则表达式的开头会导致匹配项完全不区分大小写。 例如，正则表达式“`(?i)viagra`”与 `Viagra`、vIaGrA 以及 VIAGRA 匹配。
重复次数 `{min,max}`	此正则表达式记法指示前一个标记可以重复的次数。 例如，表达式“`fo{2,3}`”与 `foo` 和 `fooo` 匹配，但不匹配 fo 或 fofo。 语句 `if(header('To') == "^.{500,}")` 查找包含 500 或更多字符的“To”信头。
或 (|)	替换或“或”运算符。如果 A 和 B 是正则表达式，表达式“`A|B`”将匹配与“A”或“B”匹配的所有字符串。 例如，表达式“`foo|bar`”将与 `foo` 或 `bar` 匹配，但与 `foobar` 不匹配。

相关主题

- 使用正则表达式过滤邮件, on page 20
- 正则表达式使用准则, on page 21
- 正则表达式和非 ASCII 字符集, on page 21
- n 次测试, on page 21
- 区分大小写, on page 21
- 编写高效的过滤器, on page 21
- PDF 和正则表达式, on page 22

使用正则表达式过滤邮件

可以使用过滤器在非 ASCII 编码的邮件内容（信头和正文）中搜索字符串和模式。具体而言，系统支持在以下对象的非 ASCII 字符集中执行正则表达式 (regex) 搜索：

- 邮件信头
- MIME 附件文件名字符串
- 邮件正文：
  - 不含 MIME 信头的正文（即传统邮件）
  - 包含表明编码的 MIME 信头，但不含 MIME 部分的正文
  - 表明编码的多部分 MIME 邮件
  - 所有以上未在 MIME 信头中表明编码的对象

可以使用正则表达式 （regexes） 匹配邮件的任何部分或正文，包括匹配的附件。附件类型包括文本、HTML、MS Word、Excel 等。可接受的字符集包括 gb2312、HZ、EUC、JIS、Shift-JIS、Big5 以及 Unicode。可通过内容过滤器 GUI 创建包含正则表达式的邮件过滤器规则，或使用文本编辑器生成文件并随后导入系统。有关详细信息，请参阅使用 CLI 管理邮件过滤器, on page 97和配置扫描行为, on page 119。

正则表达式使用准则

如果要完全匹配一个字符串，而不是一个前缀，正则表达式必须以插入符 (^) 开头，以美元符号 ($) 结尾。

Note 与空字符串匹配时，不要使用 “”，因为这实际上会匹配所有字符串。请使用 “^$”。有关示例，请参阅Subject 规则, on page 26中的第二个示例

另外，如果您要与句点的字母表达匹配，必须在正则表达式中使用转义句点。例如，正则表达式 sun.com 与字符串 thegodsunocommando 匹配，但正则表达式 ^sun\.com$ 只与字符串 sun.com. 匹配。

从技术上来说，使用的正则表达式样式是 **Python re Module** 样式正则表达式。有关 Python 样式的正则表达式的更详细讨论，请查阅 Python 正则表达式使用方法，其网址为：
http://www.python.org/doc/howto/

正则表达式和非 ASCII 字符集

在某些语言中，不存在词语或字边界或大小写概念。

在区域设置或编码未知的情况下，取决于何为/何不为构成单词的字符（在正则表达式中以“\w”表示）等概念的复杂正则表达式会带来一些问题。

n 次测试

可使用序列 == 对正则表达式进行匹配测试，使用序列 != 进行不匹配测试。例如：

```
rcpt-to ==
 "^goober@dev\\.null\\....$" (matching)


rcpt-to != "^goober@dev\\.null\\....$" (non-matching)
```

区分大小写

正则表达式区分大小写，另有说明除外。因此，如果正则表达式搜索 foo，将不匹配模式 FOO，甚至 Foo。

编写高效的过滤器

本示例展示执行相同操作的两个过滤器，但是第一个过滤器占用的CPU较多。第二个过滤器使用的正则表达式更为有效。

```
attachment-filter: if ((recv-listener == "Inbound") AND
((((((((((((((((((((((((((((((((((((((((((((((((((attachment-filename ==

"\\.386$") OR (attachment-filename == "\\.exe$")) OR (attachment-filename == "\\.ad$")) OR

(attachment-filename == "\\.ade$")) OR (attachment-filename == "\\.adp$")) OR
```

```
(attachment-filename == "\\.asp$")) OR (attachment-filename == "\\.bas$")) OR
(attachment-filename == "\\.bat$")) OR (attachment-filename == "\\.chm$")) OR
(attachment-filename == "\\.cmd$")) OR (attachment-filename == "\\.com$")) OR
(attachment-filename == "\\.cpl$")) OR (attachment-filename == "\\.crt$")) OR
(attachment-filename == "\\.exe$")) OR (attachment-filename == "\\.hlp$")) OR
(attachment-filename == "\\.hta$")) OR (attachment-filename == "\\.inf$")) OR
(attachment-filename == "\\.ins$")) OR (attachment- filename == "\\.isp$")) OR
(attachment-filename == "\\.js$")) OR (attachment-filename == "\\.jse$")) OR
(attachment- filename == "\\.lnk$")) OR (attachment-filename == "\\.mdb$")) OR
(attachment-filename == "\\.mde$")) OR (attachment-filename == "\\.msc$")) OR
(attachment-filename == "\\.msi$")) OR (attachment-filename == "\\.msp$")) OR
(attachment-filename == "\\.mst$")) OR (attachment-filename == "\\.pcd$")) OR
(attachment-filename == "\\.pif$")) OR (attachment-filename == "\\.reg$")) OR
(attachment-filename == "\\.scr$")) OR (attachment-filename == "\\.sct$")) OR
(attachment-filename == "\\.shb$")) OR (attachment-filename == "\\.shs$")) OR
(attachment-filename == "\\.url$")) OR (attachment-filename == "\\.vb$")) OR
(attachment-filename == "\\.vbe$")) OR (attachment-filename == "\\.vbs$")) OR
(attachment-filename == "\\.vss$")) OR (attachment-filename == "\\.vst$")) OR
(attachment-filename == "\\.vsw$")) OR (attachment-filename == "\\.ws$")) OR
(attachment-filename == "\\.wsc$")) OR (attachment-filename == "\\.wsf$")) OR
(attachment-filename == "\\.wsh$"))) { bounce(); }
```

在这种情况下，AsyncOS 需要启动正则表达式引擎 30 次，对每个附件类型以及 recv-listener 各启动一次。

但是，如果按如下所示编写过滤器：

```
attachment-filter: if (recv-listener == "Inbound") AND (attachment-filename == "\\.
(386|exe|ad|ade|adp|asp|bas|bat|chm|cmd|com|cpl|crt|exe|hlp|hta|inf|ins|isp|js|jse|l
nk|mdb|mde|msc|msi|msp|mst|pcd|pif|reg|scr|sct|shb|shs|
url|vb|vbe|vbs|vss|vst|vsw|ws|wsc|wsf|wsh)$") {
```

正则引擎仅需要启动两次，而且事实证明过滤器更易于维护，因为您无需担心是否添加了“()”, 拼写错误。与上述相比，这应该能够降低 CPU 占用率。

PDF 和正则表达式

根据 PDF 的生成方式，PDF 可能不包含空格或换行符。在这种情况下，扫描引擎会根据词语在页面上的位置尝试插入逻辑空格和换行符。例如，使用多个字体或字体大小输入词语时，PDF 代码显示的方式会导致扫描引擎难以确定词语和换行符。尝试将正则表达式与以这种方式构建的 PDF 文件匹配时，扫描引擎会返回意外的结果。

例如，在 PowerPoint 文档中输入每个字母都使用不同字体和字号的单词。读取此应用生成的 PDF 文件时，扫描引擎会插入逻辑空格和换行符。鉴于 PDF 的结构，引擎可能会将单词“callout”解读为“call out”或“c a l lout”。尝试根据正则表达式匹配其中一个表示时，可能找不到“callout”的匹配。

智能标识符

使用扫描邮件内容的邮件规则时，可以使用智能标识符检测数据中的特定模式。

智能标识符可检测数据中的以下模式：

- 信用卡号
- 美国社会保险号

- 统一安全委员会程序 (CUSIP) 编号
- 美国银行业协会 (ABA) 转帐号码

要在过滤器中使用智能标识符，请在过滤器规则中输入以下扫描正文或附件内容的关键字：

Table 4: 邮件过滤器中的智能标识符

关键字	智能标识符	说明
*credit	信用卡号	识别 14、15、以及 16 位信用卡号。 注意：智能标识符不识别 enRoute 卡。
*aba	美国银联转帐号	识别美国银联转帐号。
*ssn	社会保险号	识别美国社会安全保障号。*ssn 智能标识符可识别包含短划线、句点和空格的社会保险号码。
*cusip	CUSIP 号码	识别 CUSIP 号码。

相关主题

- 智能标识符语法, on page 23

智能标识符语法

在过滤器规则中使用智能标识符时，请在过滤器规则中输入扫描正文或附件文件的智能标识符关键字，并将关键字放入引号中，如下文示例所示：

```
ID_Credit_Cards:

if(body-contains("*credit")){

notify("legaldept@example.com");

}
.
```

您还可以在内容过滤器和内容词典中使用智能标识符。

Note 不能将智能标识符关键字与常规正则表达式或另一个关键字结合使用。例如，模式 `*credit|*ssn` 可能无效。

Note 为尽可能减少 *SSN 智能标识符产生的误报，有必要将 *ssn 智能标识符与其他过滤条件搭配使用。其中一个可搭配使用的过滤器是“only-body-contains”过滤条件。这样，只有当搜索字符串在邮件正文的任何 MIME 部分都存在时，表达式的值才为 true。例如，您可以创建以下过滤器：

```
SSN-nohtml: if only-body-contains(“*ssn”) { duplicate-quarantine(“Policy”);}
```

Note 邮件网关会检测在邮件内容中添加或不添加作为前缀的关键字（“ credit”、“ ssn”、“ cusip”或“ aba”）的智能标识符。

例如：如果邮件包含以下任何格式的社会保险号，则邮件网关会将社会保险号检测为智能标识符：

（“ XXX-XX-XXXX”，“ ssn XXX-XX-XXXX”，“ ssn：XXX-XX-XXXX”等）。

示例：不带前缀的智能标识符

创建以下过滤器以检测在智能标识符之前不存在关键字的智能标识符。

```
ID_Credit_Cards:
if(body-contains("*credit", 1))
{
notify("legaldept@example.com");
}
```

位置

“ `credit`”表示信用卡号智能标识符，

“`1`” 表示要使该规则求值为 true 所需的匹配数量。

示例：带前缀的智能标识符

创建以下过滤器以仅在智能标识符之前存在关键字（（'credit，"ssn，"cusip，'或'aba'）时检测智能标识符。

```
ID_Credit_Cards:
if(body-contains("*credit", 1, “prefix”))
{
notify("legaldept@example.com");
}
```

位置

“ `credit`”表示信用卡号智能标识符，

“`1`” 表示要使该规则求值为 true 所需的匹配数量，

“`prefix`”表示仅当智能标识符具有以智能标识符为前缀的关键字时，规则才为 true。

邮件过滤器规则说明和示例

下文介绍各种邮件过滤器规则的使用方法及其示例。

相关主题

- 重复边界验证规则, on page 51
- 格式不正确的 MIME 信头检测规则, on page 51
- 地理位置规则, on page 52
- ETF 的域信誉规则, on page 52
- SDR 的域信誉规则, on page 53

True 规则

true 规则匹配所有邮件。例如，下列规则将所测试任意邮件的 IP 接口改为外部接口。

```
externalFilter:

   if (true)

   {

        alt-src-host('external');

   }
```

Valid 规则

`valid` 规则会在邮件包含不可解析/无效 MIME 部分时返回 false，反之返回 true。例如，以下规则会丢弃测试的所有不可分析的邮件。

```
not-valid-mime:

if not valid

{

drop();

}
```

Subject 规则

`subject` 规则选择主题信头的值与给定正则表达式匹配的邮件。

例如，以下过滤器会删除主题以短语 Make Money... 开头的所有邮件

```
not-valid-mime:

if not valid

{

drop();

}
```

您可以指定在信头的值中搜索非 ASCII字符。

处理信头时，注意信头的当前值包括在处理过程中所做的更改（如使用添加、删除或修改邮件标题的过滤操作做出的更改）。有关详细信息，请参阅邮件信头规则和求值, on page 5。

如果信头为空或邮件缺失信头，以下过滤器会返回 true：

```
EmptySubject_To_filter:

if (header('Subject') != ".") OR

(header('To') != ".") {

drop();

}
```

Note 如果“Subject”和“To”信头为空，此过滤器会返回 true，如果信头缺失，同样也会返回 true。如果邮件没有指定的信头，过滤器仍会返回 true。

信封收件人规则

`rcpt-to` 规则会选择所有信封收件人与给定正则表达式匹配的邮件。例如，以下过滤器会丢弃发送地址包含字符串“scarface”的所有邮件。

Note rcpt-to 规则的正则表达式不区分大小写。

```
scarfaceFilter:

if (rcpt-to == 'scarface')

{

drop();

}
```

Note `rcpt-to` 规则基于邮件。如果一个邮件有多个收件人，那么一个收件人与指定操作规则匹配，即可将指定操作应用至发送给所有收件人的邮件。

组中的信封收件人规则

`rcpt-to-group` 规则选择信封收件人属于给定 LDAP 组的邮件。例如，以下过滤器会删除发送地址属于 LDAP 组“ExpiredAccounts”的邮件。

```
expiredFilter:

if (rcpt-to-group == 'ExpiredAccounts')

{

drop();

}
```

Note rcpt-to-group 规则基于邮件。如果一个邮件有多个收件人，那么一个收件人与指定操作规则匹配，即可将指定操作应用至发送给所有收件人的邮件。

信封发件人规则

mail-from 规则选择信封发件人与给定正则表达式匹配的邮件。例如，以下过滤器会立即传送 admin@yourdomain.com 发送的所有邮件。

Note mail-from 规则的正则表达式不区分大小写。注意，以下示例中的句点字符进行了转义。

```
kremFilter:

if (mail-from == '^admin@yourdomain\\.com$')

{

skip-filters();

}
```

组中的信封发件人规则

mail-from-group 规则选择信封发件人属于运算符右侧 LADP 组（或在不等式中，发件人的邮件地址不在特定 LDAP 组）的邮件。例如，以下过滤器会立即传送邮件地址在 LDAP 组“KnownSenders”的人员所发送的任何邮件。

```
SenderLDAPGroupFilter:

if (mail-from-group == 'KnownSenders')

{

skip-filters();

}
```

发件人组规则

sendergroup 邮件过滤器会根据侦听程序主机访问表 (HAT) 中匹配的发件人组选择邮件。本规则使用“==”（匹配）或“！=”（不匹配）测试是否与给定正则表达式（表达式右侧）匹配。例如，如果邮件的发件人组与内部正则表达式匹配，以下邮件过滤器规则会得出值 true，并将邮件发送到备用邮件主机。

```
senderGroupFilter:

if (sendergroup == "Internal")

{

alt-mailhost("[172.17.0.1]");
```

```
}
```

正文大小规则

正文大小是指邮件的大小，包括信头和附件。`body-size` 规则选择正文大小可与给定数字相比的邮件。例如，以下过滤器会退回正文大小超过 5 MB的所有邮件。

```
BigFilter:

if (body-size > 5M)

{

bounce();

}
```

`body-size` 可以通过以下方式比较：

示例	对比类型
`body-size < 10M`	少于
`body-size <= 10M`	小于或等于
`body-size > 10M`	大于
`body-size >= 10M`	大于或等于
`body-size == 10M`	平分
`body-size != 10M`	不等于

为方便起见，大小的单位可以用后缀指定：

数量	说明
`10b`	10 个字节（相当于 10）
`13k`	13 千字节
`5M`	5 兆字节
`40G`	40 千兆字节（注意：邮件网关无法接收超过 100 MB 的邮件。）

远程 IP 规则

remote-ip 规则将测试发送邮件的主机的 IP 地址是否匹配特定模式。IP 地址可以是 Internet 协议第 4 版 (IPv4) 或 Internet 协议第 6 版 (IPv6) 地址。可以使用“发件人组语法”中介绍的允许的主机符号指定 IP 地址模式，SBO、IPR、dnslist 符号和特殊关键字 ALL 除外。

允许的主机符号只能识别 IP 地址的序列和数字范围（而不是主机名）。例如，以下过滤器会退回未从 10.1.1 形式的 IP 地址注入的任何邮件。*X*，其中，其中 X 为 50、51、52、53、54 或 55。

```
notMineFilter:

if (remote-ip != '10.1.1.50-55')

{

bounce();

}
```

接收侦听程序规则

recv-listener 规则选择指定侦听程序接收的邮件。侦听程序名称必须是系统中当前配置的某个侦听程序的昵称。例如，以下过滤器会立即传送来自侦听程序 expedite 的任何邮件。

```
expediteFilter:

if (recv-listener == 'expedite')

{

skip-filters();

}
```

接收 IP 接口规则

recv-int 规则选择指定接口接收的邮件。接口名称必须是系统中当前配置的某个接口的昵称。例如，以下过滤器会退回来自接口 outside 的所有邮件。

```
outsideFilter:

if (recv-int == 'outside')

{

bounce();

}
```

日期规则

date 规则会对照指定的时间和日期检查当前时间和日期。日期规则与包含 *MM/DD/YYYY hh:mm:ss* 格式的时间戳的字符串进行比较。此规则可用于以美国日期格式指定在特定时间前后执行操作。（请注意，如果是使用非美国日期格式搜索邮件，则可能有问题。）以下邮件过滤器会退回来自 campaign1@yourdomain.com 的在 2003 年 7 月 28 日下午 1 点后注入的所有邮件：

```
TimeOutFilter:
```

```
if ((date > '07/28/2003 13:00:00') and (mail-from ==

'campaign1@yourdomain\\.com'))

{

bounce();

}
```

Note 不要将 `date` 规则与 `$Date` 邮件过滤操作变量混为一谈。

信头规则

`header()` 规则检查邮件信头中是否存在必须以（“*header name*”）格式指定的特定信头。此规则可视为正则表达式（类似于 subject 规则），也可以使用不含比较的单独形式。如单独使用，规则会在于邮件中找到信头时返回“true”，找不到信头时返回“false”。例如，以下示例检查是否存在信头 `X-Sample`，以及信头值是否包含字符串“`sample text`”。如果发现匹配，邮件就会被退回。

```
FooHeaderFilter:

if (header('X-Sample') == 'sample text')

{

bounce();

}
```

您可以指定在信头的值中搜索非 ASCII 字符。

以下示例展示不包含比较的信头规则。在这种情况下，如果发现 `X-DeleteMe` 信头，则从邮件中删除信头。

```
DeleteMeHeaderFilter:

if header('X-DeleteMe')

{

strip-header('X-DeleteMe');

}
```

处理信头时，注意信头的当前值包括在处理过程中所做的更改（如使用添加、删除或修改邮件标题的过滤操作做出的更改）。有关详细信息，请参阅邮件信头规则和求值, on page 5。

随机规则

`random` 规则生成一个介于零和 N-1 的随机数，其中 N 是规则后面括号中的整数值。正如 `header()` 规则，本规则可以在比较中使用，也可以以“一元”形式单独使用。如果生成的随机数为非零值，一元形式的规则将求出 `true` 值。例如，以下两个过滤器实际上相同，一半时间选择虚拟网关地址 A，另一半时间选择虚拟网关地址 B：

```
load_balance_a:
```

```
if (random(10) < 5)
{

alt-src-host('interface_a');
}

else

{

alt-src-host('interface_b');

}

load_balance_b:

if (random(2))

{

alt-src-host('interface_a');

}

else

{

alt-src-host('interface_b');

}
```

收件人计数规则

`rcpt-count` 规则按照与 `body-size` 规则类似的方式，将邮件的收件人数量与整数值进行对比。这可防止用户将邮件同时发送给多名收件人，或确保此类大规模传送活动通过特定虚拟网关地址。以下示例通过特定虚拟网关地址发送任何收件人数超过 100 人的邮件：

```
large_list_filter:

if (rcpt-count > 100) {

alt-src-host('mass_mailing_interface');

}
```

地址计数规则

`addr-count()` 邮件过滤器规则采用一个或多个信头字符串，计算每行中的收件人数，并返回收件人的累积数量。此过滤器与 `rcpt-count` 过滤器规则的不同之处在于，它的作用对象是邮件正文信头，不是信封收件人。以下示例展示将收件人长列表替换为“undisclosed-recipients”别名的过滤器规则：

```
count: if (addr-count("To", "Cc") > 30)
{
 strip-header("To");
 strip-header("Cc");
 insert-header("To", "undisclosed-recipients");
}
```

正文扫描规则

`body-contains()` 规则扫描传入邮件及其所有附件，以确定是否存在规则参数定义的特定模式。这包括传送状态部分和关联附件。`body-contains()` 规则不执行多行匹配。可在“扫描行为”(Scan Behavior) 页面或在 CLI 中使用 `scanconfig` 命令修改扫描逻辑，定义具体应该扫描或不扫描哪些 MIME 类型。您还可以指定扫描得出 true 值需要扫描引擎找到的最小匹配数。

