内容过滤器

本章包含以下部分：

内容过滤器概述

使用内容过滤器可自定义其他内容安全功能（例如防病毒扫描或 DLP）的标准例行处理之外的邮件处理。例如，如果内容需要隔离以便稍后进行检查，或者公司策略要求某些邮件在传送前需进行加密，则您可以使用内容过滤器。

内容过滤器的工作原理

内容过滤器与邮件过滤器类似，只不过在邮件管道中的应用位置较为靠后 - 在邮件过滤之后，在为每个匹配的邮件策略将一封邮件“拆分”为多封独立的邮件之后（有关详细信息，请参阅邮件拆分），以及对邮件进行反垃圾邮件和防病毒扫描之后应用。

内容过滤器将扫描传入或外发邮件。不能定义同时扫描两类邮件的过滤器。邮件网关针对每类邮件配有一个单独的内容过滤器“主列表”。该主列表还确定设备以什么顺序运行内容过滤器。但是，各个邮件策略可在邮件与策略相匹配时，确定将执行哪些特定的过滤器。

内容过滤器按用户（发件人或收件人）扫描邮件。

内容过滤器包含以下组件：

- 条件，确定邮件网关何时使用内容过滤器扫描邮件（可选）
- 操作，即邮件网关对邮件所采取的操作（必需）
- 操作变量，即修改邮件时邮件网关可向其添加的操作变量（可选）

相关主题

- 如何使用内容过滤器扫描邮件内容, on page 2
- 内容过滤器条件, on page 2
- 内容过滤器操作, on page 9
- 操作变量, on page 15

如何使用内容过滤器扫描邮件内容

Procedure

	Command or Action	Purpose
步骤 1	（可选）定义内容过滤器的支持功能。	创建要与您的内容过滤器配合使用的以下任何项目： • 加密配置文件 • 免责声明模板 • 通知模板 • 策略隔离区 • URL 允许列表
步骤 2	定义传入或传出内容过滤器。	内容过滤器可能由下列各项组成： • 内容过滤器条件, on page 2（可选） • 内容过滤器操作, on page 9 • 操作变量, on page 15（可选） 创建内容过滤器, on page 17
步骤 3	定义要为其设置内容安全规则的用户组。	创建传入或传出邮件策略。
步骤 4	将内容过滤器分配给要将过滤器用于其传入或传出邮件的用户组。	请参阅邮件策略

内容过滤器条件

条件为“触发”条件，可确定邮件网关是否对符合相关邮件策略的邮件使用过滤器。为内容过滤器指定条件是可选的。无条件的内容过滤器将应用于符合相关邮件策略的所有邮件。

在内容过滤器条件中，添加在邮件正文或附件中搜索特定模式的过滤器规则时，可以为必须找到模式的次数指定最小阈值。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。可以为文本、智能标识符或内容词典术语指定此阈值。

可以为每个过滤器定义多个条件。当定义了多个条件时，可以选择是以逻辑 OR（“以下任一条件...”）还是逻辑 AND（“以下所有条件”）的形式将条件联系在一起。

Table 1: 内容过滤器条件

情况	说明
无条件	在内容过滤器中指定条件是可选的。如果没有指定条件，则意味着使用true规则。true 规则会匹配所有邮件，并且始终会执行操作。
邮件正文或附件	**包含文本**：邮件正文是否包含文本或与特定模式匹配的附件？ **包含智能标识符**：邮件正文或附件中的内容是否与智能标识符匹配？ • 信用卡号 • 美国社会保险号 • CUSIP（统一证券识别程序委员会）号码 • ABA（美国银行协会）路由号码 **包含智能标识符前缀**：邮件正文或附件中的内容是否与带有前缀（‘credit,' 'ssn,' 'cusip,' 或 'aba) 的智能标识符匹配？ **包含内容词典中的术语**：邮件正文是否包含名为<词典名称>的内容词典中的任何正则表达式或术语？ 要启用此选项，必须已创建词典。请参阅内容词典。 **Note** 词典相关的条件仅在启用了一个或多个词典时才可用。有关创建内容词典的详细信息，请参阅内容词典。 **需要的匹配数量**。指定要使该规则求值为 true 所需的匹配数量。可以为文本、智能标识符或内容词典术语指定此阈值。 这包括传送-状态部分和关联的附件。