默认情况下，系统扫描所有附件，除 MIME 类型为 `video/*`、`audio/*`、`image/*` 的附件之外。系统扫描存档附件 - 包含多个文件的 `.zip`、`.bzip`、`.compress`、`.tar` 或 `.gzip` 附件。您可以设置要扫描的“嵌套”存档附件数（如 `.zip` 中包含的 `.zip`。）

有关详细信息，请参阅 配置扫描行为, on page 119。

正文扫描

执行正文扫描时，AsyncOS 会扫描正文文本和附件是否存在正则表达式。您可以为表达式分配一个最小阈值，如果扫描引擎发现最少次数的正则表达式，则表达式的值为 `true`。

AsyncOS 会对邮件的不同 MIME 部分求值，并扫描任何属于文本内容的 MIME 部分。如果 MIME 类型在第一部分指定文本，AsyncOS 会识别文本部分。AsyncOS 将根据邮件中指定的编码确定编码，并将文本转换为 Unicode，然后在 Unicode 中搜索正则表达式。如果邮件中未指定编码，AsyncOS 将使用您在“扫描行为”(Scan Behavior) 页面或使用 `scanconfig` 命令指定的编码。

有关 AsyncOS 如何在扫描邮件过程中对 MIME 求值的详细信息，请参阅邮件正文与邮件附件, on page 5。

如果 MIME 部分不属于文本内容，AsyncOS 将从 .zip 或 .tar 存档文件中提取文件，或对压缩文件进行解压缩。提取数据后，扫描引擎会确定文件的编码并以 Unicode 编码形式返回文件中的数据。AsyncOS 然后会在 Unicode 中搜索正则表达式。

以下示例在正文文本和附件中搜索短语“Company Confidential”。示例指定两个实例的最小阈值，因此，如果找到短语的两个或多个实例，扫描引擎会退回所有匹配邮件，并通知法律部门此次尝试：

```
ConfidentialFilter:

if (body-contains('Company Confidential',2)) {

notify ('legaldept@example.domain');

bounce();

}
```

如仅扫描邮件的正文，请使用 `only-body-contains`：

```
disclaimer:

if (not only-body-contains('[dD]isclaimer',1) ) {

notify('hresource@example.com');

}
```

加密检测规则

encrypted规则检查邮件内容中是否包含加密数据。它不会对加密数据进行解码，仅检查邮件内容中是否存在加密数据。这可以防止用户发送加密邮件。

Note encrypted 规则只能检测邮件内容中的加密数据，不检测加密的附件。

encrypted规则与true规则的相似之处在于，它不使用参数，也无法进行比较。如果发现加密数据，此规则会返回true，如果未找到加密数据，返回 false。由于此功能需要扫描邮件，它将使用您在“扫描行为”(Scan Behavior) 页面或使用 scanconfig 命令定义的扫描设置。有关配置这些选项的详细信息，请参阅配置扫描行为, on page 119。

下列过滤器检查所有通过侦听程序发送的邮件，因此，如果邮件中包含加密数据，该邮件将密件抄送到法律部门然后被退回:

```
prevent_encrypted_data:

if (encrypted) {

bcc ('legaldept@example.domain');

bounce();

}
```

附件类型规则

attachment-type规则会检查邮件中每个附件的MIME类型，确定附件是否匹配指定模式。模式必须采用“扫描行为”(Scan Behavior) 页面或 scanconfig 命令中的形式（如配置扫描行为, on page 119所述），因此可能会使用星号替换斜线 (/) 的任意一侧，以作为通配符。如果邮件中包含与指定 MIME 类型匹配的附件，此规则会返回“true”。

由于此功能需要扫描邮件，它将应用配置扫描行为, on page 119所述的所有选项。

有关可以使用哪些邮件过滤器规则来管理邮件附件的详细信息，请参阅附件扫描, on page 86。

下列过滤器检查所有通过侦听程序发送的邮件，如果邮件中包含 MIME 类型为 video/* 的附件，邮件会被退回：

```
bounce_video_clips:

if (attachment-type == 'video/*') {

bounce();

}
```

附件文件名规则

attachment-filename 规则会检查邮件中每个附件的文件名，确定文件名是否匹配给定正则表达式。比较文件名时区分大小写。但是，比较会检查空格，如果文件名以空格结尾，过滤器就会跳过附件。如果邮件的其中一个附件与文件名匹配，此规则会返回“true”。

请注意以下问题：

- 每个附件的文件名从 MIME 信头头中捕获。MIME 信头中的文件名可能包含行尾空格。
- 如果附件是存档文件，邮件网关会从存档文件中收集文件名，并相应地应用扫描配置规则（请参阅配置扫描行为, on page 119）。
  - 如果附件是单个压缩文件（不论文件扩展名如何），设备不会视其为存档文件，不会收集压缩文件的文件名。这意味着文件不被 attachment-filename 规则处理。通过 gzip 压缩的可执行程序 (.exe) 便是这类文件。
  - 对于包括一个压缩文件的 foo.exe.gz 等附件，可使用正则表达式搜索压缩文件中的特定文件类型。请参阅附件文件名和存档文件中的单个压缩文件, on page 35。

有关可以使用哪些邮件过滤器规则来管理邮件附件的详细信息，请参阅附件扫描, on page 86。

下列过滤器检查所有通过侦听程序发送的电子邮件，如果邮件中包含文件名为 *.mp3 的附件，邮件会被退回：

```
block_mp3s:

if (attachment-filename == '(?i)\\.mp3$') {

bounce();

}
```

相关主题

- 附件文件名和存档文件中的单个压缩文件, on page 35

附件文件名和存档文件中的单个压缩文件

此示例展示如何匹配存档文件中的单个压缩文件（如 gzip 创建的存档文件）：

```
quarantine_gzipped_exe_or_pif:

if (attachment-filename == '(?i)\\.(exe|pif)($|.gz$)') {

quarantine("Policy");

}
```

DNS 列表规则

dnslist() 规则会查询使用 DNSBL 方法（有时称为“ip4r 查询”）进行查询的公共 DNS 列表服务器。传入连接的 IP 地址被放入括号中并以反写的形式（即 IP 1.2.3.4.4 变成 4.3.2.1)添加为服务器名称的前缀（如果服务器名称不以 1 开头，则添加句点将服务器名称与 IP 地址隔开）。然后执行 DNS 查询，系统会返回 DNS 失败响应（表示在服务器列表中找不到连接的 IP 地址）或 IP 地址（表示找

到该地址）。返回的 IP 地址的格式 通常 是 `127.0.0.x`，其中 `x` 几乎可以是从 0 到 255 之间的任何数字（不允许 IP 地址范围）。实际上，有些服务器会根据列入原因返回不同的数字，其他服务器则会对所有匹配返回相同的结果。

正如 `header()` 规则，`dnslist()` 规则也可用于一元或二进制比较。本质上，此规则会在收到响应时返回 `true` 值，在收不到响应时返回 `false` 值（例如，如果无法与 DNS 服务器通信）。

如果发件人已通过思科担保发件人信息服务计划进行担保，则以下过滤器会立即传送邮件：

```
allowedlist_bondedsender:

if (dnslist('query.bondedsender.org')) {

skip-filters();

}
```

或者，您可以使用等于 (==) 或不等于 (!=) 表达式，将结果与字符串进行比较。

下列过滤器丢弃了服务器对其做出出“`127.0.0.2`”响应的邮件。如果响应是其他结果，规则会返回“false”，过滤器会被忽略。

```
blockedlist:

if (dnslist('dnsbl.example.domain') == '127.0.0.2') {

drop();

}
```

IP 信誉规则

`reputation` 规则根据另一个值检查 IP 信誉得分。支持所有比较运算符，例如，>、==、<= 等。如果邮件根本没有 IP 信誉得分（由于从未检查过该得分，或由于系统收不到 IP 信誉服务查询服务器的响应），所有信誉比较都会失败（数字不会大于、小于、等于或不等于任何值）。您可以使用下文介绍的 `no-reputation` 规则，检查 IP 信誉得分是否为“无”(None)。以下示例将邮件的“Subject:”行调整为，在 IP 信誉服务返回的信誉得分小于阈值 -7.5 时添加前缀“`*** BadRep ***`”。

```
note_bad_reps:

if (reputation < -7.5) {
strip-header ('Subject');
insert-header ('Subject', '*** BadRep $Reputation *** $Subject');
}
```

有关详细信息，请参阅“发件人信誉过滤”一章。另请参阅绕过反垃圾邮件系统操作, on page 80

IP 信誉规则的值介于 -10 和 10 之间，但也可能会返回值 NONE。要指定查找值 `NONE`，请使用 `no-reputation` 规则。

```
none_rep:

if (no-reputation) {

strip-header ('Subject');

insert-header ('Subject', '*** Reputation = NONE *** $Subject');
```

```
}
```

词典规则

如果邮件正文包含“*dictonary_name*”词典中的任何正则表达式或术语，则 `dictionary-match(< dictonary_name >)` 规则将返回 `true` 值。如果词典不存在，此规则的值为 `false`。有关定义词典的详细信息（包括大小写和词边界设置），请参阅“文本资源”一章。

当思科扫描包含“secret_words”词典中任何词语的邮件时，下列过滤器将密件抄送管理员。

```
copy_codenames:

if (dictionary-match ('secret_words')) {

bcc('administrator@example.com');

}
```

以下示例将邮件发送到“策略”(Policy) 隔离区，如果邮件正文中包含“secret_words”词典中的任何词语。与 `only-body-contains` 条件不同的是，`body-dictionary-match` 条件不要求所有内容部分均与词典匹配。每个内容部分的得分（考虑到多部分/备用部件）相加。

```
quarantine_data_loss_prevention:

if (body-dictionary-match ('secret_words'))

{

quarantine('Policy');

}
```

在以下过滤器中，主题与指定词典中某个术语匹配的邮件被隔离：

```
quarantine_policy_subject:

if (subject-dictionary-match ('gTest'))

{

quarantine('Policy');

}
```

此示例匹配“to”信头中的邮件地址，并密件抄送管理员：

```
headerTest:

if (header-dictionary-match ('competitorsList', 'to'))

{

bcc('administrator@example.com');

}
```

`attachment-dictionary-match(<dictonary_name>)` 规则的原理与上文的 `dictionary-match` 规则相似，不同的是本规则搜索附件中的匹配项。

下列过滤器会将邮件发送到 Policy 隔离区，如果邮件附件包含“secret_words”词典中的任何词语。

```
quarantine_codenames_attachment:

if (attachment-dictionary-match ('secret_words'))

{

quarantine('Policy');

}
```

`header-dictionary-match(<dictonary_name>, <header>)` 规则的原理与上文的 dictionary-match 规则相似，不同的是本规则在信头中搜索 *<header >* 中指定的匹配项。信头名称不区分大小写，因此，“subject”和“Subject”都适用。

下列过滤器会将邮件发送到“策略”(Policy) 隔离区，如果邮件的“cc”信头包含“ex_employees”词典中的任何词语。

```
quarantine_codenames_attachment:

if (header-dictionary-match ('ex_employees', 'cc'))

{

quarantine('Policy');

}
```

您可以在词典术语中使用通配符。不必转义邮件地址中的句点。

SPF-Status 规则

收到 SPF/SIDF 验证邮件时，您可能会根据 SPF/SIDF 验证结果采取不同的操作。spf-status 规则会根据不同的 SPF 证结果执行检查。有关详细信息，请参阅验证结果。

Note 如果您配置了没有 SPF 身份的 SPF 验证邮件过滤器规则，并且如果邮件包含具有不同判定的不同 SPF 身份，则邮件中的某个判定与该规则匹配时，将触发该规则。

您可以使用以下语法检查 SPF/SIDF 验证结果：

```
if (spf-status == "Pass")
```

如果您希望在一个条件中检查多个状态判断，可以使用以下语法：

```
if (spf-status == "PermError, TempError")
```

此外，您还可以使用以下语法，根据 HELO、MAIL FROM 以及 PRA 身份检查验证结果：

```
if (spf-status("pra") == "Fail")
```

以下示例展示 spf-status 过滤器的实际应用：

```
skip-spam-check-for-verified-senders:
if (sendergroup == "TRUSTED" and spf-status == "Pass"){
skip-spamcheck();
}
quarantine-spf-failed-mail:
if (spf-status("pra") == "Fail") {
if (spf-status("mailfrom") == "Fail"){
# completely malicious mail
quarantine("Policy");
} else {
if(spf-status("mailfrom") == "SoftFail") {
# malicious mail, but tempting
quarantine("Policy");
}
}
} else {
if(spf-status("pra") == "SoftFail"){
if (spf-status("mailfrom") == "Fail"
or spf-status("mailfrom") == "SoftFail"){
# malicious mail, but tempting
quarantine("Policy");
}
}
}
stamp-mail-with-spf-verification-error:
if (spf-status("pra") == "PermError, TempError"

or spf-status("mailfrom") == "PermError, TempError"
or spf-status("helo") == "PermError, TempError"){
# permanent error - stamp message subject
```

```
strip-header("Subject");

insert-header("Subject", "[POTENTIAL PHISHING] $Subject"); }

.
```

SPF-Passed 规则

以下示例展示使用 `spf-passed` 规则隔离未标记为 spf-passed 的邮件：

```
quarantine-spf-unauthorized-mail:

if (not spf-passed) {

quarantine("Policy");

}
```

Note 不同于 `spf-status` 规则，spf-passed 规则将 SPF/SIDF 验证值简化为简单的布尔值。以下验证结果在 `spf-passed` 规则中被视为未通过：None、Neutral、Softfail、TempError、PermError 以及 Fail。要基于更为精细的结果对邮件执行操作，请使用 `spf-status` 规则。

S/MIME 网关邮件规则

S/MIME 网关邮件规则检查邮件是否经过 S/MIME 签名、加密或签名并加密。下列邮件过滤器检查邮件是否为 S/MIME 邮件，并在使用 S/MIME 的验证或解密失败时对邮件进行隔离。

```
quarantine_smime_messages:
if (smime-gateway-message and not smime-gateway-verified) {
quarantine("Policy");
}
```

有关详细信息，请参阅 S/MIME 安全服务。

S/MIME 网关验证规则

S/MIME 网关邮件验证规则检查邮件是否成功通过验证、解密或已成功解密并验证。下列邮件过滤器检查邮件是否为 S/MIME 邮件，并在使用 S/MIME 的验证或解密失败时对邮件进行隔离。

```
quarantine_smime_messages:
if (smime-gateway-message and not smime-gateway-verified) {
quarantine("Policy");
}
```

有关详细信息，请参阅S/MIME 安全服务

工作队列计数规则

`workqueue-count` 规则根据指定值检查队列计数。支持所有比较运算符，例如，`>`、`==`、`<=` 等。

下列过滤器检查队列计数，并在队列超过指数目时跳过垃圾邮件检查。

```
wqfull:

if (workqueue-count > 1000) {

skip-spamcheck();

}
```

有关 SPF/SIDF 的详细信息，请参阅SPF 和 SIDF 验证概述。

SMTP 身份验证用户匹配规则

如果您的邮件网关使用 SMTP 身份验证发送邮件，`smtp-auth-id-matches` (<*target*> *[,* <*sieve-char*>*]*) 规则将根据发件人的SMTP身份验证用户ID检查邮件的信头和信封发件人，确定传出邮件是否包含欺骗性的信头。系统可使用此过滤器隔离或阻止潜在欺骗邮件。

`smtp-auth-id-matches` 规则会将 SMTP 身份验证 ID 与以下对象进行对比：

目标	说明
*EnvelopeFrom	比较 SMTP 会话中信封发件人（也称为 MAIL FROM）的地址
*FromAddress	比较从“From”信头解析出的地址。“From:”信头允许多个地址，一个地址匹配即可。
*Sender	比较“Sender”信头中指定的地址。
*Any	匹配在 SMTP 验证会话期间创建的任何邮件，不论各方身份如何。
*None	匹配并非在 SMTP 验证会话期间创建的邮件。此选项在身份验证非必选时（首选）时非常实用。

过滤器执行非严格匹配。不区分大小写。如果提供 *sieve-char* 可选参数，对比将忽略地址中指定字符后面的最后一部分。例如，如果参数中包含 + 字符，过滤器将忽略地址 address `joe+folder@example.com` 中 + 字符后面的部分。如果地址是 `joe+smith+folder@example.com`，过滤器仅忽略 `+folder` 部分。如果SMTP身份验证用户ID字符串是简单的用户名，而不是完全限定的邮件地址，过滤器将仅检查对象的用户名部分，确定是否存在匹配。必须使用单独的规则验证域。

此外，您可以使用 $SMTPAuthID 变量将 STMP 身份验证用户 ID 插入信头。

下表展示使用 `smtp-auth-id-matches` 过滤器规则对比 SMTP 身份验证用户 ID 和邮件地址以及他们是否匹配的情景：

SMTP 身份验证 ID	Sieve Char	对比地址	是否匹配？
someuser		otheruser@example.com	否
someuser		someuser@example.com	是
someuser		someuser@another.com	是
SomeUser		someuser@example.com	是

SMTP 身份验证 ID	Sieve Char	对比地址	是否匹配？
someuser		someuser+folder@example.com	否
someuser	+	someuser+folder@example.com	是
someuser@example.com		someuser@forged.com	否
someuser@example.com		someuser@example.com	是
SomeUser@example.com		someuser@example.com	是

下列过滤器检查在 SMTP 验证会话期间创建的所有邮件，确定“From”信头中的地址和信封发件人是否与 SMTP 身份验证用户 ID 匹配。如果地址和 ID 匹配，过滤器将验证域。如果不匹配，邮件网关将隔离邮件。

```
Msg_Authentication:

if (smtp-auth-id-matches("*Any"))

{

# Always include the original authentication credentials in a

# special header.

insert-header("X-Auth-ID","$SMTPAuthID");

if (smtp-auth-id-matches("*FromAddress", "+") and

smtp-auth-id-matches("*EnvelopeFrom", "+"))

{

# Username matches. Verify the domain

if header('from') != "(?i)@(?:example\\.com|alternate\\.com)" or

mail-from != "(?i)@(?:example\\.com|alternate\\.com)"

{

# User has specified a domain which cannot be authenticated

quarantine("forged");

}

} else {

# User claims to be an completely different user

quarantine("forged");

}

}
```

已签名规则

已签名规则检查邮件是否已签名。该规则将返回布尔值，表明邮件是否已签名。此规则将评估签名是否根据 ASN.1 DER 编码规则编码，以及是否采用 CMS SignedData 结构类型（RFC 3852 第 5.1 节）。它并不验证签名是否与内容匹配，也不检查证书的有效性。

以下示例使用已签名规则将信头插入签名邮件：

```
signedcheck: if signed { insert-header("X-Signed", "True"); }
```

以下示例使用已签名规则删除来自特定发件人组未签名邮件的附件：

```
Signed: if ((sendergroup == "NOTTRUSTED") AND NOT signed) {

html-convert();

if (attachment_size > 0)

{

drop_attachments("");

}

}
```

签名证书规则

signed-certificate 规则选择 X.509 证书颁发机构或邮件签署人与指定正则表达式匹配的 S/MIME 邮件。此规则仅支持 X.509 证书。

规则语法为 signed-certificate (<字段> [<运算符> <正则表达式>])，其中：

- <字段> 是带引号的字符串“issuer”或“signer”，
- <运算符> 是 == 或 !=，
- <正则表达式> 是匹配“issuer”或“signer”的值。

使用多个签名对邮件签名时，如果其中任何一个颁发机构或签署人匹配正则表达式，规则会返回 true。此规则的简短形式 signed-certificate(“issuer”) 和 signed-certificate(“signer”) 会在 S/MIME 邮件包含颁发机构或签署人时返回 true。

相关主题

- 签署人, on page 43
- 颁发机构, on page 44
- 正则表达式中的转义, on page 44
- $CertificateSigners 操作变量, on page 44
- 示例 1, on page 45

签署人

规则会从 X.509 证书的 subjectAltName 扩展名中抽取 rfc822Name 名称序列作为邮件的签署人。如果签名证书没有 subjectAltName 字段，或者此字段没有任何 rfc822Name 名称，

signed-certificate(“signer”) 规则会求出值 false。在极少数存在多个 rfc822Name 名称的情况下，规则会尝试将所有名称与正则表达式进行匹配，并在找到第一个匹配项时求出值 true。

颁发机构

颁发机构是 X.509 证书中非空的可识别名称。AsyncOS 将从证书提取颁发机构并将其转换为 LDAP - UTF8 Unicode 字符串。例如：

- C=US、S=CA、O=IronPort
- C=US、CN=Bob Smith

由于 X.509 证书需要颁发机构字段，signed-certificate(“issuer”) 将评估 S/MIME 邮件是否包含 X.509 证书。

正则表达式中的转义

LDAP - UTF8 定义了可在正则表达式中使用的转义机制。有关 LDAP - UTF8 中转义字符的深入探讨，请参阅“轻量级目录访问协议 (LDAP)：可识别名称的字符串表示”（访问地址：http://www.ietf.org/rfc/rfc4514.txt）。

signed-certificate 规则中正则表达式的转义规则不用于 LDAP-UTF8 中定义的转义规则，前者仅对需要转义的字符进行转义。LDAP-UTF8 允许对无需转义即可表示的字符进行选择性转义。例如，以下两个针对“Example, Inc.”的字符串在使用 LDAP-UTF8 转义规则时都被视为正确：

- Example\, Inc.
- Example\,\ Inc\.

但是，signed-certificate 规则仅匹配 Example\, Inc.。正则表达式不允许在匹配时转义空格和句点，因为这些字符不需要转义，即使在 LDAP-UTF8 中允许转义。为 signed-certificate 规则创建正则表达式时，如果字符无需转义即可表示，请不要对字符转义。

$CertificateSigners 操作变量

`$CertificateSigners` 操作变量是从签名证书的 `subjectAltName` 要素中获取的签署人逗号分隔列表。列表包含单个签署人的多个邮件地址，而且已删除重复地址。

例如，Alice 使用两个证书对邮件签名。Bob 使用唯一证书对邮件签名。这些证书由同一家公司机构颁发。邮件通过 S/MIME 扫描后，提取的数据包含三个要素：

```
[

{

'issuer': 'CN=Auth,O=Example\, Inc.',

'signer': ['alice@example.com', 'al@private.example.com']

},

{

'issuer': 'CN=Auth,O=Example\, Inc.',

'signer': ['alice@example.com', 'al@private.example.com']

},
```

```
{
'issuer': 'CN=Auth,O=Example\, Inc.',
'signer': ['bob@example.com', 'bob@private.example.com']
}
]
```

`$CertificateSigners` 变量扩展为：

```
"alice@example.com, al@private.example.com, bob@example.com, bob@private.example.com"
```

示例 1

以下示例在证书颁发机构来自美国时插入新的信头：

```
Issuer: if signed-certificate("issuer") == "(?i)C=US" {
insert-header("X-Test", "US issuer");
}
```

以下示例在签署人并非来自 example.com 时通知管理员：

```
NotOurSigners: if signed-certificate("signer") AND
signed-certificate("signer") != "example\\.com$" {
notify("admin@example.com");
}
```

以下示例在邮件包含 X.509 证书时添加信头：

```
AnyX509: if signed-certificate ("issuer") {
insert-header("X-Test", "X.509 present");
}
```

以下示例在邮件的证书不含签署人时添加信头：

```
NoSigner: if not signed-certificate ("signer") {
insert-header("X-Test", "Old X.509?");
}
```

信头重复规则

如果在给定时间点检测到满足以下条件的指定数量邮件，信头重复规则将得出 true 值：

- 在前一小时内检测到主题相同的邮件。
- 在前一小时内检测来自同一信封发件人的邮件。

您可以使用此规则检测大量邮件。例如，政治运动会通过某些网站向机构发送大量邮件。反垃圾邮件引擎将此类邮件处理为正常邮件，不会停止邮件传送。

此规则的语法是 header-repeats (<target>, <threshold> [, <direction>])，其中：

- <target> 是 subject 或 mail-from。AsyncOS 会计入目标的重复值。
- <threshold> 是前一小时内收到的指定对象值相同的邮件的数量，超出该数量后，规则将得出 true 值。
- <direction> 是传入和/或传出。如果未指定方向，规则求值时将对传入或外发邮件计数。

只要信头重复规则得出 true 值，设备就会发送系统警告。请参阅系统警告。

Note 如果信头字段包含逗号或分号分隔值，规则在跟踪时会考虑整个字符串。此规则忽略主题信头为空的邮件。

信头重复规则将不断变化的邮件总数量精确到一分钟内。因此，达到设置阈值后，触发规则可能会出现一分钟的延迟。

相关主题

- 将信头重复规则与其他规则结合使用, on page 46
- 示例, on page 46

将信头重复规则与其他规则结合使用

您可以使用 AND 或 OR 运算符，将信头重复规则与其他规则结合使用。例如，使用以下过滤器，可以将一部分邮件列入允许列表：

```
F1: if (recv_listener == 'Gray')  AND (header-repeats('subject', X, 'incoming') { drop();}
```

使用 AND 或 OR 运算符将信头重复规则与其他规则结合使用时，设备将最后对信头重复规则求值，并且只在必要时求值。如果不对给定邮件求信头重复规则的值，则与指定阈值比较时将不计入 subject 或 mail-from。

由于仅在必要时最后求信头重复规则的值，使用 OR 运算符将其与其他规则结合使用时，此规则的行为可能会有所不同。以下示例过滤器使用签名和信头重复规则的 OR 条件。

```
f1: if signed OR (header-repeats('subject', 10)) { drop();}
```

在本例中，如果过滤器处理的前九封邮件是主题相同的签名邮件，信头重复规则将不处理这些邮件。如果第十封邮件是主题信头与前九封邮件相同的未签名邮件，即使已达到阈值，过滤器也不会执行配置的操作。

示例

在下面的示例中，在任何给定时间，如果过滤器在前一小时内检测到 X 封或更多主题相同的传入邮件，主题相同的后续邮件将被发送到“策略”隔离区。

```
f1 : if header-repeats('subject', X, 'incoming') { quarantine('Policy');}
```

在下面的示例中，在任何给定时间，如果过滤器在前一小时内检测到 X 封或更多来自来自同一信封发件人的外发邮件，来自同一信封发件人的后续邮件将被删除。

```
f2 :  if header-repeats('mail-from', X, 'outgoing') {drop();}
```

在下面的示例中，在任何给定时间，如果过滤器在前一小时内检测到 X 封或更多主题相同的传入或外发邮件，每检测到一封主题相同的后续邮件，设备都会通知管理员。

```
f3: if header-repeats('subject', X) {notify('admin@xyz.com');}
```

URL 信誉规则

使用 URL 信誉规则定义基于邮件中所有 URL 信誉得分的邮件操作。有关重要详细信息，请参阅防御恶意或不需要的 URL中的按 URL 信誉或 URL 类别过滤：条件和规则

在这些规则中：

- `Msg_filter_name` 为邮件过滤器的名称。
- `allowedlist` 为已定义 URL 列表的名称（通过 urllistconfig 命令定义）。指定允许列表为可选。

要在信誉服务提供得分时执行操作，请执行以下操作：

使用 `url-reputation` 规则。

使用 url-reputation 规则时，过滤器语法如下：

```
<msg_filter_name>:

if url-reputation('<min_score'>, <'max_score'>, '<allowedlist>',
'<include_attachments>','<include_message_body_subject>')

{<action>}
```

其中：

- `min_score` 和 `max_score` 是操作应用范围的最小和最大得分。指定的值应该在该范围内。

最小和最大得分必须介于 `-10.0` 和 `10.0` 之间。

- `include_attachments` 用于扫描邮件附件中的 URL。值“1”表示已启用对邮件附件的 URL 扫描，值“0”表示未启用对邮件附件的 URL 扫描。
- `include_message_body_subject` 用于扫描邮件正文和主题中的 URL。值“1”表示已启用对邮件正文和主题的 URL 扫描，值“0”表示未启用对邮件正文和主题的 URL 扫描。

要在信誉服务不提供得分时执行操作，请执行以下操作：

使用 `url-no-reputation` 规则。

使用 `url-no-reputation` 规则时，过滤器语法如下：

```
<msg_filter_name>:

if url_no_reputation('<allowedlist>',
'<include_attachments>','<include_message_body_subject>')

{<action>}
```

URL 类别规则

使用 URL 类别定义基于邮件中 URL 类别的邮件操作。有关重要详细信息，请参阅防御恶意或不需要的 URL中的按 URL 信誉或 URL 类别过滤：条件和规则。

使用 `url-category` 规则时，过滤器语法如下：

```
<msg_filter_name>: if url-category ([ '<category-name1>' ,' <category-name2>' ,...,
 '<category-name3>' ],' <url_allowed_list>' ,'<include_attachments>','<include_message_body_subject>')

<action>
```

其中：

- `msg_filter_name` 是此邮件过滤器的名称。
- `action` 是任何邮件过滤器操作。
- `category-name` 是 URL 类别。使用逗号分隔多个类别。要获得正确的类别名称，请查看内容过滤器中的 URL 类别条件或操作。有关类别的说明和示例，请参阅关于 URL 类别。
- `url_allowed_list` 为已定义 URL 列表的名称（通过 urllistconfig 命令定义）。
- `include_attachments` 用于扫描邮件附件中的 URL。值“1”表示已启用对邮件附件的 URL 扫描，值“0”表示未启用对邮件附件的 URL 扫描。
- `include_message_body_subject` 用于扫描邮件正文和主题中的URL。值“1”表示已启用对邮件正文和主题的 URL 扫描，值“0”表示未启用对邮件正文和主题的 URL 扫描。

损坏的附件规则

如果邮件中包含损坏的附件，则损坏的附件规则的值为 true。损坏的附件是扫描引擎不可扫描且识别为已损坏的附件。

相关主题

- 示例, on page 48

示例

在下面的示例中，如果过滤器检测到邮件中存在损坏的附件，邮件将被隔离到 Policy 隔离区。

```
quar_corrupt_attach: if (attachment-corrupt) { quarantine("Policy"); }
```

邮件语言规则

您可能希望基于邮件语言采取不同的邮件操作。例如，您可能需要：

- 将俄语中的免责声明添加到使用俄语的邮件中
- 丢弃无法确定其语言的邮件

使用邮件语言规则根据邮件主题和正文的语言来执行邮件操作。

Note 此条件不会检查附件和信头使用的语言。

语言检测工作原理

邮件网关使用内置语言检测引擎来检测邮件中所采用的语言。邮件网关将提取主题和邮件正文，并将其传递到语言检测引擎。

语言检测引擎将确定提取的文本中每种语言的概率，并将其传递回邮件网关。邮件网关将概率最高的语言视为邮件的语言。在下列某种情况下，邮件网关会将邮件的语言视为“待定”：

- 如果邮件网关不支持检测到的语言
- 如果邮件网关无法检测到邮件的语言
- 如果发送到语言检测引擎的提取文本的总大小小于 50 字节。

邮件过滤器语法

```
<msg_filter_name>: if (message-language <operator> "<language1>, <language2>,..., <language n>") {<action>}
```

其中：

- `msg_filter_name` 是此邮件过滤器的名称。
- 运算符为 `==` 或 `!=`。
- `language` 是要在此邮件过滤器中指定的邮件语言的值。使用逗号分隔多个条目。有关支持的邮件语言和值的列表，请查看内容过滤器中的邮件语言条件。值用方括号（[和]）括起来。
- `action` 是任何邮件过滤器操作。

示例

以下示例展示了如何丢弃无法确定其语言的邮件：

```
DropMessagesWithUndeterminedLanguage: if (message-language == "unknown") { drop(); }
```

以下示例展示了如何将俄语免责声明添加到俄语邮件中：

```
ussianDisclaimerRule: if (message-language == "ru") { add-heading("RussianDisclaimer");
```

宏检测规则

可以使用宏检测规则来检测指定文件类型的邮件中启用了宏的附件。

注释 如果存档或嵌入文件包含宏，则会从邮件中删除父文件。

注释 如果任何附件（例如 Excel 或 Word）不包含任何宏，但具有宏扩展名（例如 .xlsm 或 .docm），它们仍将被视为具有宏的文件。这些文件将被关联的过滤器标记为启用宏的附件。

宏检测语法

```
<msg_filter_name>: if (macro-detection-rule (['file_type-1', 'file_type-2',...
,' file_type-n'])) {<action>}
```

其中：

- `msg_filter_name` 是此邮件过滤器的名称。
- `file_type` 可以是以下任一受支持的文件类型：
  - `Adobe 便携式文档格式`
  - `Microsoft Office 文件`
  - `OLE 文件类型`
- `action` 是任何邮件过滤器操作。

示例

下面的示例演示如何删除包含启用了宏的 Microsoft Office 附件的邮件：

```
Drop_Messages_With_Macro-enabled_Office_Files: if (macro-detection-rule (['Microsoft Office
Files'])) { drop(); }
```

在下面的示例中，如果将包含启用宏的 PDF 格式附件的邮件发送到特定用户，则会删除该邮件：

```
Strip_Macro_enabled_PDF: if (rcpt-to == "joe@example.com") {
drop-macro-enabled-attachments(['Adobe Portable Document Format']); }
```

伪造邮件检测规则

您可能希望检测带有伪造发件人地址（“发件人:”信头）的欺诈邮件，并对此类邮件执行操作。

使用 forged-email-detection 规则检测此类邮件。在配置此规则时，必须指定内容词典以及将邮件视为潜在伪造邮件的阈值（1 到 100）。

forged-email-detection 规则将“发件人:”信头与内容词典中的用户进行比较。在此过程中，邮件网关将根据相似性为词典中的每个用户分配相似性得分。以下列出某些示例：

- 如果“发件人:”信头为 <j0hn.sim0ns@example.com>，并且内容词典包含用户“John Simons”，则邮件网关会将相似性得分 82 分配给该用户。
- 如果“发件人:”信头为 <john.simons@diff-example.com>，并且内容词典包含用户“John Simons”，则邮件网关会将相似性得分 100 分配给该用户。

相似性得分越高，邮件是伪造邮件的可能性就越大。如果相似性得分高于或等于指定的阈值，则会触发过滤器操作。

有关详细信息，请参阅伪造邮件检测。

邮件过滤器语法

```
<filter_name>: if (forged-email-detection(“<content_dictionary>”, threshold)) {<action>;}
```

其中：

- filter_name 是邮件过滤器的名称
- content_dictionary 是内容词典的名称
- threshold 是将邮件视为潜在伪造邮件的阈值（1 到 100）

示例

以下邮件过滤器将邮件中的“发件人:”信头与词典中的术语进行比较，如果内容词典中用户的相似性得分大于或等于 70，则邮件过滤器将删除“发件人:”信头并将其替换为信封发件人。

```
FED_CF: if (forged-email-detection("Execs", 70)) { fed("from", ""); }
```

重复边界验证规则

可以使用 duplicate_boundaries 规则检测包含重复 MIME 边界的邮件。

Note 基于附件的规则（例如，attachment-contains）或操作（例如，drop-attachments-where-contains）将无法处理格式错误的邮件（具有重复的 MIME 边界）。

邮件过滤器语法

```
<filter_name>: if (duplicate_boundaries){<action>;}
```

示例

以下邮件过滤器将隔离包含重复 MIME 边界的所有邮件。

```
DuplicateBoundaries: if (duplicate_boundaries) { quarantine("Policy"); }
```

格式不正确的 MIME 信头检测规则

可以使用格式不正确的信头规则检测包含格式错误的 MIME 信头的邮件。

邮件过滤器语法

```
<filter_name>: if (malformed-header){<action>;}
```

示例

下面的示例展示了如何隔离 MIME 信头的格式错误的所有邮件：

```
quarantine_malformed_headers: if (malformed-header)
{
quarantine("Policy");
}
```

地理位置规则

您可以使用地理位置规则来处理来自您所选特定国家/地区的传入邮件。

地理位置语法

```
<msg_filter_name>: if (geolocation-rule (['country_name-1', 'country_name-2',...
,' country_name-n'])) {<action>}
```

其中：

- `msg_filter_name` 是此邮件过滤器的名称。
- `country_name` 可以是您所选的任何国家/地区的名称。
- `action` 是任何邮件过滤器操作。

示例

下面的示例演示如何隔离来自 Country1 和 Country2 的传入邮件：

```
Quarantine_Incoming_Messages_from_Country1_and_Country2: if (geolocation-rule
(['Country1', 'Country2'])) {quarantine("Policy");}
```

ETF 的域信誉规则

例如，使用以下邮件过滤器规则语法来检测使用 ETF 引擎的邮件中的恶意域，并对此类邮件执行适当的操作。

语法：

```
quarantine_msg_based_on_ETF: if (domain-external-threat-feeds (['etf_source1'],
 ['mail-from', 'from'], <'domain_exception_list'>)) { quarantine("Policy"); }
```

位置

- ‘`domain-external-threat-feeds`' 是域信誉邮件过滤器规则。
- ‘`etf_source1`' 是用于在邮件的信头中检测恶意域的 ETF 源。
- ‘`mail-from`','`from`' 是用于检查域信誉的所需信头。
- '`domain_exception_list`' 是域例外列表的名称。如果不存在域例外列表，它将显示为 ""。

示例

在以下示例中，如果 ETF 引擎检测到 'Errors To:' 自定义信头中的域为恶意域，则该邮件将被隔离。

```
Quaranting_Messages_with_Malicious_Domains: if domain-external-threat-feeds
(['threat_feed_source'], ['Errors-To'], "")) {quarantine("Policy");}
```

SDR 的域信誉规则

您可以使用域信誉规则根据 SDR 过滤邮件，并对此类邮件执行相应的操作：

- 发件人域判定
- 发件人域有效期
- 发件人域不可扫描

根据发件人域判定过滤邮件

注释 建议的阻止阈值为“差”。有关 SDR 的详细信息，请联系思科 Talos：https://www.talosintelligence.com。

语法：

```
drop_msg_based_on_sdr_verdict:
if sdr-reputation (['awful', 'poor'], "<domain_exception_list>")
{drop();}
```

其中：

- `'drop_msg_based_on_sdr_verdict'` 是邮件过滤器的名称。
- `'sdr-reputation'` 是域信誉邮件过滤器规则。
- `'awful','poor'` 是用于根据 SDR 过滤邮件的发件人域判定的范围。
- `'domain_exception_list'` 是域例外列表的名称。如果不存在域例外列表，它将显示为 ""。
- `'drop'` 是在邮件上应用的操作。

示例

在以下邮件中，如果 SDR 判定为“未知”，则该邮件将被隔离。

```
quarantine_unknown_sdr_verdicts:
if sdr-reputation (['unknown'], "")
{quarantine("Policy")}
```

根据发件人域有效期过滤邮件

注释 “发件人域有效期”(Sender Domain Age) 选项将在下一个 AsyncOS 版本中删除。

语法：

```
<msg_filter_name>
if sdr-age (< ‘unit'>, < ‘operator'> < ‘actual value’ >)
{<action>}
```

其中：

- ‘sdr-reputation' 是域信誉邮件过滤器规则。
- ‘sdr_age’ 是用于根据 SDR 过滤邮件的发件人域的有效期。
- ‘unit' 是“天数”、“年”、“月”或“周”选项，用于根据发件人域有效期过滤邮件
- ‘operator' 是以下比较运算符，用于根据发件人域有效期过滤邮件：
  - - >（大于）
  - - >=（大于或等于）
  - - <（小于）
  - - <=（小于或等于）
  - - ==（等于）
  - - !=（不等于）
  - - 未知
- ‘actual value' 是用于根据发件人的域有效期过滤邮件的编号。

示例

在以下邮件中，如果发件人的域有效期未知，则该邮件将被丢弃。

```
Drop_Messages_Based_On_SDR_Age: if (sdr-age ("unknown", "")) {drop();}
```

在以下邮件中，如果发件人的域有效期少于一个月，则该邮件将被丢弃。

```
Drop_Messages_Based_On_SDR_Age: if (sdr-age ("months", <, 1, "")) { drop(); }
```

根据发件人域不可扫描过滤邮件

语法：

```
<msg_filter_name>
if sdr-unscannable (<'domain_exception_list'>)
{<action>}
```

其中：

- 'sdr-unscannable' 是域信誉邮件过滤器规则。

  'domain_exception_list' 是域例外列表的名称。如果不存在域例外列表，它将显示为 ""。

示例

在以下邮件中，如果邮件未通过 SDR 检查，则该邮件将被隔离。

```
Quarantine_Messages_Based_On_Sender_Domain_Unscannable: if (sdr-unscannable (""))
{quarantine("Policy");}
```

邮件过滤器操作

邮件过滤器的目的是对所选邮件执行操作。

操作分为两类：

- 最终操作（例如，传送、删除以及退回）会结束邮件处理，并且不允许通过后续过滤器对邮件做更多处理。
- 非最终操作，允许对邮件做进一步处理。

Note 非最终邮件过滤器操作可以累积。如果邮件与多个过滤器匹配，且每个过滤器都指定了不同的操作，那么这些操作会累积，并一并实施。但是，如果邮件与指定相同操作的多个过滤器匹配，那么前面的操作将被覆盖，只执行最终过滤器操作。

相关主题

- “过滤器操作”摘要表, on page 55
- 操作变量, on page 64
- 匹配内容可视性, on page 66
- 邮件过滤器操作说明和示例, on page 67

“过滤器操作”摘要表

邮件过滤器可以将以下操作应用于邮件，如下表所示：

Table 5: 邮件过滤器操作

操作	语法	说明
修改源主机	alt-src-host	更改发送邮件的源主机名和 IP 接口（虚拟网关地址）。请参阅修改源主机（虚拟网关地址）操作, on page 76。
修改收件人	alt-rcpt-to	更改邮件的收件人。请参阅修改收件人操作, on page 75。
修改邮件主机	alt-mailhost	更改邮件的目标邮件主机。请参阅修改传送主机操作, on page 75。
通知	notify	将此邮件报告给另一个收件人请参阅通知和通知并抄送操作, on page 70。