情况	说明
消息内容	**包含文本**：邮件正文是否包含与特定模式匹配的文本？ **包含智能标识符**：邮件正文中的内容是否与智能标识符匹配？智能标识符可以检测以下模式： • 信用卡号 • 美国社会保险号 • CUSIP（统一证券识别程序委员会）号码 • ABA（美国银行协会）路由号码 **包含智能标识符前缀**：邮件正文中的内容是否与带有前缀（‘credit,' 'ssn,' 'cusip,' 或 'aba) 的智能标识符匹配？ **包含内容词典中的术语**：邮件正文是否包含名为<词典名称>的内容词典中的任何正则表达式或术语？ 要启用此选项，必须已创建词典。请参阅内容词典。 **Note** 词典相关的条件仅在启用了一个或多个词典时才可用。有关创建内容词典的详细信息，请参阅内容词典。 **需要的匹配数量**。指定要使该规则求值为 true 所需的匹配数量。可以为文本或智能标识符指定此阈值。 此规则仅适用于邮件的正文。它不包括附件或信头。
URL 类别	请参阅按 URL 信誉或 URL 类别过滤：条件和规则 和 关于 URL 类别。
消息大小	正文大小是否在指定的范围内？正文大小是指邮件的大小，包括信头和附件。body-size 规则选择正文大小与指定数字相匹配的邮件。
宏检测	传入或传出邮件是否包含启用宏的附件？ 您可以使用宏检测条件检测所选文件类型的邮件中启用宏的附件。 **Note** 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。

情况	说明
附件内容	**包含文本**。邮件是否包含文本或另一个附件与指定模式匹配的附件？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。 **包含智能标识符**。邮件附件中的内容是否与指定的智能标识符匹配？ **包含智能标识符前缀**：邮件附件中的内容是否与带有前缀 (‘credit,' 'ssn,' 'cusip,' 或 'aba) 的智能标识符匹配？ **包含内容词典中的术语**。附件是否包含名为<词典名称>的内容词典中的任何正则表达式或术语？ 要搜索词典术语，必须已创建词典。请参阅内容词典。 **Note** 词典相关的条件仅在启用了一个或多个词典时才可用。有关创建内容词典的详细信息，请参阅内容词典。 **需要的匹配数量**。指定要使该规则求值为 true 所需的匹配数量。可以为文本、智能标识符或内容词典匹配指定此阈值。

情况	说明
附件文件信息	**文件名**。邮件是否包含其文件名与特定模式匹配的附件？ **文件名包含内容词典中的术语**。邮件是否包含其文件名包含名为 <词典名称> 的内容词典中的任何正则表达式或术语的附件？ 要启用此选项，必须已创建词典。请参阅内容词典。 **Note** 词典相关的条件仅在启用了一个或多个词典时才可用。有关创建内容词典的详细信息，请参阅内容词典。 **文件类型**。邮件是否具有其文件类型基于指纹与特定模式匹配的附件（与 UNIX 的 file 命令类似）？ **MIME 类型**。邮件是否具有特定 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。） **文件散列列表**。邮件是否包含与特定文件 SHA-256 或 MD5 值匹配的附件？从下拉列表中选择所需的文件散列列表。 **Note** 您只能选择包含 SHA-256 文件散列类型的文件散列列表。 **图像分析**。邮件是否具有与指定的图像判定匹配的图像附件？有效的图像分析判定包括：可疑、不当、可疑或不当、不可扫描或者正常。 **外部威胁源**：文件是否与选定外部威胁源来源的威胁信息相匹配？ **选择文件散列异常列表**：（可选）选择您不希望邮件网关检测威胁的已在允许之列的文件散列列表。 有关详细信息，请参阅将邮件网关配置为使用外部威胁源。 **附件已损坏**。此邮件是否具有已损坏的附件？ **Note** 损坏的附件是扫描引擎不可扫描且识别为已损坏的附件。
附件保护	**包含受密码保护或加密的附件**。 （例如，使用此条件来识别可能不可扫描的附件） **包含未受密码保护或加密的附件**。
主题信头	**主题信头**：主题信头是否与特定模式匹配？ **包含内容词典中的术语**：主题信头是否包含名为<词典名称>的内容词典中的任何正则表达式或术语？ 要搜索词典术语，必须已创建词典。请参阅内容词典。 **Note** 词典相关的条件仅在启用了一个或多个词典时才可用。有关创建内容词典的详细信息，请参阅内容词典。