操作	语法	说明
通知抄送	notify-copy	执行与 notify 相同的操作，但同时会像 bcc-scan 操作一样发送副本。请参阅通知和通知并抄送操作, on page 70。
密件抄送	bcc	将此邮件（邮件副本）匿名发送给另一收件人。请参阅密件抄送操作, on page 72。
密件抄送并扫描	bcc-scan	将邮件匿名发送给另一收件人，并按照处理新邮件的方式通过工作队列处理该邮件。请参阅密件抄送操作, on page 72。
存档	存档	将邮件存档为 mbox 格式的文件。请参阅存档操作, on page 76。
隔离	`quarantine (quarantine_name`	将邮件标记为发送到 *quarantine_name* 隔离区。请参阅隔离和复制操作, on page 74。
副本（隔离）	`duplicate-quarantine (quarantine_name`	将邮件的副本发送到指定隔离区。请参阅隔离和复制操作, on page 74。
删除信头	strip-header	传送前从邮件中删除指定信头。请参阅删除信头操作, on page 77。
插入信头	insert-header	传送前在邮件中插入信头和值对。请参阅插入信头操作 , on page 77。
编辑信头文本	edit-header-text	将指定信头文本替换为过滤条件中指定的文本字符串。请参阅编辑信头文本操作, on page 78。
编辑正文文本	edit-body-text()	从邮件正文删除正则表达式，并将其替换为指定文本。如果您要删除和替换邮件正文中的特定内容（如 URL），可能要使用此过滤器。请参阅编辑正文文本操作, on page 78。
转换 HTML	html-convert()	从邮件正文删除 HTML 标记，保留邮件的纯文本内容。如果您要将邮件中的所有 HTML 文本转换为纯文本，可能要使用此过滤器。HTML 转换操作, on page 79。

操作	语法	说明
分配退回配置文件	bounce-profile	为邮件分配特定退回配置文件。请参阅退回配置文件操作, on page 80。
绕过反垃圾邮件系统	skip-spamcheck	确保思科系统中的反垃圾邮件系统不应用于邮件。请参阅绕过反垃圾邮件系统操作, on page 80。
绕过灰色邮件操作	skip-marketingcheck	绕过针对营销邮件的操作。请参阅绕过灰色邮件操作, on page 80。
	skip-socialcheck	绕过针对社交网络邮件的操作。请参阅绕过灰色邮件操作, on page 80。
	skip-bulkcheck	绕过针对批量邮件的操作。请参阅绕过灰色邮件操作, on page 80。
绕过防病毒系统	skip-viruscheck	确保思科系统中的防病毒系统不应用于邮件。请参阅绕过防病毒系统操作, on page 81。
绕过文件信誉过滤和文件分析	skip-ampcheck	确保文件信誉过滤和文件分析不应用于邮件。请参阅绕过文件信誉过滤和文件分析系统操作, on page 81。
跳过病毒爆发过滤器扫描	skip-vofcheck	确保邮件不通过病毒爆发过滤器扫描处理。请参阅绕过防病毒系统操作, on page 81。
按名称删除附件	drop-attachments-by-name	删除邮件中所有文件名与指定正则表达式匹配的附件。如果存档文件附件（zip、tar）、Microsoft Office 附件（doc、.docx）和邮件附件 (winmail.dat) 包含匹配的文件，则此类附件将被丢弃。请参阅附件扫描邮件过滤器示例, on page 93。
按类型丢弃附件	drop-attachments-by-type	删除邮件中 MIME 类型的所有附件，根据指定 MIME 类型或文件扩展名做出判断。如果存档文件附件 (zip、tar) 包含匹配的文件，也将丢弃这些附件。请参阅附件扫描邮件过滤器示例, on page 93。

操作	语法	说明
按文件类型删除附件	`drop-attachments-by-filetype`	删除与指定的文件“指纹”匹配的所有附件。如果存档文件附件(zip、tar)包含匹配的文件，也将丢弃这些附件。有关详细信息，请参阅附件扫描邮件过滤器示例, on page 93。
按 MIME 类型丢弃附件	`drop-attachments-by-mimetype`	删除邮件中具有指定 MIME 类型的所有附件。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。请参阅附件扫描邮件过滤器示例, on page 93。
根据文件散列列表删除附件	`drop-attachments-by-hash`	丢弃与文件散列列表中的特定文件 SHA-256 值匹配的邮件中的所有邮件附件。请参阅丢弃与文件 SHA-256 过滤器匹配的邮件附件, on page 119和如果附件与文件 SHA-256 过滤器匹配，则丢弃邮件, on page 119。
按大小删除附件	`drop-attachments-by-size`	删除邮件中原始编码等于或大于给定大小（以字节为单位）的所有附件。注意，对于存档或压缩文件，此操作不会检查未压缩的大小，而是检查执行任何编码之前实际附件的大小。请参阅附件扫描邮件过滤器示例, on page 93。
按内容丢弃附件	`drop-attachments-where-contains`	丢弃邮件中包含正则表达式的所有附件。模式是否出现了为阈值指定的最少次数？如果存档文件（zip、rar）包含的任何文件与正则表达式模式匹配，则存档文件将被丢弃。请参阅附件扫描邮件过滤器示例, on page 93。 可选注释用来修改用于替换已丢弃附件的文本。附件页脚会直接附加到邮件。

操作	语法	说明

丢弃带有宏的附件	`drop-macro-enabled-attachments`	丢弃指定文件类型的所有启用宏的附件。
		Note 如果存档或嵌入文件包含宏，则会从邮件中删除父文件。
		语法
		`drop-macro-enabled-attachments ([ ‘file_type-1', 'file_type-2', …,'file_type-n'], “custom_replacement_message” )`
		其中：
		• `File_type` 可以是以下任一受支持的文件类型：
		  • `Adobe 便携式文档格式`
		  • `Microsoft Office 文件`
		  • `OLE 文件类型`
		• **自定义替换**邮件是一个可选邮件，用于在丢弃附件时替换添加到邮件正文底部的系统生成的默认邮件。
		请参阅 宏检测规则, on page 49

按词典匹配删除附件	`drop-attachments-where-dictionary-match`	根据词典术语匹配条目删除附件。如果 MIME 部分中的术语被视为词典术语的附件匹配（且达到用户定义的阈值），则从邮件中删除附件。请参阅附件扫描邮件过滤器示例, on page 93。
添加页脚	`add-footer(`*`footer-name`*`)`	将免责声明文本作为页脚添加到邮件中。有关详细信息，请参阅“文本资源”一章中的“邮件免责声明标记”。
添加页眉	`add-heading(`*`heading-name`*`)`	将免责声明文本作为页眉添加到邮件中。有关详细信息，请参阅“文本资源”一章中的“邮件免责声明标记”。
传送时加密	`encrypt-deferred`	传送时加密意味着，邮件继续进入下一处理环节，并在完成所有处理后进行加密和传送。

操作	语法	说明
传送时进行 S/MIME 签名/加密	`smime-gateway-deferred (“sending_profile”)`	在传送过程中，使用指定发送配置文件对邮件执行 S/MIME 签名或加密。请参阅 传送时 S/MIME 签名或加密操作, on page 69。
S/MIME 签名/加密	`smime-gateway(“sending_profile”)`	使用指定发送配置文件对邮件执行 S/MIME 签名或加密，并传送邮件，跳过任何进一步处理。请参阅S/MIME 签名或加密操作, on page 70。
添加邮件标记	`tag-message(tag-name)`	将自定义术语添加到邮件以与 DLP 策略过滤配合使用。您可以将 DLP 策略配置为仅扫描包含邮件标记的邮件。邮件标记对收件人不可见。请参阅添加邮件标记操作, on page 82和“数据丢失预防”一章。
添加日志条目	`log-entry`	在信息级别将自定义文本添加到文本邮件日志。文本可包含操作变量。日志条目将显示在邮件跟踪中。有关详细信息，请参阅添加日志条目操作, on page 82。
添加 CEF 日志条目	`cef-log-entry("label", "value")`	将自定义文本插入到合并事件日志中。文本可包含操作变量。如果在配置“合并事件日志”(Consolidated Event Logs) 日志订用时，“选定日志字段”(Selected Log Fields) 中包含“自定义日志条目”(Custom Log Entries)，则 CEF 日志条目会出现在“合并事件日志”(Consolidated Event Logs) 中。有关详细信息，请参阅添加 CEF 日志条目操作, on page 82。 **Note** 在您的邮件网关中，通过系统日志推送方法使用整合事件日志时，CEF 日志行的长度限制为 65535 个字符。您的外部 SIEM 解决方案也可能对 CEF 日志文件允许的字符数规定了的限制。请确保根据邮件网关和 SIEM 解决方案中允许的字符数相应地配置要记录的和“合并事件日志”(Consolidated Event Logs) 订用字段中的自定义文本。

操作	语法	说明
根据 URL 信誉将 URL 替换为文本	• `url-reputation-replace` • `url-no-reputation-replace`	根据 URL 的信誉修改 URL 或其行为。 使用单独操作处理信誉服务不提供 URL 得分的情况。 请参阅URL 信誉操作 , on page 83。
根据URL信誉去除URL 中的威胁	• `url-reputation-defang` • `url-no-reputation-defang`	
根据URL信誉，将URL 重定向到思科安全代理	• `url-reputation-proxy-redirect` • `url-no-reputation-proxy-redirect`	
根据 URL 类别将 URL 替换为文本	`url-category-replace`	根据 URL 类别修改 URL 或其行为。 请参阅URL 类别操作 , on page 85。
根据URL类别去除URL 中的威胁	`url-category-defang`	
根据 URL 类别将 URL 重定向到思科安全代理	`url-category-proxy-redirect`	
伪造邮件检测	`fed`	系统会从伪造邮件中去掉“发件人：”信头，并将其替换为“信封发件人”。请参阅伪造邮件检测操作, on page 86。
无操作	`no-op`	未执行任何操作。请参阅无操作, on page 86。
*跳过剩余的邮件过滤器	`skip-filters`	确保邮件不被任何其他邮件过滤器处理，并继续通过邮件管道。请参阅跳过剩余的邮件过滤器操作, on page 68。
*删除邮件	`drop`	删除并删除邮件。请参阅丢弃操作, on page 68。
*退回邮件	`bounce`	将邮件发回给发件人。请参阅退回操作, on page 69。
*加密并立即传送	`encrypt`	使用思科邮件加密对外发邮件加密。请参阅加密操作, on page 69。
* 最终操作		

相关主题

- 附件组, on page 62

附件组

可以在 `attachment-filetype` 和 `drop-attachments-by-filetype rules` 中指定某一种文件类型（如“exe”文件）或公共组的附件。AsyncOS 按下表中列出的组对附件分组。

如果您创建的邮件过滤器使用 `!=`运算符匹配不含特定文件类型附件的邮件，那么如果存在至少一个想要过滤的文件类型的附件，过滤器便会对邮件执行操作。例如，下列过滤器会删除附件类型不是 **`.exe`** 文件类型的所有邮件：

```
exe_check: if (attachment-filetype != "exe") {

drop();

}
```

如果一封邮件包含多个附件，那么如果至少一个附件为 `.exe` 文件，邮件网关便会删除该邮件，即使其他附件不是 .exe 文件。

Table 6: 附件组

附件组名称	扫描的文件类型
文档	• doc • docx • mdb • mpp • ole • pdf • ppt • pptx • rtf • wps • x-wmf • xls • xlsx
可执行程序	• exe • java • msi • pif **Note** 过滤可执行程序组还将扫描 .dll 和 .scr 文件，但不能单独过滤这些文件类型。

附件组名称	扫描的文件类型
压缩	• ace (ACE Archiver compressed file) • arc (SQUASH Compressed archive) • arj (Robert Jung ARJ compressed archive) • binhex • bz (Bzip compressed file) • bz2 (Bzip compressed file) • cab (Microsoft cabinet file) • gzip* (Compressed file - UNIX gzip) • lha (Compressed Archive [LHA/LHARC/LZH]) • rar (Compressed archive • sit (Compressed archive - Macintosh file [Stuffit]) • tar* (Compressed archive) • unix (UNIX compress file) • zip* (Compressed archive - Windows) • zoo (ZOO Compressed Archive File) *这些文件类型可以进行“正文扫描”
文本	• txt • html • xml
图像	• bmp • cur • gif • ico • jpeg • pcx • png • psd • psp • tga • tiff

附件组名称	扫描的文件类型
媒体	• aac • aiff • asf • avi • 闪存 • midi • mov • mp3 • mpeg • ogg • ram • snd • wav • wma • wmv

操作变量

bcc()、bcc-scan()、notify()、notify-copy()、add-footer()、add-heading() 和 insert-headers() 操作具有一些使用特定变量的参数，这些变量在执行操作时可自动替换为原始邮件中的信息。这些特殊变量称为操作变量。邮件网关支持以下操作变量：

Table 7: 消息过滤器操作变量

变量	语法	说明
所有信头	`$AllHeaders`	返回邮件信头。
正文大小	`$BodySize`	返回字节表示的邮件大小。
证书签署人	`$CertificateSigners`	返回来自签名证书 subjectAltName 要素的签署人。有关详细信息，请参阅 $CertificateSigners 操作变量, on page 44。
日期	`$Date`	使用 MM/DD/YYYY 格式返回当前日期。
已丢弃的文件名	`$dropped_filename`	仅返回最近丢弃的文件名。
已丢弃的文件名	`$dropped_filenames`	显示已删除文件的列表（与 $filenames 类似）。
已删除的文件类型	`$dropped_filetypes`	显示已删除文件类型的列表（类似于 $filetypes）。

变量	语法	说明
信封发件人	`$EnvelopeFrom`	返回邮件的信封发件人 (<MAIL FROM>)。
信封收件人	`$EnvelopeRecipients`	返回邮件的所有信封收件人 (<RCPT TO>)。
文件名	`$filenames`	返回邮件附件文件名的逗号分隔列表。
文件大小	`$filesizes`	返回邮件附件文件大小的逗号分隔列表。
文件类型	`$filetypes`	返回邮件附件文件类型的逗号分隔列表。
过滤器名称	`$FilterName`	返回正在处理的过滤器的名称。
GMTimeStamp	`$GMTimeStamp`	以 GMT 时间形式返回邮件消息中“接收时间：”(Received:) 行中的当前时间和日期。
HAT 组名	`$Group`	返回注入邮件时发件人匹配的发件人组的名称。如果发件人组没有名称，则插入字符串“>Unknown<”。
匹配的内容	`$MatchedContent`	返回触发扫描过滤器规则的内容（包括 body-contains 等过滤器规则和内容词典）。
邮件流策略	`$Policy`	返回注入邮件时应用至发件人的 HAT 策略的名称。如果未使用预定义的策略名称，则插入字符串“>Unknown<”。
信头	`$Header['string']`	如果原始邮件中包含匹配的信头，返回引用信头的值。请注意，也可以使用双引号。
主机名	`$Hostname`	返回邮件网关的主机名。
内部邮件 ID	`$MID`	返回内部用来标识邮件的邮件 ID 或“MID”。请勿与 RFC822 的“Message-Id”值（使用 $Header 检索该值）混淆。
接收侦听程序	`$RecvListener`	替换为接收邮件的侦听程序的昵称。
接收接口	`$RecvInt`	返回接收邮件的接口的昵称。
远程 IP 地址	`$RemoteIP`	返回将邮件发送给邮件网关的系统的 IP 地址。
远程主机地址	`$remotehost`	返回向邮件网关发送邮件的系统的主机名。
IP 信誉得分	`$Reputation`	返回发件人的 IP 信誉得分。如果没有信誉得分，会替换为“无”。

变量	语法	说明
主题	`$Subject`	返回邮件的主题。
时间	`$Time`	返回本地时区的当前时间。
时间戳	`$Timestamp`	返回邮件消息“接收时间：”(Received:) 行中本地时区的当前时间和日期。

相关主题

- 非 ASCII 字符集和邮件过滤器操作变量, on page 66

非 ASCII 字符集和邮件过滤器操作变量

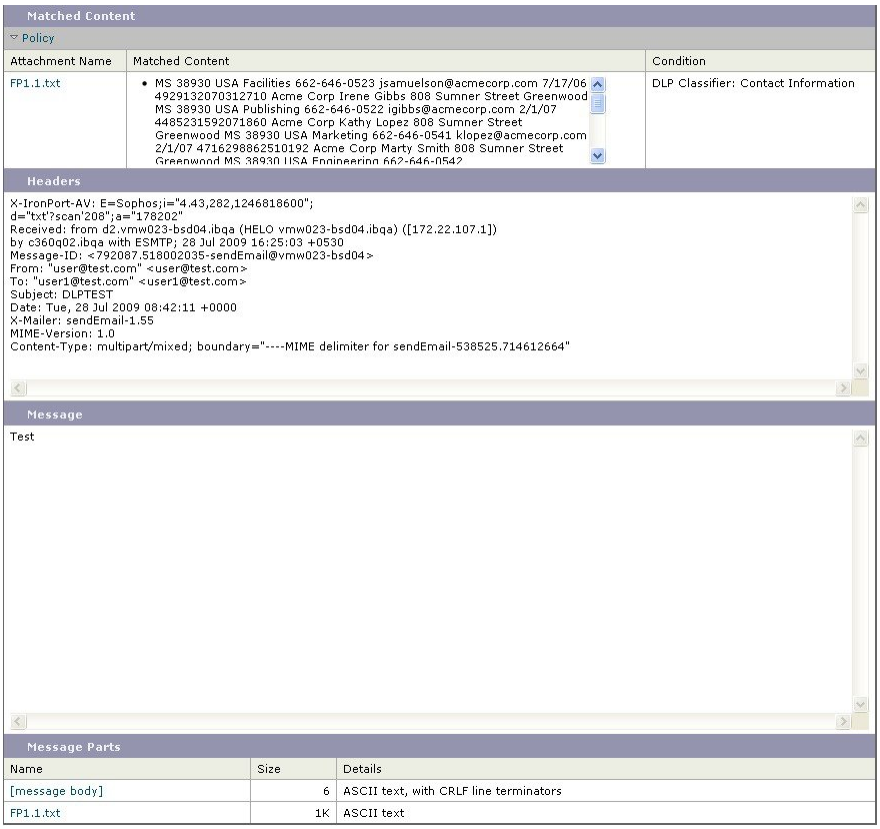
系统支持包含 ISO-2022 样式字符编码（信头值的编码方式）的操作变量扩展，并支持通知中的国际文本。它们将结合生成可作为 UTF-8 可打印引用消息发送的通知。

匹配内容可视性

为匹配附件内容条件、邮件正文或附件条件、邮件正文条件或附件内容条件的邮件配置隔离区操作时，可以查看被隔离邮件中的匹配内容。显示邮件正文时，匹配的内容将以黄色突出显示。另外，还可以使用 $MatchedContent 操作变量在邮件主题中包括匹配的内容。

查看本地隔离区中已触发邮件或内容过滤器规则的邮件时，GUI 可能会显示未实际触发过滤器操作的内容（以及已触发过滤器操作的内容）。GUI 显示应用作查找内容匹配项的准则，但是未必会反映内容匹配项的精确列表。发生此情况是因为 GUI 使用的内容匹配逻辑不如过滤器中所使用的严格。此问题仅适用于邮件正文中的突出显示。列出邮件中每个部分的匹配字符串以及相关过滤器规则的表格是正确的。

Figure 2: 在策略隔离区查看的匹配内容



邮件过滤器操作说明和示例

以下部分介绍各种邮件过滤器操作的实际应用和相关示例。

跳过剩余的邮件过滤器操作

`skip-filters` 操作可确保邮件跳过邮件过滤器的任何进一步处理，并继续通过邮件管道。如果邮件网关执行此类扫描，触发 `skip-filters` 操作的邮件将进行反垃圾邮件扫描和防病毒扫描。`skip-filters` 操作是邮件过滤器的默认最终操作。

下列过滤器首先通知 `customercare@example.com`，随即传送目标为 `boss@admin` 的所有邮件。

```
bossFilter:

if(rcpt-to == 'boss@admin$')

{

notify('customercare@example.com');

skip-filters();

}
```

丢弃操作

`drop` 操作会丢弃邮件，不进行任何传送。邮件不会退回给发件人、不会发送到原定收件人，也不会做任何进一步处理。

下列过滤器首先通知 `george@whitehouse.gov`，之后删除主题以 `SPAM` 开头的所有邮件。

```
spamFilter:

if(subject == '^SPAM.*')

{

notify('george@whitehouse.gov');
```

```
drop();
}
```

退回操作

bounce 操作会将邮件发送回给发件人（信封发件人），不做进一步处理。

下列过滤器退回来自以 @yahoo\\.com 结尾的邮件地址的所有邮件。

```
yahooFilter:
if(mail-from == '@yahoo\\.com$')
{
bounce();
}
```

加密操作

encrypt 操作使用配置的加密配置文件向邮件收件人传送加密邮件。

下列过滤器对主题中包含词语 [encrypt] 的邮件进行加密：

```
Encrypt_Filter:
if ( subject == '\\[encrypt\\]' )
{
encrypt('My_Encryption_Profile');
}
```

Note 必须将网络中的加密设备或托管密钥服务配置为使用此过滤器操作。同时，还必须配置使用此过滤器操作的加密配置文件。

传送时 S/MIME 签名或加密操作

在传送过程中，smime-gateway-deferred 操作使用指定的发送配置文件，对邮件执行 S/MIME 签名或加密。这意味着，邮件继续进入下一处理环节，并在完成所有处理后进行签名，或加密并传送。

在传送过程中，下列过滤器对所有来自特定发件人的外发邮件进行 S/MIME 加密：

```
smime-deferred:if(mail-from == "user@example.com"){smime-gateway-deferred("smime-encrypt");}
```

S/MIME 签名或加密操作

smime-gateway 操作使用指定的发送配置文件对邮件执行 S/MIME 签名或加密，并进行传送，跳过任何后续处理。

下列过滤器对来自特定发件人的所有外发邮件执行 S/MIME 签名，并立即传送这些邮件：

```
smime-deliver-now:if(mail-from == "user@example.com"){smime-gateway("smime-sign");}
```

通知和通知并抄送操作

`notify` 和 `notify-copy` 操作会将邮件的邮件摘要发送到指定邮件地址。`notify-copy` 操作还会发送原始邮件的副本，类似于 bcc-scan 操作。通知摘要包括：

- 邮件传输协议会话中针对邮件的信封发件人和信封收件人（`MAIL FROM` 和 `RCPT TO`）命令内容。
- 邮件的邮件信头。
- 邮件匹配的邮件过滤器的名称。

您可以指定收件人、主题行、源地址和通知模板。下列过滤器选择大小超过 4 MB 的邮件，每发现一个匹配邮件向 `admin@example.com` 发送一封通知邮件，并最终删除邮件：

```
bigFilter:

if(body-size >= 4M)

{

notify('admin@example.com');

drop();

}
```

或

```
bigFilterCopy:

if(body-size >= 4M)

{

notify-copy('admin@example.com');

drop();

}
```

信封收件人参数可以是任何有效的邮件地址（例如，上述示例中的 `admin@example.com`），也可以是指定邮件的所有信封收件人的操作变量 `$EnvelopeRecipients`（请参阅操作变量, on page 64）：

```
bigFilter:

if(body-size >= 4M)

{
```

```
notify('$EnvelopeRecipients');

drop();

}
```

`notify` 操作还支持最多三个额外的可选参数，通过这些参数可指定主题信头、信封发件人和可用于通知邮件的预定义文本资源。这些参数必须按顺序出现，因此，如果要设置信封发件人或指定通知模板，必须提供主题。

主题参数可能包含可替换为原始邮件中数据的操作变量（请参阅操作变量, on page 64）。主题参数默认设置为 `Message Notification`。

信封发件人参数可以是任何有效的邮件地址，也可以是将邮件的退回路径设为原始邮件路径的操作变量 `$EnvelopeFrom`。

通知模板参数是现有通知模板的名称。有关详细信息，请参阅通知, on page 93。

此示例对上一示例进行了扩展，只是将主题改为 `[bigFilter] Message too large`，将退回路径设为原始发件人，并使用“message.too.large”模板：

```
bigFilter:

if (body-size >= 4M)

{

notify('admin@example.com', '[$FilterName] Message too large',

'$EnvelopeFrom', 'message.too.large');

drop();

}
```

您还可以使用 `$MatchedContent` 操作变量通知发件人或管理员已触发内容过滤器。`$MatchedContent` 操作变量可显示触发过滤器的内容。例如，以下过滤器会在邮件包含ABA帐户信息时通知管理员。

```
ABA_filter:

if (body-contains ('*aba')){

notify('admin@example.com','[$MatchedContent]Account Information Displayed');

}
```

相关主题

- 通知模板, on page 71

通知模板

您可以使用“文本资源”(Text Resources) 页面或 `textconfig` CLI 命令将自定义通知模板配置为用于 `notify()` 和 `notify-copy()` 操作的文本资源。如果不创建自定义通知模板，可使用默认模板。默认

模板包括邮件信头，但自定义通知模板默认不包括邮件信头。要在自定义通知中添加邮件信头，请添加 `$AllHeaders` 操作变量。

有关详细信息，请参阅“文本资源”一章。

在下面的示例中，当大型邮件触发下文所示的过滤器时，系统会向预设收件人发送邮件告知邮件过大：

```
bigFilter:

if (body-size >= 4M)

{

notify('$EnvelopeRecipients', '[$FilterName] Message too large',

'$EnvelopeFrom', 'message.too.large');

drop();

}
```

密件抄送操作

`bcc` 操作会将邮件的匿名副本发送给指定收件人。操作有时被称为邮件复制。由于原始邮件中并未提到抄送，且匿名副本决不会成功退回给收件人，邮件的原始发件人和收件人不一定知晓已发送副本。

下列过滤器将 `johnny` 发送至 sue 的每一封邮件密件抄送给 `mom@home.org`：

```
momFilter:

if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))

{

bcc('mom@home.org');

}
```

bcc 操作还支持最多三个额外的可选参数，通过这些参数可指定在抄送邮件上使用的主题信头、信封发件人以及备用邮件主机。这些参数必须按顺序出现，因此，如果要设置信封发件人必须提供主题。

主题参数可能包含可替换为原始邮件中数据的操作变量（请参阅操作变量, on page 64）。默认情况下，这将设置为原始邮件的主题（相当于 `$Subject`）。

信封发件人参数可以是任何有效的邮件地址，也可以是将邮件的退回路径设为原始邮件路径的操作变量 `$EnvelopeFrom`。

此示例将主题设为 `[Bcc] <original subject>`，将退回路径设为 `badbounce@home.org`，扩展了上一示例：

```
momFilter:

if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))
```

```
{
bcc('mom@home.org', '[Bcc] $Subject', 'badbounce@home.org');
}
```

The alt-mailhost is the fourth parameter:

```
momFilterAltM:
if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))
{
bcc('mom@home.org', '[Bcc] $Subject', '$EnvelopeFrom',
'momaltmailserver.example.com');
}
```

Caution `Bcc()`、`notify()` 以及 `bounce()` 过滤器操作会忽视网络中的病毒。密件抄送过滤器操作会创建一封新邮件，也即原始邮件的完整副本。通知过滤器操作会创建一封包含原始邮件信头的新邮件。信头可能包含病毒，尽管很少出现这种情况。退回过滤器操作会创建一封包含原始邮件前 10k 内容的新邮件。在这三种情况下，新邮件将不做防病毒或反垃圾邮件扫描处理。

要发送到多个主机，您可以多次调用 `bcc()` 操作：

```
multiplealthosts:
if (recv-listener == "IncomingMail")
{
insert-header('X-ORIGINAL-IP', '$remote_ip');
bcc ('$EnvelopeRecipients', '$Subject', '$EnvelopeFrom', '10.2.3.4');
bcc ('$EnvelopeRecipients', '$Subject', '$EnvelopeFrom', '10.2.3.5');
bcc ('$EnvelopeRecipients', '$Subject', '$EnvelopeFrom', '10.2.3.6');
}
```

相关主题

- 密件抄送并扫描发送给竞争对手的邮件, on page 113

bcc-scan() 操作

`bcc-scan` 操作的原理与 bcc 操作相似，不同之处在于发送的邮件被视为新邮件，因此会通过整个邮件管道。

```
momFilter:
```

```
if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))

{

bcc-scan('mom@home.org');

}
```

隔离和复制操作

quarantine(‘quarantine_name’)操作将标记出应放入隔离区队列的邮件。有关隔离区的详细信息，请参阅“隔离区”一章。duplicate-quarantine (‘quarantine_name’)操作会立即将邮件的副本发送到指定隔离区，而原始邮件将继续通过邮件管道。隔离区名称区分大小写。

在标记为放入隔离区的同时，邮件继续通过邮件管道的其余部分。当邮件到达管道末尾时，如果此邮件被标记为放入一个或多个隔离区，邮件将加入这些队列。否则，邮件将被传送。请注意，如果邮件没有到达管道末尾，邮件不会被放入隔离区。

相应地，如果邮件过滤器包含 quarantine() 操作，在此之后还有 bounce() 或 drop() 操作，邮件不会被放入隔离区，因为最终操作阻止邮件到达管道末尾。果邮件过滤器包含隔离区操作，但邮件稍后被反垃圾邮件或防病毒扫描或内容过滤器丢弃，也会发生上述情况。skip-filters() 操作会导致邮件跳过任何剩余邮件过滤器，但内容过滤器可能仍然适用。例如，如果邮件过滤器将邮件标记为放入隔离区，并包括 skip-filters() 操作，那么邮件将跳过所有剩余的邮件过滤器，并被隔离，除非邮件管道中的另一个操作导致邮件被丢弃。

在下面的示例中，如果邮件包含“secret_word”词典中的任何词语，邮件将被发送至Policy隔离区。

```
quarantine_codenames:

if (dictionary-match ('secret_words'))

{

quarantine('Policy');

}
```

在下面的示例中， 假定公司制定了丢弃所有 .mp3 文件附件 的正式策略。如果入站邮件包含 .mp3 附件，那么该附件将被剥离，其余信息（原始正文和剩余附件）将发送到原始收件人。一个包含所有附件的原始邮件副本将被隔离（发送到“策略”[Policy]隔离区。）如果 有必要接收被阻止的附件，原始收件人需请求从隔离区释放邮件。

```
strip_all_mp3s:

if (attachment-filename == '(?i)\\.mp3$') {

duplicate-quarantine('Policy');

drop-attachments-by-name('(?i)\\.mp3$');

}
```

修改收件人操作

`alt-rcpt-to` 操作会在传送时将邮件的所有收件人改为指定收件人。

下列过滤器将发送信封收件人地址中包含 `.freelist.com` 的所有邮件，并将邮件的所有收件人更改为 `system-lists@myhost.com`：

```
freelistFilter:

if(rcpt-to == '\\.freelist\\.com$')

{

alt-rcpt-to('system-lists@myhost.com');

}
```

修改传送主机操作

`alt-mailhost` 操作将选定邮件的所有收件人的 IP 地址改为给定的数字 IP 地址或主机名。

Note `alt-mailhost` 操作可防止反垃圾邮件扫描引擎归类为垃圾邮件的邮件被隔离。`alt-mailhost` 操作将覆盖 `quarantine` 操作并将邮件发送到指定的邮件主机。

下列过滤器将所有邮件的收件人地址重定向到主机 example.com。

```
localRedirectFilter:

if(true)

{

alt-mailhost('example.com');

}
```

因此，定向到 `joe@anywhere.com` 的邮件被传送至位于 example.com，且信封收件人地址为 `joe@anywhere.com` 的邮件主机。注意，`smtproutes` 命令指定的所有额外路由信息仍会影响邮件的传送。（请参阅路由本地域的邮件。）

Note `alt-mailhost` 操作不支持指定端口号。因此，请添加 SMTP 路由。

下列过滤器将所有邮件重定向到 `192.168.12.5`：

```
local2Filter:

if(true)

{
```

```
alt-mailhost('192.168.12.5');
}
```

修改源主机（虚拟网关地址）操作

`alt-src-host` 操作会将邮件的源主机改为指定的源。源主机包括邮件来源的 IP 接口或 IP 接口组。如果选择一组 IP 接口，系统会在传送邮件时轮询组中所有作为源接口的 IP 接口。实际上，此操作可以在一个邮件网关上创建多个虚拟网关地址。有关详细信息，请参阅使用 Virtual Gateway™ 技术为所有托管的域配置邮件网关。

IP 接口只能改为系统当前配置的 IP 接口或接口组。下列过滤器使用出站（传送）IP 接口 `outbound2` 为来自 IP 地址为 `1.2.3.4` 的远程主机的所有邮件创建虚拟网关。

```
externalFilter:
if(remote-ip == '1.2.3.4')
{
alt-src-host('outbound2');
}
```

下列过滤器对从 IP 地址为 `1.2.3.4` 的远程主机接收的所有邮件使用 IP 接口组 Group1。

```
groupFilter:
if(remote-ip == '1.2.3.4')
{
alt-src-host('Group1');
}
```

存档操作

`archive` 操作可在邮件网关上将原始邮件（包括所有邮件信头和收件人）保存为 mbox 格式的文件。此操作将使用保存邮件的日志文件名称参数。系统会在您创建过滤器时自动创建使用指定文件名的日志订用，您也可以指定现有的过滤器日志文件。过滤器和过滤器日志文件创建后，可以使用 `filters -> logconfig` 子命令编辑过滤器日志选项。

Note `logconfig` 命令是 `filters` 的子命令。有关如何使用此子命令的完整说明，请参阅使用 CLI 管理邮件过滤器, on page 97。

mbox 格式是标准的 UNIX 邮箱格式，而且有多种实用程序可帮助您更轻松地查看邮件。对于大多数 UNIX 系统，您可以键入“`mail -f` *mbox.filename*”来查看文件。mbox 格式是纯文本，因此可使用简单的文本编辑器来查看邮件的内容。

在下面的示例中，如果信封发件人与 joesmith@yourdomain.com 匹配，则将邮件副本保存至名为 joesmith 的日志：

```
logJoeSmithFilter:

if(mail-from == '^joesmith@yourdomain\\.com$')

{

archive('joesmith');

}
```

删除信头操作

strip-header 操作会检查邮件是否存在特定信头，并从邮件中删除这些行，然后再传送邮件。存在多个信头时，操作会删除所有信头实例（例如“接收时间：”(Received:) 信头）。

在下面的示例中，所有邮件在传送前均被删除信头 X-DeleteMe：

```
stripXDeleteMeFilter:

if (true)

{

strip-header('X-DeleteMe');

}
```

处理信头时，注意信头的当前值包括在处理过程中所做的更改（如使用添加、删除或修改邮件标题的过滤操作做出的更改）。有关详细信息，请参阅邮件信头规则和求值, on page 5。

插入信头操作

insert-header 操作可将新的信头插入到邮件中。AsyncOS 不验证插入的信头是否符合标准；必须确保生成的邮件符合互联网邮件标准。

在下面的示例中，如果在邮件中找不到信头，则插入名为 X-Company 且值设为 My Company Name 的信头：

```
addXCompanyFilter:

if (not header('X-Company'))

{

insert-header('X-Company', 'My Company Name');

}
```

Insert-header() 操作允许在信头文本中使用非 ASCII 字符，但信头名称必须是 ASCII（合规要求）。传输代码采用可打印的引用格式，以最大限度地提高可读性。

Note strip-headers 和 insert-header 操作可以结合使用，重写原始邮件的所有邮件信头。在某些情况下，可以使用多个相同的信头（如 接收时间：(Received:)）；而在某些情况下，多个相同的信头实例可能会困扰 MUA（如多个“主题：”(Subject:)信头）。

处理信头时，注意信头的当前值包括在处理过程中所做的更改（如使用添加、删除或修改邮件标题的过滤操作做出的更改）。有关详细信息，请参阅邮件信头规则和求值, on page 5。

编辑信头文本操作

edit-header-text 操作支持使用正则表达式替换功能重写指定的信头文本。过滤器匹配信头中的正则表达式，并将其替换为指定正则表达式。

例如，邮件包含下列主题信头：

```
Subject: SCAN Marketing Messages
```

下列过滤器删除信头中的“SCAN”文本，同时保留文本“Marketing Messages”：

```
Remove_SCAN: if true

{

edit-header-text (‘Subject’, ‘^SCAN\\s*’,’’);

}
```

过滤器处理邮件后返回下列信头：

```
Subject: Marketing Messages
```

编辑正文文本操作

edit-body-text() 邮件过滤器与 Edit-Header-Text() 过滤器相似，但该过滤器作用于邮件正文，不是其中一个信头。

edit-body-text() 邮件过滤器使用下列语法，其中第一个参数是要搜索的正则表达式，第二个参数是替换文本：

```
Example: if true {

edit-body-text("parameter 1","parameter 2");

}
```

edit-body-text() 邮件过滤器仅作用于邮件正文部分有关判断 MIME 部分为邮件“正文”还是邮件“附件”的详细信息，请参阅邮件正文与邮件附件, on page 5。

以下示例展示 URL 从邮件中删除，并替换为文本“URL REMOVED”：

```
URL_Replaced: if true {
```

```
edit-body-text("(?i)(?:https?|ftp)://[^\\s\">]+", "URL REMOVED");

}
```

以下示例展示社会保险号码从邮件正文删除，并替换为文本“XXX-XX-XXXX”：

```
ssn: if true {

edit-body-text("(?!000)(?:[0-6]\\d{2}|7(?:[0-6]\\d|7[012]))([
-]?)(?!00)\\d\\d\\1(?!0000)\\d{4}",

"XXX-XX-XXXX");

}
```

Note 此时无法在 `edit-body-text()` 过滤器中使用智能标识符。

HTML 转换操作

RFC 2822 定义了邮件的文本格式，但现在文本格式有了一定扩展（如 MIME）以便传输 RFC 2822 邮件中的其他内容。AsyncOS 现在可以使用 `html-convert()` 邮件过滤器通过以下语法将 HTML 转换为纯文本：

```
Convert_HTML_Filter:

if (true)

{

html-convert();

}
```

思科邮件过滤器将判断给定 MIME 部分属于邮件“正文”还是“附件”。`html-convert()` 过滤器仅作用于邮件正文部分。有关邮件正文和附件的详细信息，请参阅邮件正文与邮件附件, on page 5。

`html-convert()` 过滤器会根据文件格式使用不同的方法，将 HTML 从文档中删除。

如果邮件是纯文本 (text/plain)，邮件将原样通过过滤器。如果邮件是简单的 HTML 邮件 (text/html)，所有 HTML 标签将从邮件中删除，所产生的正文将替换 HTML 邮件。邮件中的行没有重新格式化，并且 HTML 不会显示为纯文本。如果邮件的结构是 MIME（采用多部分/备用结构），且同时包含内容相同的 text/plain 部分和 text/html 部分，过滤器将删除邮件的 text/html 部分，保留 text/plain 部分。对于其他 MIME 类型（例如多部分/混合），过滤器将删除 HTML 正文部分的 HTML 标记，并将 HTML 正文重新插入邮件。

如存在邮件过滤器，`html-convert()` 过滤器操作仅将邮件标记为需要处理，但不会立即更改邮件结构。所有处理完成后，对邮件的更改才会生效。这样便于其他过滤器操作处理修改之前的原始邮件正文。

退回配置文件操作

`bounce-profile` 操作为邮件分配预配置的退回配置文件。（请参阅定向退回的邮件。）如果邮件无法发送，则使用通过退回配置文件配置的退回选项。使用此功能将覆盖从侦听程序的配置中分配给邮件的退回配置文件（如果已分配）。

在下面的过滤器示例中，为信头为 `X-Bounce-Profile: fastbounce` 的所有外发邮件分配退回配置文件“fastbounce”：

```
fastbounce:

if (header ('X-Bounce-Profile') == 'fastbounce') {

bounce-profile ('fastbounce');

}
```

绕过反垃圾邮件系统操作

`skip-spamcheck` 操作会指示系统允许邮件绕开系统上配置的任何基于内容的反垃圾邮件过滤。如果未配置基于内容的反垃圾邮件过滤，或如果从未将邮件标记为首先进行垃圾邮件扫描，此操作不会对邮件进行处理。

以下示例允许高 IP 信誉得分的邮件绕过基于内容的反垃圾邮件过滤功能：

```
allowed_list_on_reputation:

if (reputation > 7.5)

{

skip-spamcheck();

}
```

相关主题

- 传入中继如何影响功能
- 避免垃圾邮件过滤器过滤邮件网关生成的邮件

绕过灰色邮件操作

如果您不想在某些邮件上应用灰色邮件操作，可使用下列邮件过滤器操作绕过这类操作：

邮件过滤器操作	说明
`skip-marketingcheck`	绕过针对营销邮件的操作
`skip-socialcheck`	绕过针对社交网络邮件的操作
`skip-bulkcheck`	绕过针对批量邮件的操作

以下示例指定在侦听程序“private_listener”上接收的邮件必须绕过针对社交网络邮件的灰色邮件操作。

```
internal_mail_is_safe:

if (recv-listener == 'private_listener')

{

skip-socialcheck();

}
```

绕过防病毒系统操作

`skip-viruscheck`操作指示系统允许邮件绕过系统上配置的所有病毒防护系统。如果未配置防病毒系统，或如果从未将邮件标记为首先进行病毒扫描，此操作不会对邮件进行处理。

以下示例指定在侦听程序“private_listener”上接收的邮件应绕过反垃圾邮件和防病毒系统。

```
internal_mail_is_safe:

if (recv-listener == 'private_listener')

{

skip-spamcheck();

skip-viruscheck();

}
```

绕过文件信誉过滤和文件分析系统操作

skip-ampcheck 操作指示系统允许邮件绕过系统上配置的文件信誉过滤和文件分析。如果未配置文件信誉过滤和文件分析，或如果从未将邮件标记为首先进行文件信誉过滤和文件分析扫描，此操作不会对邮件进行处理。

以下示例指定包含 PDF 附件的邮件应绕过文件信誉过滤和文件分析。

```
skip_amp_scan:
if (attachment-filetype == 'pdf')
{
skip-ampcheck();
}
```

绕过病毒爆发过滤器扫描操作

`skip-vofcheck`操作指示系统允许邮件绕过病毒爆发过滤器扫描。如果病毒爆发过滤器扫描未启用，此操作不会对邮件进行处理。

以下示例指定在侦听程序“private_listener”上接收的邮件应绕过爆发过滤器扫描。

```
internal_mail_is_safe:
```

```
if (recv-listener == 'private_listener') Outbreak Filters
{
skip-vofcheck();
}
```

添加邮件标记操作

tag-message 操作会在外发邮件中插入自定义术语，以便使用 DLP 策略过滤。您可以将 DLP 策略配置为仅扫描包含邮件标记的邮件。邮件标记对收件人不可见。标签名称可以包含 [a-zA-Z0-9_-.] 字符集中字符的任意组合。.