情况	说明
其他信头	**信头名称**：邮件是否包含特定信头？ **信头值**：该信头的值是否与特定模式匹配？ **信头值包含内容词典中的术语**。指定的信头是否包含名为<词典名称>的内容词典中的任何正则表达式或术语？ 要搜索词典术语，必须已创建词典。请参阅内容词典 **Note** 词典相关的条件仅在启用了一个或多个词典时才可用。有关创建内容词典的详细信息，请参阅内容词典。 有关如何显示如何使用此选项的示例，请参阅使用自定义信头将疑似垃圾邮件中的 URL 重定向到思科网络安全代理：配置示例。
信封发件人	**信封发件人**。信封发件人（即，<MAIL FROM>）是否与指定模式匹配？ **匹配 LDAP 组**。信封发件人（即，<MAIL FROM>）是否在指定的 LDAP 组中？ **包含内容词典中的术语**。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？ 要搜索词典术语，必须已创建词典。请参阅内容词典。 **Note** 词典相关的条件仅在启用了一个或多个词典时才可用。有关创建内容词典的详细信息，请参阅内容词典。
信封收件人	**信封收件人**。信封收件人（即 Envelope To <RCPT TO>）是否与指定模式匹配？ **匹配 LDAP 组**。信封收件人（即 Envelope To <RCPT TO>）是否在指定的 LDAP 组中？ **包含内容词典中的术语**。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？ 要搜索词典术语，必须已创建词典。请参阅内容词典。 **Note** 词典相关的条件仅在启用了一个或多个词典时才可用。有关创建内容词典的详细信息，请参阅内容词典。 “信封收件人”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。 信封发件人（即，<MAIL FROM>）是否在指定的 LDAP 组中？
接收侦听程序	邮件是否通过指定的侦听程序接收？侦听程序名称必须是系统上当前配置的侦听程序的名称。

情况	说明
远程 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？远程 IP 规则会进行测试以确定发送该邮件的主机的 IP 地址是否与特定模式匹配。该地址可以是互联网协议版本 4 (IPv4) 或版本 6 (IPv6) 地址。IP 地址模式使用发件人组语法中描述的允许的主机记法指定，但 SBO、IPR、dnslist 记法和特殊关键字 ALL 除外。
信誉得分	什么是发件人的 IP 信誉得分？信誉得分规则根据另一个值来检查 IP 信誉得分。
DKIM 身份验证	DKIM 身份验证已通过、部分验证、暂时无法验证且返回、永久失败还是未返回 DKIM 结果？
伪造邮件检测	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。 选择内容词典并输入阈值（1 到 100），以将邮件视为潜在伪造邮件。 伪造的邮件检测条件将“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。 如果要跳过针对特定发件人的邮件的伪造邮件检测过滤器，请从**异常列表**下拉列表中选择地址列表。 **Note** 只能选择使用完整邮件地址创建的地址列表。有关详细信息，请参阅为传入连接规则使用发件人地址列表。 有关详细信息，请参阅伪造邮件检测。
SPF 验证	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。有关 SPF 验证的详细信息，请参阅“邮件身份验证”一章。 **Note** 如果在没有 SPF 身份的情况下配置了 SPF 验证内容过滤条件，并且邮件中包含具有不同判定的而不同 SPF 身份，则当邮件中的其中一个判定与该条件匹配时，将会触发该条件。
S/MIME 网关邮件	邮件是否已经过 S/MIME 签名、加密或签名并加密？有关详细信息，请参阅S/MIME 安全服务

情况	说明
S/MIME 网关已验证	S/MIME 邮件是否已成功通过验证，解密或已成功解密并验证？有关详细信息，请参阅S/MIME 安全服务
邮件语言	邮件（主题和正文）是否为其中一种所选语言？此条件不会检查附件和报头中的语言。 **语言检测的工作原理是什么？** 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。
重复边界验证	邮件是否包含重复的 MIME 边界？ 如果要对包含重复 MIME 边界的邮件执行操作，请使用此条件。 **Note** 基于附件的条件（例如，附件内容）或操作（例如，按内容删除附件）将无法处理格式不正确的邮件（具有重复的 MIME 边界）。
地理定位	邮件是否来自选定的国家/地区？ 您可以使用地理定位条件来处理来自您所选特定国家/地区的传入邮件。 **Note** 在使用地理定位内容过滤器之前，请启用邮件网关上的反垃圾邮件引擎。
域信誉	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 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