有关配置 DLP 邮件过滤策略的信息，请参阅“防数据丢失”一章。

以下示例将邮件标记插入主题中包含“[Encrypt]”的邮件。然后，您可以创建 DLP 策略，如果思科邮件加密可用，则该策略将在传送具有此邮件标记的邮件之前对其进行加密。

```
Tag_Message:
if (subject == '^\\[Encrypt\\]')
{
tag-message('Encrypt-And-Deliver');
}
```

添加日志条目操作

log-entry 操作在信息级别向文本邮件日志中插入自定义文本。文本可包含操作变量。您可以使用此操作插入用于调试的文本，以及解释邮件过滤器为何执行某一操作的信息。日志条目也将显示在邮件跟踪中。

以下示例插入了解释邮件因为涉嫌包含公司机密信息而被退回的日志条目：

```
CompanyConfidential:
if (body-contains('Company Confidential'))
{
log-entry('Message may have contained confidential information.');
bounce();
}
```

添加 CEF 日志条目操作

cef-log-entry操作会将自定义文本插入合并事件日志中。文本可包含操作变量。如果在配置“合并事件日志”(Consolidated Event Logs) 日志订用时，“选定日志字段”(Selected Log Fields) 中包含“自

定义日志条目”(Custom Log Entries)，则 CEF 日志条目会出现在“合并事件日志”(Consolidated Event Logs) 中。

以下示例插入一个标签为“confidential”、值为“true”的 CEF 日志条目，该日志条目在合并事件日志中显示如下：`ESACustomLogs={'confidential': ['true']}`

```
CEFLogEntryExample:

if (body-contains('Company Confidential'))

{

cef-log-entry("confidential", "true");
}
```

URL 信誉操作

使用邮件中的 URL 信誉得分修改 URL 或其行为。有关重要详细信息和示例，请参阅防御恶意或不需要的 URL中的修改邮件中的 URL：在过滤器中使用 URL 信誉和 URL 类别操作

这些操作不需要规则。

在 URL 信誉操作中：

- `msg_filter_name` 为邮件过滤器的名称。
- `min_score` 和 `max_score` 是操作应用范围的最小和最大得分。适用范围包括您指定的值。

最小和最大得分必须介于 `-10.0` 和 `10.0` 之间。

- 要在信誉服务不提供得分的情况下指定操作，请使用操作的相应“no - reputation”版本，如以下小节所示。
- `allowedlist` 为已定义 URL 列表的名称（通过 `urllistconfig` 命令定义）。指定允许列表为可选。
- 不输入 `Preserve_signed`，而输入 0 或 1：
  - 1 - 将此操作仅应用于未签名邮件
  - 0 - 将此操作应用于所有邮件

如不指定 `preserve_signed` 值，操作将仅应用于未签名邮件。

相关主题

- 根据 URL 信誉将 URL 替换为文本, on page 83
- 根据 URL 信誉去除 URL 中的威胁, on page 84
- 根据 URL 信誉将 URL 重定向到思科安全代理 , on page 84

根据 URL 信誉将 URL 替换为文本

要在信誉服务提供得分时执行操作，请执行以下操作：

使用 `url-reputation-replace` 操作。

使用 url-reputation-replace 操作时，过滤器的语法为：

```
<msg_filter_name>:
if <condition>
{url-reputation-replace(<min_score>, <max_score>,' <replace_text>' , '< allowedlist>',< Preserve_signed> );}
```

其中，replace_text 是要替换 URL 的文本。

要在信誉服务不提供得分时执行操作，请执行以下操作：

使用 url-no-reputation-replace 操作。

使用 url-no-reputation-replace 操作时，过滤器的语法为：

```
<msg_filter_name>:
if <condition>
{url-no-reputation-replace ('<replace_text>', '<allowedlist>', <Preserve_signed>);}
```

其中，replace_text 是要替换 URL 的文本。

根据 URL 信誉去除 URL 中的威胁

要在信誉服务提供得分时执行操作，请执行以下操作：

使用 url-reputation-defang 操作。

使用 url-reputation-defang 操作时，过滤器的语法为：

```
<msg_filter_name>:
if <condition>
{url-reputation-defang (<min_score>, <max_score>, '<allowedlist>', <Preserve_signed>);}
```

要在信誉服务不提供得分时执行操作，请执行以下操作：

使用 url-no-reputation-defang 操作。

使用 url-no-reputation-defang 操作时，过滤器的语法为：

```
<msg_filter_name>:
if <condition>
{url-no-reputation-defang ('<allowedlist>', <Preserve_signed>);}
```

根据 URL 信誉将 URL 重定向到思科安全代理

要在信誉服务提供得分时执行操作，请执行以下操作：

使用 url-reputation-proxy-redirect 操作。

使用 url-reputation-proxy-redirect 操作时，过滤器的语法为：

```
<msg_filter_name>:
```

```
if <condition>
{url-reputation-proxy-redirect (<min_score>, <max_score>, '<allowedlist>',
<Preserve_signed>);}
```

要在信誉服务不提供得分时执行操作，请执行以下操作：

使用 `url-no-reputation-proxy-redirect` 操作。

使用`url-no-reputation-proxy-redirect` 操作时，过滤器的语法为：

```
<msg_filter_name>:
if <condition>
{url-no-reputation-proxy-redirect ('<allowedlist>', <Preserve_signed>);}
```

URL 类别操作

使用邮件中的 URL 类别修改 URL 或其行为。有关重要详细信息，请参阅防御恶意或不需要的 URL 中的修改邮件中的 URL：在过滤器中使用 URL 信誉和 URL 类别操作

这些操作不需要规则。

在所有 URL 类别操作中：

- msg_filter_name 是邮件过滤器的名称。
- category-name 是URL 类别。使用逗号分隔多个类别。要获得正确的类别名称，请查看内容过滤器中的 URL 类别条件或操作。有关类别的说明和示例，请参阅关于 URL 类别。
- url_allowed_list 为已定义 URL 列表的名称（通过 urllistconfig 命令定义）。
- unsigned-only：输入 0 或 1。
  - 1 - 将此操作仅应用于未签名邮件
  - 0 - 将此操作应用于所有邮件

相关主题

- 根据 URL 类别将 URL 替换为文本 , on page 85
- 基于 URL 类别去除 URL 中的威胁 , on page 86
- 根据 URL 类别将 URL 重定向到思科安全代理 , on page 86

根据 URL 类别将 URL 替换为文本

使用 `url-category-replace` 操作时，过滤器的语法为：

```
<msg_filter_name>:
if <condition>
url-category-replace([ ‘<category-name1>’ ,’ <category-name2>’ ,...,
‘<category-name3>’ ],’ <replacement-text>’ , ’ <url_allowed_list>’ , <unsigned-only>);
```

其中，`replacement-text` 是要替换 URL 的文本。

基于 URL 类别去除 URL 中的威胁

使用 `url-category-defang` 操作时，过滤器的语法为：

```
<msg_filter_name>:

if <condition>

url-category-defang([ ‘<category-name1>’,’ <category-name2>’,..., ‘<category-name3>’],
’ <url_allowed_list>’, <unsigned-only>);
```

根据 URL 类别将 URL 重定向到思科安全代理

使用 `url-category-proxy-redirect` 操作时，过滤器的语法为：

```
<msg_filter_name>:

if <condition>

url-category-proxy-redirect([ ‘<category-name1>’,’ <category-name2>’,...,
‘<category-name3>’], ’ <url_allowed_list>’, <unsigned-only>);
```

无操作

无操作操作执行 no-op 或 no 操作。如果您不想在邮件过滤器使用通知、隔离或丢弃等其他操作，可以使用此操作。例如，如要了解所创建的新邮件过滤器的行为，您可以使用无操作操作。在邮件过滤器可用后，可以使用“邮件过滤器报告”(Message Filters report) 页面监控新邮件过滤器的行为，并根据需要优化过滤器。

以下示例展示如何使用邮件过滤器中的无操作操作。

```
new_filter_test: if header-repeats ('subject', X, 'incoming') {no-op();}
```

伪造邮件检测操作

系统会从伪造邮件中去掉“发件人：”信头，并将其替换为“信封发件人”。

以下邮件过滤器会将邮件中的“发件人：”信头与词典中的术语进行比较，如果内容词典中的某术语的匹配分数大于或等于 70，则邮件过滤器会删除“发件人：”信头并将其替换为信封发件人。

```
FED_CF: if (forged-email-detection("Execs", 70)) { fed("from", ""); }
```

附件扫描

邮件网关使用内容扫描程序来删除邮件中不符合公司策略的附件，同时仍然保留传送原始邮件的能力。

您可以根据附件的特定文件类型、指纹或附件的内容，过滤附件。使用指纹确定附件的确切类型可防止用户将恶意附件扩展名（例如，.exe）重命名为常用的扩展名（例如，.doc），借此绕过附件过滤器。

扫描附件内容时，内容扫描程序将从附件文件中提取数据，搜索正则表达式。它会检查附件文件中的数据和元数据。如果扫描 Excel 或 Word 文档，附件扫描引擎还可以检测以下类型的嵌入式文件：.exe、.dll、.bmp、.tiff、.pcx、.gif、.jpeg、.png 以及 Photoshop 图像。

邮件网关中的内容扫描程序可以对以下存档文件格式执行内容扫描：

- ACE 存档
- ALZ 存档
- Apple 磁盘映像
- ARJ 存档
- bzip2 存档
- EGG 存档
- GNU Zip
- ISO 磁盘映像
- Java 存档
- LZH
- Microsoft Cabinet 存档
- RAR 多部分文件
- RedHat 软件包管理器存档
- Roshal 存档 (RAR)
- Unix AR 存档
- UNIX 压缩存档
- UNIX cpio
- UNIX Tar
- XZ 存档
- Zip 存档
- 7-Zip
- ARC

Note 您可以在 Web 界面中使用**安全服务 (Security Services)** > **扫描行为 (Scan Behavior)** 页面来查看与内容扫描程序相关的文件的详细信息，也可以在 CLI 中使用 contentscannerstatus 命令来查看。这些文件将使用更新服务器自动更新。如果您要手动更新这些文件，请参阅配置扫描行为, on page 119。

相关主题

- 用于扫描附件的邮件过滤器, on page 88
- 图像分析, on page 89
- 配置图像分析扫描引擎, on page 89
- 将邮件过滤器配置为根据图像分析结果执行操作, on page 91
- 通知, on page 93
- 附件扫描邮件过滤器示例, on page 93

用于扫描附件的邮件过滤器

下表描述的邮件过滤器操作是非最终操作。（附件被删除，邮件处理继续。）

可选注释是添加到邮件中的文本，与脚注非常相似，而且可以包含邮件过滤器操作变量（请参阅附件扫描邮件过滤器示例, on page 93）。

Table 8: 用于过滤附件的邮件过滤器操作

操作	语法	说明
按名称删除附件	`drop-attachments-by-name (<regular expression >[, <optional comment >])`	删除邮件中文件名与给定正则表达式匹配的所有附件。如果存档文件附件 (zip、tar) 包含匹配的文件，也将丢弃这些附件。请参阅附件扫描邮件过滤器示例, on page 93。
按类型丢弃附件	`drop-attachments-by-type (<MIME type >[, <optional comment >])`	丢弃邮件中 MIME 类型的所有附件（按给定 MIME 类型或文件扩展名判断）。如果存档文件附件 (zip、tar) 包含匹配的文件，也将丢弃这些附件。
按文件类型丢弃附件	`drop-attachments-by-filetype (<fingerprint name >[, <optional comment >])`	丢弃邮件中匹配给定文件“指纹”的所有附件。如果存档文件附件 (zip、tar) 包含匹配的文件，也将丢弃这些附件。
按 MIME 类型删除附件	`drop-attachments-by-mimetype (<MIME type >[, <optional comment >])`	丢弃邮件中给定 MIME 类型的所有附件。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。
按大小丢弃附件	`drop-attachments-by-size (<number >[, <optional comment >])`	丢弃邮件中按原始编码形式等于或大于指定大小（以字节为单位）的所有附件。请注意，对于存档或压缩文件，此操作不会检查解压缩后的大小，而是附件自身的实际大小。

操作	语法	说明
附件扫描	`drop-attachments-where-contains (<regular expression >[, <optional comment >])`	删除邮件中包含正则表达式的所有附件。如果存档文件（zip、rar）包含的任何文件与正则表达式模式匹配，则存档文件将被丢弃。
按词典匹配删除附件	`drop-attachments-where-dictionary-match(<dictionary name>)`	此过滤器操作将根据词典术语匹配删除附件。如果 MIME 部分中的术语被视为词典术语的附件匹配（且达到用户定义的阈值），则从邮件中删除附件。请参阅附件扫描邮件过滤器示例, on page 93。

图像分析

某些邮件包含可能需要扫描是否包含不当内容的图像。使用图像分析引擎搜索邮件中的不当内容。

图像分析器使用测量图像属性的算法来确定不适当内容的可能性。这些算法可以检测图像中的形状和颜色面板。分析器可以识别图像中的形状类型以及任何肤色相对于图像中其他颜色的百分比，以帮助识别不适当的内容。肤色颜色百分比较高的图像更有可能是不适当的内容。这些算法不会以任何方式进行区分。

图像分析不用于补充或取代您的防病毒和反垃圾邮件扫描引擎。其目的是通过识别邮件中的不当内容促进图像的合理应用。使用图像分析扫描引擎隔离和分析邮件，并检测趋势。

配置邮件网关进行图像分析后，可以使用图像分析过滤器规则处理可疑或不适当的邮件。图像扫描支持扫描以下类型的附加文件：BMP、JPG、TIF、PNG、GIF、TGA 和 PCX。

扫描图像附件时，思科指纹确定文件类型，图像分析器使用算法分析图像内容。如果图像嵌入在另一个文件中，则内容扫描程序会提取该文件。图像分析判定在完整邮件基础上得出判定结果。如果邮件不包括任何图像，邮件的分数为“0”，与“正常”判定对应。因此，不含任何图像的邮件将收到“正常”判定。

配置图像分析扫描引擎

通过 GUI 启用图像分析：

Procedure

步骤 1 依次转到**安全服务 (Security Services) > IronPort 图像分析 (IronPort Image Analysis)**。

步骤 2 点击**启用 (Enable)**。

屏幕随即显示成功消息，并显示判定设置。

图像分析过滤器规则支持用户根据以下判定确定要执行哪些操作：

- **正常**：图像不包含不恰当的内容。图像分析判定在完整邮件基础上得出判定结果，因此，不含任何图像的邮件将得到“正常”判定。
- **可疑**：图像可能包含不恰当的内容。
- **不恰当**：图像包含不恰当的内容。

这些判定是表示图像分析器算法分配用于确定存在不恰当内容的可能性的数值。

建议使用以下值：

- 正常：0 - 49
- 可疑：50 - 74
- 不恰当：75 - 100

- 微调图像分析设置, on page 90

What to do next

可以通过配置灵敏度设置优化图像扫描，帮助减少误报的数量。例如，如果发现收到误报，可以降低灵敏度设置。或者，相反，如果发现图像扫描漏掉不适当的内容，可能需要设置更高的灵敏度。灵敏度设置是介于 0（无灵敏度）和 100（高度敏感）之间的值。建议使用默认灵敏度设置 65。

相关主题

- 微调图像分析设置, on page 90

微调图像分析设置

Procedure

步骤 1 依次转到**安全服务 (Security Services) > IronPort 图像分析 (IronPort Image Analysis)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 配置图像分析敏感度设置。建议使用默认灵敏度设置 65。

步骤 4 配置正常、可疑和不恰当判定的设置。

配置值范围时，请确保值不重叠，且为整数。

步骤 5 或者，将 AsyncOSsyncOS 配置为不扫描未达到最低大小要求的图像（推荐）。默认情况下，为 100 像素的图像配置此设置。扫描小于 100 像素的图像有时可能会产生误报。

您还可以在 CLI 中使用 imageanalysisconfig 命令启用图像分析。

- 查看特定邮件的判定分数, on page 91

What to do next

相关主题

- 查看特定邮件的判定分数, on page 91

查看特定邮件的判定分数

要查看特定邮件的判定分数，您可以查看邮件日志。邮件日志可显示图像名称或文件名、特定邮件附件的得分。此外，日志还将列出文件中的图像是否可以扫描的信息。注意，日志中的信息介绍每个邮件附件的结果，而不是每个图像的结果。例如，如果邮件的压缩文件附件中包含 JPEG 图像，日志条目将包含压缩文件的名称，而不是JPEG图像的名称。此外，如果压缩文件中包括多个图像，日志条目将列出所有图像的最高得分。不可扫描的注释可表明是否有任何图像不可扫描。

日志不介绍得分如何转换为特定判定（正常、可疑或不恰当）的信息。但是，您可以使用邮件日志跟踪特定邮件的传送，因此可根据对邮件执行的操作确定邮件是否包含不当或可疑图像。

例如，下面的邮件日志显示邮件过滤器规则根据图像分析扫描结果丢弃了附件：

```
Thu Apr 3 08:17:56 2009 Debug: MID 154 IronPort Image Analysis: image 'Unscannable.jpg'
is unscannable.

Thu Apr 3 08:17:56 2009 Info: MID 154 IronPort Image Analysis: attachment
'Unscannable.jpg' score 0 unscannable

Thu Apr 3 08:17:56 2009 Info: MID 6 rewritten to MID 7 by
drop-attachments-where-image-verdict filter 'f-001'

Thu Apr 3 08:17:56 2009 Info: Message finished MID 6 done
```

将邮件过滤器配置为根据图像分析结果执行操作

启用图像分析后，必须创建对不同邮件判定执行不同操作的邮件过滤器。例如，您可能希望传送正常判定的邮件，而对判断含有不恰当内容的邮件进行隔离。

Note 思科建议您不要丢弃或退回判定为不恰当或可疑的邮件。相反，请将违规邮件副本发送到隔离区，以便开展后期审查和深度趋势分析。

以下过滤器显示如果内容不当或可疑邮件将被标记：

```
image_analysis: if image-verdict == "inappropriate" {

strip-header("Subject");

insert-header("Subject", "[inappropriate image] $Subject");

}

else {

if image-verdict == "suspect" {
```

```
strip-header("Subject");

insert-header("Subject", "[suspect image] $Subject");
}
}
```

相关主题

- 创建内容过滤器根据图像分析判定删除附件 , on page 92

创建内容过滤器根据图像分析判定删除附件

启用图像分析后，您可以创建内容过滤器根据图像分析判定删除附件，或者您可以将过滤器配置为根据不同的邮件判定执行不同的操作。例如，您可能决定隔离包含不恰当内容的邮件。

要根据图像分析判定删除附件，请执行以下操作：

Procedure

步骤 1 依次点击“邮件策略”(Mail Policies）>“传入内容过滤器”(Incoming Content Filters）。

步骤 2 点击“添加过滤器”(Add Filter)。

步骤 3 输入内容过滤器的名称。

步骤 4 在“操作”(Actions) 下，点击**添加操作 (Add Action)**。

步骤 5 在“按文件信息删除附件”(Strip Attachment by File Info) 下，点击**图像分析判定如下 (Image Analysis Verdict is)**：

步骤 6 从以下图像分析判定中选择：

- 可疑
- 不恰当
- 可疑或不适当
- 不可扫描
- 正常

配置基于图像分析判定的操作

配置基于图像分析判定的操作：

Procedure

步骤 1 依次点击“邮件策略”(Mail Policies）>“传入内容过滤器”(Incoming Content Filters）。

步骤 2 点击“添加过滤器”(Add Filter)。

步骤 3 输入内容过滤器的名称。

步骤 4 在“条件”(Conditions) 下，点击**添加条件 (Add Condition)**。

步骤 5 在“附件文件信息”(Attachment File Info) 下，点击**图像分析判定 (Image Analysis Verdict)**。

步骤 6 选择以下其中一个判定：

- 可疑
- 不恰当
- 可疑或不适当
- 不可扫描
- 正常

步骤 7 点击**添加操作 (Add Action)**。

步骤 8 选择根据图像分析判定对邮件执行的操作。

步骤 9 提交并确认更改。

通知

使用附件过滤器规则时，可使用 GUI 中的“文本资源”(Text Resources) 页面或 `textconfig` CLI 命令配置自定义通知文本作为文本资源。通知模板支持非 ASCII 字符（创建模板时系统会提示选择编码）。