内容过滤器操作

该操作是邮件网关针对与内容过滤器的条件匹配的邮件进行的操作。有许多不同类型的操作可用，包括修改邮件、将其隔离或丢弃。对邮件执行的“最终操作”为传送或丢弃，这会强制邮件安全设备立即执行该操作并放弃所有进一步的处理，例如爆发过滤器或 DLP 扫描。

必须为每个内容过滤器至少定义一个操作。

系统会按顺序对邮件执行操作，因此在为内容过滤器定义多个操作时，请考虑操作顺序。

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。有关详细信息，请参阅“文本资源”一章。

仅可为每个过滤器定义一个最终操作，而且最终操作必须是列出的最后一项操作。退回、传送和丢弃都是最终操作。为内容过滤器输入操作时，GUI 和 CLI 会强制将最终操作放在最后。

另请参阅操作变量, on page 15。

Table 2: 内容过滤器操作

操作	说明
隔离	**隔离 (Quarantine)**。标记要保留在某一个策略隔离区中的邮件。 **复制邮件**：将邮件的副本发送到指定的隔离区，并继续处理原始邮件。任何其他操作都应用于原始邮件。
传送时加密	邮件继续进行下一阶段的处理。当完成所有处理后，将加密并发送邮件。 **加密规则**：始终加密邮件，或仅在尝试先通过 TLS 连接进行发送失败时加密邮件。有关详细信息，请参阅使用 TLS 连接作为加密备用项。 **加密配置文件**。完成处理后，使用指定的加密配置文件来加密邮件，然后发送邮件。此操作与思科加密设备或托管密钥服务配合使用。 **主题**。加密邮件的主题。默认情况下，值为 **`$Subject`**。
按内容删除附件	**附件包含**。丢弃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。 **包含智能标识符**。删除包含指定的智能标识符的邮件中的所有附件。 **附件包含内容词典中的术语**。附件是否包含名为 <词典名称> 的内容词典中的任何正则表达式或术语？ **需要的匹配数量**。指定要使该规则求值为 true 所需的匹配数量。可以为文本、智能标识符或内容词典匹配指定此阈值。 **替换邮件**。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	说明
按文件信息删除附件	**文件名**。丢弃邮件中其文件名与指定的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。 **文件大小**。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。 **文件类型**。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。 **MIME 类型**。丢弃邮件中给定 MIME 类型的所有附件。 **文件散列列表**。丢弃与所选文件散列列表中的文件 SHA-256 或 MD5 值匹配的邮件中的所有附件。从下拉列表中选择所需的文件散列列表。 **Note** 您只能选择包含 SHA-256 文件散列类型的文件散列列表。 **图像分析判定**。删除与指定的图像判定匹配的图像附件。有效的图像分析判定包括：可疑、不当、可疑或不当、不可扫描或者正常。 **外部威胁源**。丢弃文件被 ETF 引擎归类为恶意的邮件中的所有邮件附件。 **选择一个文件散列异常列表**。（可选）选择您不希望思科邮件安全网关检测威胁的已列入允许列表的文件散列列表。 有关详细信息，请参阅将邮件网关配置为使用外部威胁源。 **替换邮件**。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。
删除包含宏的附件	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。 **自定义替换消息（可选）**：默认情况下，当丢弃附件时，系统生成的邮件会添加到邮件正文的底部。 以下是从邮件中丢弃启用宏的附件时系统生成的邮件示例： **`A MIME attachment of type <application/vnd.ms-excel> was removed here by a drop-macro-enabled-attachments filter rule on the host <mail.example.com>.`** 您在**自定义替换邮件 (Custom Replacement Message)** 字段中输入的自定义邮件将替换系统生成的邮件。

操作	说明
URL Reputation	请参阅修改邮件中的 URL：在过滤器中使用 URL 信誉和 URL 类别操作 和 创建允许的 URL 过滤列表。 使用“没有分数”来指定无法确定其信誉的 URL 的操作。 **Note** 邮件网关会考虑签名的邮件是否使用 S/MIME 进行加密或其是否包含 S/MIME 签名。
URL 类别	请参阅修改邮件中的 URL：在过滤器中使用 URL 信誉和 URL 类别操作 和 关于 URL 类别。 **Note** 邮件网关会考虑签名的邮件是否使用 S/MIME 进行加密或其是否包含 S/MIME 签名。
添加免责声明文本	**上方**。在邮件上方（页眉）添加免责声明。 **下方**。在邮件下方（页脚）添加免责声明。 **说明**：必须已创建免责声明文本才能使用此内容过滤器操作。 有关详细信息，请参阅免责声明模板。
忽略爆发过滤器扫描	绕过对此邮件进行的爆发过滤器扫描。
绕过 DKIM 签名	绕过对此邮件进行的 DKIM 签名。
发送副本 (Bcc:)	**邮件地址**。采用匿名方式将此邮件的副本发送给指定的收件人。 **主题**。为复制的邮件添加主题。 **返回路径（可选）**。指定返回路径。 **备用邮件主机（可选）**。指定备用邮件主机。
通知	**通知**。向指定的收件人报告此邮件。可以有选择地通知发件人和收件人。 **主题**。为复制的邮件添加主题。 **返回路径（可选）**。指定返回路径。 **使用模板**。从创建的模板中选择一个模板。 **包括原始邮件作为附件**。添加原始邮件作为附件。
更改收件人为	**邮件地址**。将邮件的收件人更改为指定的邮件地址。
传送到指定的目标主机	**邮件主机**。将邮件的目标邮件主机更改为指定的邮件主机。 **Note** 此操作可防止隔离已被反垃圾邮件扫描引擎分类为垃圾邮件的邮件。此操作将覆盖隔离区并将其发送到指定的邮件主机。

操作	说明
从 IP 接口发送	**从 IP 接口发送**。从指定的 IP 接口发送。从 IP 接口发送操作会将邮件的源主机更改为指定的源。源主机包括应从其发送邮件的 IP 接口。
删除信头	**信头名称**。在发送之前，从邮件中删除指定的信头。
添加/编辑信头	**将新的信头插入邮件中或修改现有信头**。 **信头名称**。新的或现有信头的名称。 **指定新信头的值**。在发送之前，将新信头的值插入邮件中。 **附加到现有信头值的前面**。在发送之前，附加到现有信头值的前面。 **附加到现有信头值**。在发送之前，附加到现有信头值。 **从现有信头值搜索和替换**。在**搜索 (Search for)** 字段中输入搜索词语以查找要在现有信头中替换的值。在**替换为 (Replace with)** 字段中输入要插入信头的值。可以使用正则表达式搜索该值。如果要从信头中删除该值，请将**替换为 (Replace with)** 字段留空。
伪造邮件检测	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。
添加邮件标记	将自定义术语插入邮件以与 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。有关在 DLP 策略中使用邮件标记的信息，请参阅 防数据丢失策略。
添加日志条目	将自定义文本插入 IronPort 文本邮件日志的 INFO 级别。文本可包含操作变量。日志条目也将显示在邮件跟踪中。

操作	说明
添加 CEF 日志条目	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。 **Note** 仅当您在邮件网关中配置“合并事件日志”日志订用时，才能使用此内容过滤器操作。 **标签**：为合并事件日志条目添加标签。 **Note** 标签最多只能包含 64 个字符。 **值**：为“合并事件日志”条目添加消息。 **Note** 消息不得超过 1024 个字符。 **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。 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。 **例如**：如果在“标签”字段中输入“label1”，在“值”字段中输入“value20”，则会在合并事件日志中添加以下字段： `ESACustomLogs={'label1': ['value20']}`
传送时进行 S/MIME 签名/加密	在传送期间，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。 **S/MIME 发送配置文件**：使用指定的 S/MIME 发送配置文件执行 S/MIME 签名或加密。请参阅管理 S/MIME 发送配置文件。
立即加密并传送（最终操作）	加密并传送邮件，跳过任何进一步处理。 **加密规则**：始终加密邮件，或仅在尝试先通过 TLS 连接进行发送失败时加密邮件。有关详细信息，请参阅使用 TLS 连接作为加密备用项。 **加密配置文件**。使用指定的加密配置文件来加密邮件，然后发送邮件。此操作与思科加密设备或托管密钥服务配合使用。 **主题**。加密邮件的主题。默认情况下，值为 **`$Subject`**。
S/MIME 签名/加密（最终操作）	执行 S/MIME 签名或加密并传送邮件，跳过任何进一步处理。 **S/MIME 发送配置文件**：使用指定的 S/MIME 发送配置文件执行 S/MIME 签名或加密。请参阅管理 S/MIME 发送配置文件。
退回（最终操作）	将邮件发回给发件人。