在下面的示例中，先使用 `textconfig` 命令创建可插入通知邮件正文的 `strip.mp3` 通知模板。随后创建附件过滤器规则，这样，当从邮件中删除 .mp3 文件时，系统会向预设收件人发送通知邮件，告知 .mp3 文件已被删除。

```
drop-mp3s:

if (attachment-type == '*/mp3')

{ drop-attachments-by-filetype('Media');

notify ('$EnvelopeRecipients', 'Your mp3 has been removed', '$EnvelopeFrom',

'strip.mp3');

}
```

有关详细信息，请参阅 通知和通知并抄送操作, on page 70。

附件扫描邮件过滤器示例

以下示例展示在附件上执行的操作：

- 插入信头, on page 94
- 按文件类型丢弃附件, on page 94
- 按词典匹配删除附件, on page 96

- 隔离受保护的附件, on page 96
- 检测未受保护的附件, on page 96

插入信头

在这些示例中，AsyncOS 会在附件包含指定内容时插入信头。

在以下示例中，系统对邮件中的所有附件进行关键字扫描。如果所有附件都包含关键字，插入自定义 `X-Header`：

```
attach_disclaim:

if (every-attachment-contains('[dD]isclaimer') ) {

insert-header("X-Example-Approval", "AttachOK");

}
```

在下面的示例中，系统对附件进行二进制数据模式扫描。过滤器使用 `attachment-binary-contains` 过滤器规则搜索表示 PDF 文档已加密的模式。如果二进制数据中 存在模式，则插入自定义信头：

```
match_PDF_Encrypt:

if (attachment-filetype == 'pdf' AND

attachment-binary-contains('/Encrypt')){

strip-header ( ‘Subject’ );

insert-header ( ‘Subject’ , ‘[Encrypted] $Subject’ );

}
```

按文件类型丢弃附件

在以下示例中，系统从邮件中删除“可执行程序”组附件（`.exe`、.dll 和 `.scr`）、在邮件中添加文本，同时列出被删除文件的文件名（使用 `$dropped_filename` 操作变量）。注意，`drop-attachments-by-filetype` 操作将检查附件，并根据文件的指纹删除附件，而不是只根据三个字母的文件扩展名。另外，可以指定单个文件类型（“mpeg”），也可以引用所有文件类型对象（“Media”）：

```
strip_all_exes: if (true) {

drop-attachments-by-filetype ('Executable', “Removed attachment:

$dropped_filename”);

}
```

在下面的示例中，系统从信封发件人不属于域 `example.com` 的邮件中删除同一“可执行程序”组附件（`.exe`、`.dll` 以及 `.scr`）。

```
strip_inbound_exes: if (mail-from != "@example\\.com$") {
drop-attachments-by-filetype ('Executable');
}
```

在以下示例中，将从其信封发件人不在域 example.com 内的邮件中删除文件类型的特定成员（“wmf”）以及附件的同一“可执行文件”组（.exe、.dll 和 .scr）。

```
strip_inbound_exes_and_wmf: if (mail-from != "@example\\.com$") {
drop-attachments-by-filetype ('Executable');
drop-attachments-by-filetype ('x-wmf');
}
```

在以下示例中，系统添加了更多附件名称，对“可执行程序”预定义附件组进行了扩展。（注意，此操作不检查附件的文件类型。）

```
strip_all_dangerous: if (true) {
drop-attachments-by-filetype ('Executable');
drop-attachments-by-name('(?i)\\.(cmd|pif|bat)$');
}
```

drop-attachments-by-name 操作支持非 ASCII 字符。

Note drop-attachments-by-name 操作将根据从 MIME 信头捕获的文件名匹配正则表达式。从 MIME 信头中捕获的文件名可能包含行尾空格。

在下面的示例中，如果附件不是 .exe 可执行程序类型，邮件将被丢弃。但是，如果至少有一个文件类型属于过滤类型的附件，过滤器便会对邮件执行操作。例如，下列过滤器会删除附件类型不是 **.exe** 文件类型的所有邮件：

```
exe_check: if (attachment-filetype != "exe") {
drop();
}
```

如果一封邮件包含多个附件，那么如果至少一个附件为 .exe 文件，邮件网关便会删除该邮件，即使其他附件不是 .exe 文件。

按词典匹配删除附件

`drop-attachments-where-dictionary-match` 操作将根据词典术语匹配删除附件。如果 MIME 部分中的术语被视为词典术语的附件匹配（且达到用户定义的阈值），则从邮件中删除附件。以下示例展示如果在附件中检测到“secret_words”词典中的词语将丢弃附件。注意，匹配的阈值设为一：

```
Data_Loss_Prevention: if (true) {

drop-attachments-where-dictionary-match("secret_words", 1);

}
```

隔离受保护的附件

`attachment-protected` 过滤器测试邮件中的任何附件是否受密码保护。您可以在传入邮件上使用此过滤器，确保附件可以扫描。根据定义，包含一个加密对象和未加密对象的压缩文件将被视为受保护。同样，未设打开密码的 PDF 文件不被视为受保护，即使使用密码限制复制或打印。以下示例展示受保护附件被发送到“策略”(Policy) 隔离区：

```
quarantine_protected:

if attachment-protected

{

quarantine("Policy");

}
```

检测未受保护的附件

`attachment-unprotected` 过滤器测试邮件中的任何附件是否不受密码保护。此邮件过滤器是对 `attachment-protected` 过滤器的补充。您可以在外发邮件上使用此过滤器，检测未受保护的外发邮件。以下示例展示 AsyncOS 在外发侦听程序上检测未受保护的附件，并隔离邮件：

```
quarantine_unprotected:

if attachment-unprotected

{

quarantine("Policy");

}
```

使用邮件过滤器检测邮件附件中的恶意文件

例如，使用以下邮件过滤器规则语法检测被 ETF 引擎归类为恶意的邮件附件中的文件，并对此类邮件执行适当的操作。

语法：

```
Strip_malicious_files: if (file-hash-etf-rule (['etf_source1'], <'file_hash_exception_list'>))

{ file-hash-etf-strip-attachment-action (['etf_source1'], <'file_hash_exception_list>,
 "file stripped from message attachment"); }
```

其中：

- ‘file-hash-etf-rule' 是附件文件信息邮件过滤器规则
- ‘etf_source1' 是用于根据文件散列检测邮件中的恶意文件的 ETF 源。
- 'file_hash_exception_list' 是文件散列例外列表的名称。如果不存在文件散列例外列表，它将显示为 ""。
- 'file-hash-etf-strip-attachment-action' 是要应用于包含恶意文件的邮件的操作名称。

在以下示例中，如果邮件包含 ETF 引擎检测为恶意的邮件附件，则该附件将被删除。

```
Strip_Malicious_Attachment: if (true) {file-hash-etf-strip-attachment-action
(['threat_feed_source'], "", “Malicious message attachment has been stripped from
the message.");}
```

使用 CLI 管理邮件过滤器

您可以使用 CLI 添加、删除、激活和停用、导入和导出邮件过滤器，并设置邮件过滤器的日志记录选项。下表汇总了可用的命令和子命令。下表汇总了可用的命令和子命令。

Table 9: 邮件过滤器子命令

语法	说明
filters	主命令。此命令是交互式的；需要您提供更多信息（例如，new、delete、import）。
new	创建新过滤器。如果没有指定位置，过滤器将追加到当前序列末尾。否则，该过滤器将插入到序列中的特定位置。有关详细信息，请参阅创建新的邮件过滤器, on page 99。
delete	按名称或按序列号删除过滤器。有关详细信息，请参阅删除邮件过滤器, on page 99。
move	重新排列现有过滤器。有关详细信息，请参阅创建新的邮件过滤器, on page 99。
set	将过滤器设置为活动或非活动状态。有关详细信息，请参阅创建新的邮件过滤器, on page 99。
import	将当前的过滤器集合替换为文件中存储的新集合（邮件网关的 /configuration 目录）。有关详细信息，请参阅创建新的邮件过滤器, on page 99。
export	将当前的过滤器集合导出至文件（邮件网关的 /configuration 目录）。有关详细信息，请参阅导出邮件过滤器, on page 103。

语法	说明
`list`	列出一个或多个过滤器的相关信息。有关详细信息，请参阅显示邮件过滤器列表, on page 103。
`detail`	打印指定过滤器的详细信息，包括过滤器规则自身的正文。有关详细信息，请参阅显示邮件过滤器详细信息, on page 104。
`logconfig`	进入过滤器的 logconfig 子菜单，从而可以使用 archive() 过滤器操作编辑日志订用。有关详细信息，请参阅配置过滤器日志订用, on page 104。

Note 必须发出 commit 命令，过滤器才能生效。

参数的三种类型如下：

Table 10: 过滤器管理参数

seqnum	根据过滤器在过滤器列表中的位置表示过滤器的整数。例如，*seqnum* 2 表示列表中的第二个过滤器。
filtname	过滤器的口语化名称。
range	可以使用 *X*-Y 形式的范围表示多个过滤器，其中 X 和 Y 分别是表示范围的第一个和最后一个 *seqnums*。例如，`2-4` 表示第二、第三和第四个位置的过滤器。可以省略 X 或 Y 表示开放列表。例如，`-4` 表示前四个过滤器，`2-` 表示除第一个过滤器之外的所有过滤器。您还可以使用关键字 all 表示过滤器列表中的所有过滤器。

相关主题

- 创建新的邮件过滤器, on page 99
- 删除邮件过滤器, on page 99
- 移动邮件过滤器, on page 99
- 激活和停用邮件过滤器, on page 100
- 导入预策略过滤器, on page 103
- 导出邮件过滤器, on page 103
- 查看非 ASCII 字符集, on page 103
- 显示邮件过滤器列表, on page 103
- 显示邮件过滤器详细信息, on page 104
- 配置过滤器日志订用, on page 104
- 更改邮件编码, on page 105
- 示例邮件过滤器, on page 107

创建新的邮件过滤器

```
new [seqnum|filtname|last]
```

指定新过滤器的插入位置。如果省略位置或提供关键字 last，输入的过滤器将追加到过滤器列表末尾。序列号之间不允许有间隔；不允许输入不在当前列表范围内的*seqnum*。如果输入未知的*filtname*，系统将提示您输入有效的 *filtname*、*seqnum* 或 last。

输入过滤器后，可以手动输入过滤器脚本。完成输入后，在脚本行中输入句点 (.) 可自行终止输入。

以下条件可能会导致错误：

- 序列号不在当前序列号范围内。
- 过滤器的 *filtname* 不唯一。
- 过滤器的 *filtname* 为保留字。
- 过滤器存在语法错误。
- 过滤器具有引用不存在的系统资源（如接口）的操作。

删除邮件过滤器

```
delete [seqnum|filtname|range]
```

删除标识的过滤器。

以下条件可能会导致错误：

- 不存在使用指定名称的过滤器。
- 不存在使用指定序列号的过滤器。

移动邮件过滤器

```
move [seqnum|filtname|rangeseqnum|last]
```

将第一个参数标识的过滤器移动到第二个参数标识的位置。如果第二个参数是关键字 last，过滤器将移至过滤器列表的末尾。如果要移动多个过滤器，它们的相对顺序保持不变。

以下条件可能会导致错误：

- 不存在使用指定名称的过滤器。
- 不存在使用指定序列号的过滤器。
- 序列号不在当前序列号范围内。
- 移动不会导致序列发生变化。

激活和停用邮件过滤器

指定邮件过滤器的状态有活动和非活动，以及有效和无效之分。仅当邮件过滤器处于活动且有效状态时，才能处理邮件。可以使用 CLI 将现有过滤器从活动状态改为非活动状态（以及改回原来状态）。如果过滤器引用的侦听程序或接口不存在（或已被删除），过滤器无效。

Note 您可以根据过滤器的语法判断过滤器是否处于非活动状态；AsyncOS 会将不活动过滤器的过滤器名称后面的冒号改为感叹号。如果在输入或导入过滤器时使用此语法，AsyncOS 会将过滤器标记为非活动状态。

例如，输入以下名为“filterstatus”的良性过滤器。然后使用 `filter -> set` 子命令将其设为非活动状态。请注意，显示该过滤器的详细信息时，冒号已改为感叹号（并已在下文示例中用粗体表示）。

```
mail3.example.com> filters

Choose the operation you want to perform:

- NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new

Enter filter script. Enter '.' on its own line to end.

filterstatus: if true{skip-filters();}

.

1 filters added.

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.

[]> list

Num Active Valid Name
```

```
1 Y Y filterstatus

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.

[]> set

Enter the filter name, number, or range:

[all]> all

Enter the attribute to set:

[active]> inactive

1 filters updated.

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.

[]> detail

Enter the filter name, number, or range:

[]> all
```

```
Num Active Valid Name
1 N Y filterstatus
filterstatus! if (true) {
skip-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.
[]>
```

相关主题

- 激活或停用邮件过滤器, on page 102

激活或停用邮件过滤器

`set [seqnum|filtname|range] active|inactive`

将标识的过滤器设为给定状态。有效的状态包括：

- 活动：将选定过滤器的状态设为活动。
- 非活动：将选定过滤器的状态设为非活动。

以下条件可能会导致错误：

- 不存在使用指定 *filtname* 的过滤器。
- 不存在使用指定序列号的过滤器。

Note 您可以根据语法判断过滤器是否处于非活动状态；标签（过滤器的名称）后面的冒号改为感叹号 (!)。从 CLI 手动输入或导入的包含此语法的过滤器将自动被标记为非活动。例如，系统将显示 mailfrompm!，不显示 mailfrompm:。

导入预策略过滤器

`import filename`

包含要处理的过滤器的文件的名称。如果通过 `interfaceconfig` 命令启用了对接口的 FTP/SCP 访问，则该文件必须处于设备上的 FTP/SCP 根目录的配置目录中。系统将对文件进行解析，并报告所有错误。导入的过滤器将替换当前过滤器集合中的所有过滤器。有关详细信息，请参阅FTP、SSH 和 SCP 访问。考虑导出当前过滤器列表（请参阅导出邮件过滤器, on page 103），然后在导入前编辑该文件。

导入邮件过滤器时，系统会提示您选择使用的编码。

以下条件可能会导致错误：

- 文件不存在。
- 过滤器的名称不唯一。
- 过滤器的 *filtname* 为保留字。
- 过滤器存在语法错误。
- 过滤器具有引用不存在的系统资源（如接口）的操作。

导出邮件过滤器

`export filename[seqnum|filtname|range]`

将现有过滤器集合的格式化版本输入到文件中（位于邮件网关 FTP/SCP 根目录的配置目录）。有关详细信息，请参阅FTP、SSH 和 SCP 访问。

导出邮件过滤器时，系统会提示您选择使用的编码。

以下条件可能会导致错误：

- 不存在使用指定名称的过滤器。
- 不存在使用指定序列号的过滤器。

查看非 ASCII 字符集

系统将使用 UTF-8 编码在 CLI 中显示包含非 ASCII 字符的过滤器。如果您的终端/显示器不支持 UTF-8，则无法读取过滤器。

管理过滤器中非 ASCII 字符的最佳方法是在文本文件中编辑过滤器，然后将该文本文件导入（参阅导入预策略过滤器, on page 103）邮件网关。

显示邮件过滤器列表

`list [seqnum|filtname|range]`

在表格中显示所标识过滤器的汇总信息，不打印过滤器正文。显示的信息包括：

- 过滤器名称
- 过滤器序列号
- 过滤器的活动/非活动状态

- 过滤器的有效/无效状态

以下条件可能会导致错误：

- 范围格式无效。

显示邮件过滤器详细信息

`detail [seqnum|filtname|range]`

提供所标识过滤器的完整信息，包括过滤器正文和任何其他状态信息。

配置过滤器日志订用

`logconfig`

输入相应的子菜单，为 `archive()` 操作生成的邮箱文件配置过滤器日志选项。这些选项与常规 `logconfig` 命令使用的选项非常相似，但日志只能通过添加或删除引用日志的过滤器来创建或删除。

过滤器日志订用具有以下默认值，可使用 logconfig 子命令进行修改：

- 检索方法 - FTP 轮询
- 文件大小 - 10MB
- 最大文件数 - 10

有关详细信息，请参阅“日志记录”一章。

```
mail3.example.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.
[]> logconfig
Currently configured logs:
1. "joesmith" Type: "Filter Logs" Retrieval: FTP Poll
```

```
Choose the operation you want to perform:

- EDIT - Modify a log setting.


[]> edit

Enter the number of the log you wish to edit.

[]> 1

Choose the method to retrieve the logs.

1. FTP Poll

2. FTP Push

3. SCP Push

[1]> 1

Please enter the filename for the log:

[joesmith.mbox]>

Please enter the maximum file size:

[10485760]>

Please enter the maximum number of files:

[10]>

Currently configured logs:

1. "joesmith" Type: "Filter Logs" Retrieval: FTP Poll

Enter "EDIT" to modify or press Enter to go back.

[]>
```

更改邮件编码

您可以使用 `localeconfig` 命令设置 AsyncOS 在邮件处理过程中修改邮件标题和页脚编码的行为。

```
example.com> localeconfig

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Try both body and footer or heading
encodings
Behavior when decoding errors found: Disclaimer is displayed as inline content and the
message body is added as an attachment.

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[]> setup

If a header is modified, encode the new header in the same encoding as the message body?
(Some MUAs incorrectly handle headers encoded in a different encoding than the body.
However, encoding a modified header in the same encoding as the message body may cause
```

```
certain
characters in the modified header to be lost.) [Y]>

If a non-ASCII header is not properly tagged with a character set and is being used or
modified,
impose the encoding of the body on the header during processing and final representation
of the message?
(Many MUAs create non-RFC-compliant headers that are then handled in an undefined way.
Some MUAs handle headers encoded in character sets that differ from that of the main body
in an incorrect way.
Imposing the encoding of the body on the header may encode the header more precisely.
This will be used to interpret the content of headers for processing, it will not modify
or rewrite the
header unless that is done explicitly as part of the processing.) [Y]>

Disclaimers (as either footers or headings) are added in-line with the message body whenever
 possible.
However, if the disclaimer is encoded differently than the message body, and if imposing a
 single encoding
will cause loss of characters, it will be added as an attachment. The system will always
try to use the
message body's encoding for the disclaimer. If that fails, the system can try to edit the
message body to
use an encoding that is compatible with the message body as well as the disclaimer. Should
 the system try to
re-encode the message body in such a case? [Y]>

If the disclaimer that is added to the footer or header of the message generates an error
when decoding the message body,
it is added at the top of the message body. This prevents you to rewrite a new message
content that must merge with
the original message content and the header/footer-stamp. The disclaimer is now added as
an additional MIME part
that displays only the header disclaimer as an inline content, and the rest of the message
 content is split into
separate email attachments. Should the system try to ignore such errors when decoding the
message body? [N]>

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Try both body and footer or heading
encodings
Behavior when decoding errors found: Disclaimer is displayed as inline content and the
message body
is added as an attachment.

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[]>
```

第一个提示符判断，是否应在邮件信头更改（例如，通过过滤器更改）后修改邮件信头的编码，以匹配邮件正文。

第二个提示符控制信头未使用正确的字符集标记时，邮件网关是否应对邮件信头应用邮件正文的编码。

第三个提示符用于配置免责声明标记（和多编码）在邮件正文中的应用。有关详细信息，请参阅“文本资源”一章中的“免责声明标记和多编码”部分。

第四个提示用于配置免责声明标记的行为（如果系统在邮件正文解码期间生成了错误）。如果选择“是”(Yes)，则系统将忽略解码错误并标记免责声明。如果选择“否”(No)，则免责声明文本将作为附件添加到邮件中。

示例邮件过滤器

在下面的示例中，使用 filter 命令创建了三个新过滤器：

- 第一个过滤器名为 **big_messages**。它使用 body-size 规则丢弃大于 10 MB 的邮件。
- 第二个过滤器名为 **no_mp3s**。它使用 attachment-filename 规则删除附件文件扩展名为 .mp3 的邮件。
- 第三个过滤器名为 **mailfrompm**。它使用 mail-from 规则检查所有来自 postmaster@example.com 的邮件，并密件抄送至 administrator@example.com。

使用 filter -> list 子命令，系统会列出过滤器以确认其处于活动状态并有效，然后使用 move 子命令切换第一个和最后一个过滤器的位置。最后，确定更改，以便过滤器生效。

```
mail3.example.com> filters

Choose the operation you want to perform:

- NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new

Enter filter script. Enter '.' on its own line to end.

big_messages:

if (body-size >= 10M) {

drop();

}

.

1 filters added.

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.

[]> new
```

```
Enter filter script. Enter '.' on its own line to end.
no_mp3s:
if (attachment-filename == '(?i)\\.mp3$') {
drop();
}
.
1 filters added.
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new
Enter filter script. Enter '.' on its own line to end.
mailfrompm:
if (mail-from == "^postmaster$")
{ bcc ("administrator@example.com");}
.
1 filters added.
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.
[]> list
Num Active Valid Name
1 Y Y big_messages
2 Y Y no_mp3s
3 Y Y mailfrompm
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.
[]> move
Enter the filter name, number, or range to move:
[]> 1
Enter the target filter position number or name:
[]> last
1 filters moved.
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.
[]> list
Num Active Valid Name
1 Y Y no_mp3s
2 Y Y mailfrompm
3 Y Y big_messages
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.
[]> move
Enter the filter name, number, or range to move:
[]> 2
Enter the target filter position number or name:
[]> 1
1 filters moved.
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.

[]> list
Num Active Valid Name
1 Y Y mailfrompm
2 Y Y no_mp3s
3 Y Y big_messages
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.
[]>
mail3.example.com> commit
Please enter some comments describing your changes:
[]> entered and enabled 3 filters: no_mp3s, mailfrompm, big_messages
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

邮件过滤器示例

本节介绍一些真实的过滤器示例及其相关的简要说明。

相关主题

- 开放中继防御过滤器, on page 112
- 策略实施过滤器, on page 112
- 路由和域欺骗, on page 116
- 丢弃与文件 SHA-256 过滤器匹配的邮件附件, on page 119
- 如果附件与文件 SHA-256 过滤器匹配，则丢弃邮件, on page 119

开放中继防御过滤器

此过滤器将退回邮件地址中使用 %、多余 @ 以及 ! 字符的邮件：

- `user%otherdomain@validdomain`
- `user@otherdomain@validdomain:`
- `domain!user@validdomain`