操作	说明
跳过保留内容过滤器（最终操作）	将邮件传送到下一处理阶段，跳过任何进一步的内容过滤器。根据配置，这可能意味着会将邮件传送给收件人、隔离区或开始进行爆发过滤器扫描。
丢弃（最终操作）	删除并丢弃邮件。
安全打印	使用“安全打印”(Safe Print) 内容过滤器操作以安全打印邮件附件。 您可以通过以下任何一种方式使用“安全打印”(Safe Print) 内容过滤器操作： • **安全打印匹配附件 (Safe print matching attachments)**：使用此选项可安全打印与已配置的内容过滤器条件匹配的所有邮件附件。 • **安全打印所有附件 (Safe print all attachments)**：使用此选项可安全打印配置的内容过滤器条件成立时的所有邮件附件 选择**是 (Yes)** 可删除标记为不可扫描的邮件附件。 **Note** 默认情况下，当附件不可扫描时，系统生成的邮件将添加为附件文本文件。您可以在**自定义替换邮件 (Custom Replacement Message)** 字段中输入自定义邮件。 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。

相关主题

- 操作变量, on page 15

操作变量

添加到由内容过滤器处理的邮件的信头可包含变量，当执行相应操作时，这些变量会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 3: 操作变量

变量	语法	说明
所有信头	`$AllHeaders`	替换为邮件信头。
正文大小	`$BodySize`	替换为邮件的大小（以字节为单位）。
日期	`$Date`	替换为当前日期，采用 MM/DD/YYYY 格式。
已丢弃的文件名	`$dropped_filename`	仅返回最近丢弃的文件名。

变量	语法	说明
已丢弃的文件名	`$dropped_filenames`	与 $filenames 相同，但显示已丢弃的文件的列表。
已删除的文件类型	`$dropped_filetypes`	与 $filetypes 相同，但显示已丢弃的文件类型的列表。
信封发件人	`$envelopefrom` or `$envelopesender`	替换为邮件的信封发件人（即，<MAIL FROM>）。
信封收件人	`$EnvelopeRecipients`	替换为邮件的所有信封收件人（信封目标，<RCPT TO>）。
文件名	`$filenames`	替换为邮件附件文件名的逗号分隔列表。
文件大小	`$filesizes`	替换为邮件附件文件大小的逗号分隔列表。
文件类型	`$filetypes`	替换为邮件附件文件类型的逗号分隔列表。
过滤器名称	`$FilterName`	替换为所处理过滤器的名称。
GMTimeStamp	`$GMTimeStamp`	替换为当前时间和日期，即电子邮件的“接收时间：”(Received:) 行中的时间，采用 GMT 时间。
HAT 组名	`$Group`	替换为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<”。
邮件流策略	`$Policy`	替换为注入邮件时应用于发件人的 HAT 策略的名称。如果未使用预定义的策略名称，则插入字符串“>Unknown<”。
匹配的内容	`$MatchedContent`	替换为内容扫描过滤器触发的一个或多个值。匹配的内容可以是内容词典匹配、智能标识符或与正则表达式的匹配。
信头	`$Header['string']`	如果原始邮件包含匹配的信头，则替换为被引用信头的值。请注意，也可以使用双引号。
主机名	`$Hostname`	替换为邮件网关的主机名。
内部邮件 ID	`$MID`	替换为邮件 ID，或内部用来标识邮件的“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。

变量	语法	说明
接收接口	`$RecvInt`	替换为接收邮件的接口的昵称。
远程 IP 地址	`$RemoteIP`	替换为将邮件发送给邮件网关的系统的 IP 地址。
远程主机地址	`$remotehost`	替换为将邮件发送到邮件网关的系统的主机名。
SenderBase 信誉得分	`$Reputation`	替换为发件人的 SenderBase 信誉得分。如果没有信誉得分，会替换为“无”。
主题	`$Subject`	替换为邮件的主题。
时间	`$Time`	替换为本地时区中的当前时间。
时间戳	`$Timestamp`	替换为当前时间和日期，即电子邮件的“接收时间：”(Received:) 行中的时间，采用本地时区时间。

根据内容过滤邮件的方法

相关主题

- 创建内容过滤器, on page 17
- 默认情况下为所有收件人启用内容过滤器, on page 18
- 将内容过滤器应用到特定用户组的邮件, on page 19
- 有关在 GUI 中配置内容过滤器的说明, on page 19

创建内容过滤器

准备工作

- 如果要加密与内容过滤器匹配的邮件，请创建加密配置文件。
- 如果要将免责声明添加到匹配的邮件，请创建免责声明模板以用于生成免责声明。
- 如果因匹配邮件的原因要将通知邮件发送给用户，请创建用于生成通知的通知模板。
- 如果要隔离邮件，可为这些邮件创建新策略隔离区或使用现有的隔离区。

Procedure

步骤 1 点击**邮件策略 (Mail Policies) > 传入邮件策略 (Incoming Mail Policies)**

或

邮件策略 (Mail Policies) > 传出邮件策略 (Outgoing Mail Policies)。

步骤 2 点击**添加过滤器 (Add Filter)**。

步骤 3 输入过滤器的名称和描述。

步骤 4 （交叉参考）点击**可编辑者（角色）(Editable By [Roles])** 链接，选择策略管理员，然后点击**确定 (OK)**。

属于策略管理员用户角色的委派管理员可以编辑此内容过滤器，以及在其邮件策略中使用该内容过滤器。

步骤 5 （可选）添加条件来触发过滤器。

a) 点击“添加条件”(Add Condition)。
b) 选择条件类型。
c) 定义条件的规则。
d) 点击**确定 (OK)**。
e) 为要添加到过滤器的任何其他条件重复执行这些步骤。为内容过滤器定义多个条件时，可以定义需要应用所有定义的操作（即逻辑 AND）还是任何定义的操作（逻辑 OR）才能将内容过滤器视为匹配。

Note 如果不添加条件，则邮件网关将对匹配与过滤器关联的一个邮件策略的任何邮件执行内容过滤器的操作。

步骤 6 为邮件网关添加要对匹配过滤器条件的邮件执行的操作。

a) 点击“添加操作”(Add Action)。
b) 选择操作类型。
c) 定义操作。
d) 点击**确定 (OK)**。
e) 对希望邮件网关执行的任何其他操作重复先前的步骤。
f) 对于多个操作，按照希望邮件网关将它们应用到邮件的顺序来安排操作。每个过滤器仅可有一个“最终”操作，并且 AsyncOS 会自动将最终操作移动到顺序的末尾。

步骤 7 提交并确认更改。

What to do next

- 可以在默认传入或传出邮件策略中启用内容过滤器。
- 可以在邮件策略中为特定用户组启用内容过滤器。

默认情况下为所有收件人启用内容过滤器

Procedure

步骤 1 依次点击**邮件策略 (Mail Policies) > 传入邮件策略 (Incoming Mail Policies)**。

或

邮件策略 (Mail Policies) > 传出邮件策略 (Outgoing Mail Policies)。

步骤 2 点击默认策略行中的内容过滤器安全服务链接。

步骤 3 在“内容过滤”(Content Filtering) 安全服务页面上，将“默认策略的内容过滤”(Content Filtering for Default Policy) 从“禁用内容过滤器”(Disable Content Filters) 更改为“启用内容过滤器（自定义设置）”(Enable Content Filters [Customize settings])。

在主列表中定义的内容过滤器（在内容过滤器概述 , on page 1中创建）会显示在此页面上。将值更改为“启用内容过滤器（自定义设置）”(Enable Content Filters [Customize settings]) 时，每个过滤器的复选框将变为已启用状态。

步骤 4 针对要启用的每个内容过滤器选中**启用 (Enable)** 复选框。

步骤 5 提交并确认更改。

将内容过滤器应用到特定用户组的邮件

准备工作

- 为要将内容过滤器应用到其邮件的用户组创建传入或传出邮件策略。有关详细信息，请参阅为发件人和收件人组创建邮件策略。

Procedure

步骤 1 依次点击**邮件策略 (Mail Policies) > 传入邮件策略 (Incoming Mail Policies)**。

或

邮件策略 (Mail Policies) > 传出邮件策略 (Outgoing Mail Policies)。

步骤 2 点击要将内容过滤器应用到的邮件策略所对应的内容过滤器安全服务（“内容过滤器”[Content Filters] 列）的链接。

步骤 3 在“内容过滤”(Content Filtering) 安全服务页面上，将“策略的内容过滤：工程”(Content Filtering for Policy: Engineering) 从“启用内容过滤（继承默认策略设置）”(Enable Content Filtering [Inherit default policy settings]) 更改为“启用内容过滤（自定义设置）”(Enable Content Filtering [Customize settings])。