```
sourceRouted:

if (rcpt-to == "(%|@|!)(.*)@") {

bounce();

}
```

邮件网关不易受到通常利用传统 Sendmail/Qmail 系统的第三方中继黑客的攻击。由于很多此类符号（如 %）可以是完整合法邮件地址的一部分，邮件网关将这些地址视为有效地址，并将其与配置的收件人列表进行对比，然后传递到下一个内部服务器。邮件网关不会将这些邮件传送到外部。

这些过滤器的目的是，保护可能将开源 MTA 错误配置为允许中继这类邮件的用户。

Note 您还可以配置处理此类地址的侦听程序。有关详细信息，请参阅通过使用 Web 界面创建侦听程序侦听连接请求。

策略实施过滤器

- 基于主题发送通知过滤器, on page 113
- 密件抄送并扫描发送给竞争对手的邮件, on page 113
- 阻止特定用户过滤器, on page 113
- 存档和丢弃邮件过滤器, on page 114

基于主题发送通知过滤器

此过滤器基于主题中是否包含指定词语决定是否发送通知：

```
search_for_sensitive_content:

if (Subject == "(?i)plaintiff|lawsuit|judge" ) {

notify ("admin@company.com");

}
```

密件抄送并扫描发送给竞争对手的邮件

此过滤器会对发送给竞争对手的邮件进行扫描和密件抄送。注意，您可以使用词典和 `header-dictionary-match()` 规则指定更灵活的竞争对手列表（请参阅词典规则, on page 37）：

```
competitorFilter:
if (rcpt-to == '@competitor1.com|@competitor2.com') {
bcc-scan('legal@example.com');
}
```

阻止特定用户过滤器

使用此过滤器可以阻止来自特定地址的邮件：

```
block_harrasing_user:
if (mail-from == "ex-employee@hotmail\\.com") {
notify ("admin@company.com");
drop ();
}
```

存档和丢弃邮件过滤器

仅记录和删除包含匹配文件类型的邮件：

```
drop_attachments:
if (mail-from != "user@example.com") AND (attachment-filename ==
'(?i)\\.(asp|bas|bat|cmd|cpl|exe|hta|ins|isp|js)$')
{
archive("Drop_Attachments");
insert-header("X-Filter", "Dropped by: $FilterName MID: $MID");
drop-attachments-by-name("\\.(asp|bas|bat|cmd|cpl|exe|hta|ins|isp|js)$");
}
```

超大“收件人：”信头过滤器

查找“To”信头超大的邮件。

使用 `archive()` 行验证操作是否恰当，同时启用或禁用 drop() 增强安全：

```
toTooBig:
if(header('To') == "^.{500,}") {
archive('tooTooBigdropped');
drop();
}
```

空白“发件人：”过滤器

识别空白“From:”信头

此过滤器可以减少各种形式的“from”地址空白的邮件：

```
blank_mail_from_stop:
if (recv-listener == "InboundMail" AND header("From") == "^$|<\\s*>") {
drop ();
}
```

如果您还希望删除空白信封发件人的邮件，请使用以下过滤器：

```
blank_mail_from_stop:
if (recv-listener == "InboundMail" AND (mail-from == "^$|<\\s*>" OR header ("From") ==
```

```
"^$|<\\s*>"))

{

drop ();
}
```

IP 信誉过滤器

IP 信誉过滤器：

```
note_bad_reps:
if (reputation < -2) {
strip-header ('Subject');

insert-header ('Subject', '***BadRep $Reputation *** $Subject');
}
```

更改 IP 信誉过滤器

更改某些域的IP 信誉得分阈值：

```
mod_ipr:
if ( (rcpt-count == 1) AND (rcpt-to == "@domain\\.com$") AND (reputation < -2) ) {
drop ();
}
```

文件名 Regex 过滤器

此过滤器指定邮件正文的大小范围，并查找匹配正则表达式的附件（与“eadme.zip”、“readme.exe”、“attach.exe”等文件匹配）：

```
filename_filter:
if ((body-size >= 9k) AND (body-size <= 20k)) {
if (body-contains ("(?i)(readme|attach|information)\\.(zip|exe)$")) {
drop ();

}

}
```

显示信头中 IP 信誉得分过滤器

务必记录信头（请参阅“日志记录”一章），以便在邮件日志中显示信头：

```
Check_ipr:

if (true) {

insert-header('X-ipr', '$Reputation');

}
```

在信头中插入策略过滤器

显示接受连接的邮件流策略：

```
Policy_Tracker:

if (true) {

insert-header ('X-HAT', 'Sender Group $Group, Policy $Policy applied.');

}
```

收件人过多退回过滤器

退回所有来自 2 个以上唯一域、收件人超过 50 个的出站邮件：

```
bounce_high_rcpt_count:

if ( (rcpt-count > 49) AND (rcpt-to != "@example\\.com$") ) {

bounce-profile ("too_many_rcpt_bounce"); bounce ();

}
```

路由和域欺骗

使用虚拟网关过滤器

使用虚拟网关对流量分段。假定系统上有两个接口，分别是“public1”和“public2”，默认传送接口为“public1”。这会迫使所有出站流量通过第二个接口；因为退回和其他类似邮件不通过过滤器，而是通过 public1 传送：

```
virtual_gateways:

if (recv-listener == "OutboundMail") {

alt-src-host ("public2");

}
```

传送和接收使用同一侦听程序过滤器

使用同一侦听程序发送和接收邮件。此过滤器可将公共侦听程序“listener1”上收到的所有邮件发送到接口“listener1”（需要为配置的每个公共侦听程序设置唯一过滤器）：

```
same_listener:

if (recv-inj == 'listener1') {

alt-src-host('listener1');

}
```

单个侦听程序过滤器

将过滤器设置为应用到单个侦听程序。例如，指定执行邮件过滤处理的特定侦听程序，而不在系统范围内执行处理。

```
textfilter-new:

if (recv-inj == 'inbound' and body-contains("some spammy message")) {

alt-rcpt-to ("spam.quarantine@spam.example.com");

}
```

删除欺骗域过滤器（单个侦听程序）

删除带有欺骗域的邮件（假装来自内部地址；与单个侦听程序结合使用）。下面的 IP 地址表示 mycompany.com 的虚构域：

```
DomainSpoofed:

if (mail-from == "mycompany\\.com$") {

if ((remote-ip != "1.2.") AND (remote-ip != "3.4.")) {

drop();

}

}
```

丢弃欺骗域过滤器（多个侦听程序）

和上文相似，但与多个侦听程序结合使用：

```
domain_spoof:

if ((recv-listener == "Inbound") and (mail-from == "@mycompany\\.com")) {

archive('domain_spoof');
```

```
drop ();

}
```

其他丢弃欺骗域过滤器

摘要: 反域伪装过滤器：

```
reject_domain_spoof:

if (recv-listener == "MailListener") {

insert-header("X-Group", "$Group");

if ((mail-from == "@test\\.mycompany\\.com") AND (header("X-Group") != "RELAYLIST")) {

notify("me@here.com");

drop();

strip-header("X-Group");

}
```

检测循环过滤器

此过滤器用于检测、终止和确定导致邮件循环的因素。此过滤器可以帮助确定Exchange服务器或其他位置的配置问题。

```
External_Loop_Count:

if (header("X-ExtLoop1")) {


if (header("X-ExtLoopCount2")) {

if (header("X-ExtLoopCount3")) {

if (header("X-ExtLoopCount4")) {

if (header("X-ExtLoopCount5")) {

if (header("X-ExtLoopCount6")) {

if (header("X-ExtLoopCount7")) {

if (header("X-ExtLoopCount8")) {

if (header("X-ExtLoopCount9")) {

notify ('joe@example.com');

drop();

}

else {insert-header("X-ExtLoopCount9", "from
$RemoteIP");}}
```

```
else {insert-header("X-ExtLoopCount8", "from $RemoteIP");}}
else {insert-header("X-ExtLoopCount7", "from $RemoteIP");}}
else {insert-header("X-ExtLoopCount6", "from $RemoteIP");}}
else {insert-header("X-ExtLoopCount5", "from $RemoteIP");}}
else {insert-header("X-ExtLoopCount4", "from $RemoteIP");}}
else {insert-header("X-ExtLoopCount3", "from $RemoteIP");}}
else {insert-header("X-ExtLoopCount2", "from $RemoteIP");}}
else {insert-header("X-ExtLoop1", "1");
}
```

Note 默认情况下，AsyncOS 会自动检测邮件循环并在经过 100 次循环后删除邮件。

丢弃与文件 SHA-256 过滤器匹配的邮件附件

使用此过滤器以丢弃与文件散列列表中的特定文件 SHA-256 值匹配的邮件中的所有邮件附件

```
File_Hash_Message_Filter: if (true)
{ drop-attachments-by-hash("SHA-256_hash_list"); }
```

如果附件与文件 SHA-256 过滤器匹配，则丢弃邮件

如果邮件附件与文件散列列表中的特定文件 SHA-256 值匹配，则使用此过滤器丢弃所有邮件。

```
File_Hash_Message_Filter: if (attachment-hashlist-match("SHA-256_hash_list"))
{ drop(); }
```

配置扫描行为

可以通过配置扫描参数控制正文和附件扫描的行为，例如，在扫描期间跳过的附件类型。使用“扫描行为”(Scan Behavior) 页面或 `scanconfig` 命令可配置这些参数。扫描行为设置为全局设置，意味着它们会影响所有扫描的行为。

Note 如果要扫描包含在 zip 或压缩文件中的 MIME 类型，必须在扫描列表中添加“compressed”或“zip”或“application/zip”列表。

Procedure

步骤 1 点击**安全服务 (Security Services)** > **扫描行为 (Scan Behavior)**。

步骤 2 定义附件类型映射。执行以下操作之一：

- 添加新的附件类型映射。点击**添加映射 (Add Mapping)**。
- 使用配置文件导入附件类型映射列表。点击**导入列表 (Import List)**，并从配置目录导入所需的配置文件。

  Note 要执行此步骤，配置文件必须位于邮件网关的配置目录中。请参阅管理配置文件。

- 点击**编辑 (Edit)** 修改现有的附件类型映射。

步骤 3 配置全局设置。执行以下操作：

a) 在“全局设置 (Global Settings)”下，点击**编辑全局设置 (Edit Global Settings)**。

b) 编辑必填字段：

字段	说明
针对上表中 MIME 类型/指纹的附件的操作	选择扫描还是跳过附件类型映射中定义的附件类型。
要扫描的最大附件递归深度	指定附件扫描的最大递归深度。
附件扫描的最大大小	指定附件扫描的最大大小。
附件元数据扫描	指定扫描还是跳过附件的元数据。
附件扫描超时	指定扫描超时间隔。
如果出于任何原因不执行扫描，则假设附件匹配模式	指定是否将不经扫描的附件视为匹配搜索模式。
当邮件无法解构以移除指定附件时的操作	指定当邮件无法解构以删除指定附件时要执行的操作。
当内容或邮件过滤器发生错误时绕过所有过滤器	指定是否在内容或邮件过滤器发生错误时绕过所有过滤器。
未指定编码时所应使用的编码	指定在未指定编码时所应使用的编码。
将秘文签署的邮件转换为明文签署的邮件（S/MIME 解包）	指定是否将秘文签署的邮件转换为明文签署的邮件（S/MIME 解包）。
安全打印设置	

字段	说明
最大文件大小	输入安全打印附件的最大附件大小。 **Note** 如果“最大文件大小”值超过为邮件网关上的爆发过滤器配置的“扫描的最大邮件大小”值，则邮件管道中的爆发过滤器不会对邮件和邮件附件进行扫描。
最大页数	输入您要在邮件附件中安全打印的最大页数。
文档质量	选择**使用默认值 (70) (Use Default Value [70])** 选项，将建议的图像质量值用于安全打印的附件。 **Note** 您还可以选择**输入自定义值 (Enter Custom Value)** 选项，并为安全打印的附件输入自定义图像数量值。
文件类型选择	从相应的文件组（例如，“Microsoft 文档”）中选择安全打印邮件附件所需的文件类型。
水印	选择**已启用 (Enabled)** 选项可在安全打印的附件中添加水印。 **Note** 您可以在**输入自定义文本：(Enter Custom Text:)** 字段中为水印输入自定义文本。
封面页	选择**已启用 (Enabled)** 选项可在安全打印的附件中添加封面。 **Note** 您可以在**输入自定义文本：(Enter Custom Text:)** 字段中为封面输入自定义文本。
有关详细信息，请参阅如何将邮件网关配置为安全的印邮件附件。	
受密码保护的附件扫描	

字段	说明
启用受密码保护的附件扫描：	选择**入站邮件流量 (Inbound Mail Traffic)** 或**出站邮件流量 (Outbound Mail Traffic)** 下的**已启用 (Enabled)** 选项，以便允许邮件网关中的内容扫描程序扫描传入或传出邮件中受密码保护的附件的内容。 此功能支持以下语言 - 英语、意大利语、葡萄牙语、西班牙语、德语、法语、日语和韩文。 **Note** 假设您的邮件网关中启用了 DLP 扫描引擎。在这种情况下，如果密码提取成功，则 DLP 引擎会根据配置的 DLP 策略来扫描受密码保护的附件内容。 **Important** • 假设内容扫描程序可以从邮件正文中提取密码并成功扫描附件内容。在这种情况下，如果您的邮件网关中配置了密码和附件，则系统会将密码和附件发送到 Cisco Secure Malware Analytics (Threat Grid)，同时建议使用该文件进行文件分析。 • 内容扫描程序会尽力从邮件正文中提取密码。扫描完成后，提取的密码不会存储在邮件网关中。

字段	说明
供分析的可能的用户定义密码：	选择**已启用 (Enabled)** 选项以创建用户定义的密码，用于保护传入或传出邮件中受密码保护的附件。 如果要添加多个用户定义的密码，请点击**添加行 (Add Row)**。 **说明：** • 您可以创建最多 128 个字符的用户定义密码。。 • 最多可以创建五个用户定义的密码。 • 您可以通过在与所需优先级对应的**密码 (Password)** 字段中输入所需的用户定义的密码，以便更改用户定义的密码的优先级。 • [仅适用于入站邮件]从邮件正文提取的密码优先于用户定义的口令，后者用于打开传入邮件的受密码保护的附件。 • [仅适用于出站邮件]用户定义的密码优先于从用于打开外发邮件的受密码保护的附件的邮件正文中提取的密码。 [可选] **仅应用用户定义的密码 (Apply User-defined Passwords Only)** 复选框：如果要仅使用用户定义的密码打开传入和传出邮件中受密码保护的附件，请选中此复选框。选中此复选框时，邮件网关不会使用从邮件正文中提取的密码来打开受密码保护的附件。 **Note** 如果未启用“可能用于分析的用户定义的密码”(Probable User-defined Password for Analysis) 选项按钮，则默认情况下会禁用“仅应用用户定义的密码”(Apply User-defined Passwords Only) 复选框。
由于在 URL 过滤操作过程中发现解码错误而导致邮件不可扫描时的操作	指定由于在URL过滤操作期间发现解码错误而无法由内容扫描程序扫描邮件时要执行的操作。
由于提取失败而导致邮件不可扫描时要执行的操作	指定当内容扫描程序由于附件提取失败而不可扫描邮件时要执行的操作。
由于 RFC 违规而导致邮件不可扫描时要执行的操作	指定当内容扫描程序由于RFC违规而不可扫描邮件时要执行的操作。

c) 点击**提交 (Submit)**。

步骤 4 （可选）手动更新内容扫描程序文件。在**当前内容扫描程序文件 (Current Content Scanner files)** 下，点击**立即更新 (Update Now)**。

通常，这些文件将使用更新服务器自动更新。

Note 您也可使用 CLI 中的 `contentscannerupdate` 来手动更新这些文件。

步骤 5 确认更改。

为不可扫描的邮件配置邮件处理操作

邮件网关中的内容扫描程序现在可以处理由于以下原因而未扫描的邮件：

- 文件提取失败
- RFC 违规
- 在 URL 过滤操作期间发现解码错误

您可以对内容扫描程序未扫描的邮件配置下列任何一个邮件处理操作：

- 删除邮件
- 原样传送邮件
- 将邮件发送到策略隔离区

您可以点击 Web 界面的“安全服务”(Security Services) > “扫描行为”(Scan Behavior) 页面中的**编辑全局设置 (Edit Global Settings)** 按钮，以便在内容扫描程序未扫描的邮件上启用和配置邮件处理操作。

传送邮件

如果选择传送邮件，可以执行以下附加操作：

- 修改邮件主题
- 在邮件中添加自定义信头
- 修改邮件收件人
- 将邮件发送到备用目标主机

注释 这些操作相互之间并不排斥，在不同的传入或外发策略中可以不同的方式组合其中某些或全部操作，以满足用户组的不同处理需求。

修改邮件主题

通过前加或后加某些文本字符串，可以更改内容扫描程序不扫描的邮件文本，以帮助用户轻松识别邮件，并对已识别的邮件排序。

注释 “修改邮件主题”字段中不会忽略空格。在此字段中输入的文本后面（如果是前置）或前面（如果是后加）添加空格，可分隔添加的文本与邮件的原始主题。例如，如果要前置，可在文本 `[WARNING: UNSCANNABLE EXTRACTION FAILURE]` 后面添加几个拖尾空格。

添加到内容扫描程序不扫描的邮件主题的默认文本：

原因	添加到主题的默认文本
提取失败	[WARNING: UNSCANNABLE EXTRACTION FAILED]
RFC 违规	[WARNING: UNSCANNABLE RFC NON-COMPLIANT]
在 URL 过滤操作期间发现解码错误	[警告：应用 URL 过滤操作时出现解码错误]

在邮件中添加自定义信头

您可以定义一个附加的自定义信头，将其添加到内容扫描程序不扫描的所有邮件中。点击**是 (Yes)**，并定义信头名称和文本。

修改邮件收件人

您可以修改邮件收件人，使内容扫描程序不扫描的邮件传送到其他地址。点击**是 (Yes)**，并输入新的收件人地址。

发送邮件到备用目标主机

针对内容扫描程序不扫描的邮件，可以选择将通知发送到其他收件人或目标主机。点击**是 (Yes)**，并输入备用地址或主机。

例如，您可以将内容扫描程序不扫描的邮件路由到管理员的邮箱或特殊邮件服务器，以进行后续检查。如果该邮件包含多个收件人，则只会向备用收件人发送一个副本。

将邮件发送到策略隔离区

标记为要进行隔离时，内容扫描程序未扫描的邮件将继续通过邮件管道的其余部分。当邮件到达管道末尾时，如果此邮件被标记为放入一个或多个隔离区，邮件将加入这些队列。请注意，如果邮件没有到达管道末尾，邮件不会被放入隔离区。

例如，内容过滤器可能导致邮件被丢弃或退回，在这种情况下，不会隔离邮件。

注释 如果邮件网关中未定义策略隔离区，则无法向隔离区发送邮件。

如果选择将邮件发送到策略隔离区，则可以执行以下附加操作：

- 修改邮件主题
- 在邮件中添加自定义信头

修改邮件主题信头

您可以通过前置或后加某些文本字符串来更改发送至策略隔离区的邮件文本，从而帮助用户轻松识别邮件及对识别的邮件进行排序。

注释 “修改邮件主题”字段中不会忽略空格。在此字段中输入的文本后面（如果是前置）或前面（如果是后加）添加空格，可分隔添加的文本与邮件的原始主题。例如，如果要前置，可在文本 `[WARNING: UNSCANNABLE EXTRACTION FAILURE]` 后面添加几个拖尾空格。

添加到发送到策略隔离区的邮件主题的默认文本：

原因	添加到主题的默认文本
提取失败	[WARNING: UNSCANNABLE EXTRACTION FAILED]
RFC 违规	[WARNING: UNSCANNABLE RFC NON-COMPLIANT]
在 URL 过滤操作期间发现解码错误	[警告：应用 URL 过滤操作时出现解码错误]

在邮件中添加自定义信头

您可以定义一个附加的自定义信头，以将其添加到发送至策略隔离区的所有邮件。点击**是 (Yes)**，并定义信头名称和文本。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。