步骤 4 选择要使用的内容过滤器对应的复选框。

步骤 5 提交并确认更改。

有关在 GUI 中配置内容过滤器的说明

- 在创建内容过滤器时，不需要指定条件。如果未定义操作，则定义的任何操作都始终在规则中应用。（不指定条件等同于使用 true() 邮件过滤器规则 - 如果将内容过滤器应用于某个策略,，则会匹配所有邮件。）

- 如果未将自定义用户角色分配给某个内容过滤器，则该内容过滤器是公开的，并且可以由任何授权管理员用于其邮件策略。有关授权管理员和内容过滤器的详细信息，请参阅“常规管理任务”一章。
- 管理员和操作员可以查看和编辑邮件网关上的所有内容过滤器，即使内容过滤器分配到自定义用户角色也是如此。
- 为过滤器规则和操作输入文本时，以下元字符在正则表达式匹配中具有特殊含义：^ $ * + ? { [ ] \ | ( )

  如果不想使用正则表达式，则应使用“\”（反斜线）来转义任何这些字符。例如：“*警告*”

- 可以通过创建“良性”内容过滤器来测试邮件分流和内容过滤器。例如，可以创建其唯一的操作为“传送”的内容过滤器。此内容过滤器不会影响邮件处理；但是，可以使用此过滤器来测试邮件安全管理器策略处理如何影响系统中的其他元素（例如，邮件日志）。
- 相反，使用传入或传出内容过滤器的“主列表”概念时，可以创建功能非常强大且内容宽泛的内容过滤器，它们会立即影响邮件网关对所有邮件的处理。该过程如下：
  - 使用“传入或传出内容过滤器”(Incoming or Outgoing Content Filters) 页面创建顺序编号为 1 的新内容过滤器。
  - 使用“传入或传出邮件策略”(Incoming or Outgoing Mail Policies) 页面为默认策略启用新的内容过滤器。
  - 为其余所有策略启用该内容过滤器。
- 内容过滤器中提供的“Bcc:”和“隔离”(Quarantine) 操作可以帮助确定创建的隔离区的保留设置。（请参阅策略、病毒和病毒爆发隔离区）可以创建模拟进出策略隔离区的邮件流的过滤器，以便不会从系统过于快速地放行邮件（即，隔离区不会太快地填充其分配的磁盘空间）。
- 由于它使用与“扫描行为”(Scan Behavior) 页面或 **scanconfig** 命令相同的设置，因此“整个邮件”(Entire Message) 条件不会扫描邮件的信头；选择“整个邮件”(Entire Message) 将仅扫描邮件正文和附件。使用“主题”(Suject) 或“信头”(Header) 条件搜索特定信头信息。
- 如果在邮件网关中配置了 LDAP 服务器（即，使用 **ldapconfig** 命令将设备配置为查询具有特定字符串的特定 LDAP 服务器），则按 LDAP 配置用户查询仅会显示在 GUI 中。
- 如果没有预先配置资源，则内容过滤器规则生成器的某些部分不会显示在 GUI 中。例如，如果先前未使用“文本资源”(Text Resources) 页面或 CLI 中的 **textconfig** 命令配置通知模板和邮件免责声明，则它们不会显示为选项。
- 内容过滤器功能可识别、包含和/或扫描采用以下字符编码的文本：
  - Unicode (UTF-8)
  - Unicode (UTF-16)
  - 西欧语言/拉丁语-1 (ISO 8859-1)
  - 西欧语言/拉丁语-1 (Windows CP1252)
  - 繁体中文 (Big 5)
  - 简体中文 (GB 2312)
  - 简体中文 (HZ GB 2312)
  - 韩语 (ISO 2022-KR)
  - 韩语 (KS-C-5601/EUC-KR)

- 日语 (Shift-JIS (X0123)
- 日语 (ISO-2022-JP)
- 日语 (EUC)

可以在一个内容过滤器中混搭多个字符集。要获取有关显示和输入采用多个字符编码的文本的帮助，请参考网络浏览器文档。大多数浏览器都可同时显示多个字符集。

- 在传入或传出内容过滤器摘要页面上，使用“说明”(Description)、“规则”(Rules) 和“策略”(Policies) 链接更改为内容过滤器提供的视图：
  - **说明 (Description)** 视图显示在每个内容过滤器的说明字段中输入的文本。（这是默认视图）。
  - **规则 (Rules)** 视图显示规则生成器页面生成的规则和正则表达式。
  - **策略 (Policies)** 显示为其启用各个内容过滤器的策略。

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。