邮件策略和内容过滤器示例

本附录包含以下部分：

传入邮件策略概述

以下示例通过介绍以下任务展示了邮件策略的功能：

1. 编辑默认传入邮件策略的反垃圾邮件、防病毒、病毒爆发过滤器和内容过滤器。
2. 为不同的用户组（销售组织和工程组织）添加两个新策略，然后为每个组配置不同的邮件安全设置。
3. 创建要在传入邮件概述策略表中使用的三个新内容过滤器。
4. 再次编辑策略以便仅为部分组启用内容过滤器。

此示例旨在显示管理邮件策略的反垃圾邮件、防病毒、病毒爆发过滤器和内容过滤器的基于收件人的不同设置时可具备的能力与灵活性。此示例为它们分配了称为“策略管理员”的自定义用户角色，并且为其提供邮件策略和内容过滤器访问权限。有关反垃圾邮件、防病毒、病毒爆发过滤器和授权管理工作原理的更多详细信息，请参阅此章节后的各章节：

- 管理垃圾邮件和灰色邮件
- 防病毒
- 病毒爆发过滤器
- 分配管理任务

访问邮件策略

可以使用“邮件策略”(Mail Policies) 菜单以访问传入和传出邮件策略。

在全新的系统中，如果完成了系统设置向导中的所有步骤，并且选择启用反垃圾邮件、Sophos 或 McAfee 防病毒和病毒爆发过滤器，则“传入邮件策略”页面将与下图类似。

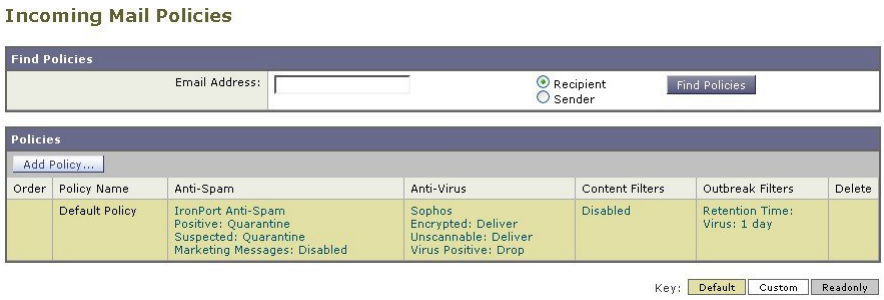
默认情况下，会为默认传入邮件策略启用这些设置：

- 反垃圾邮件（如果启用了垃圾邮件隔离区）：已启用

- 确认的垃圾邮件：隔离区，预置邮件主题
- 疑似垃圾邮件：隔离区，预置邮件主题
- 营销邮件：未启用扫描

- 反垃圾邮件（如果未启用垃圾邮件隔离区）：已启用
  - 确认的垃圾邮件：传送，预置邮件主题
  - 疑似垃圾邮件：提供，预置邮件主题
  - 营销邮件：未启用扫描
- 防病毒：已启用，扫描并修复病毒，包括具有防病毒扫描结果的 X 信头
  - 修复的邮件：传送，预置邮件主题
  - 加密的邮件：传送，附加邮件主题
  - 不可扫描的邮件：传送，附加邮件主题
  - 受病毒感染的邮件：丢弃
- Outbreak Filters: Enabled
  - 任何文件扩展名均不例外
  - 具有可疑病毒附件的邮件的保留时间为 1 天
  - 未启用邮件修改
- 内容过滤器：禁用

Figure 1: *“传入邮件策略”(Incoming Mail Policies)* 页面：全新邮件网关的默认设置



Note 在本例中，传入邮件策略将在启用了垃圾邮件隔离区的情况下使用默认反垃圾邮件设置。

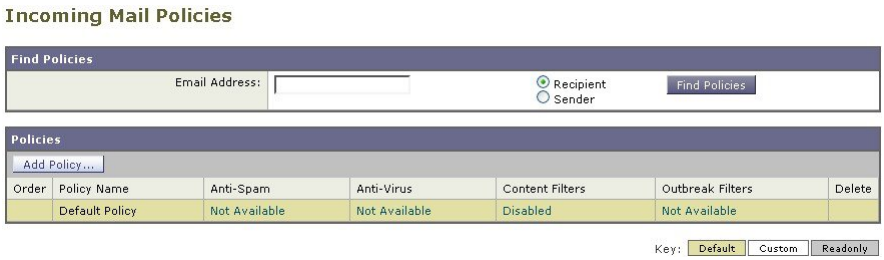
已启用、已禁用和“不可用”

邮件策略表中的列（传入或传出）会针对每个策略名称显示安全服务状态对应的链接。如果服务已启用，则会显示词语“已启用”(Enabled) 或配置摘要。同样，如果服务已禁用，则显示词语“已禁用”(Disabled)。

如果尚未接受某个服务的许可协议或服务已过期，则链接会显示为“不可用”(Not Available)。在这些情况下，单击“不可用”(Not Available) 链接将在“安全服务”(Security Services) 选项卡中显示全

局页面，而不是用于为按策略为服务配置设置的页面。此时会显示警报，指明页面已更改到其他选项卡。请参阅下图。

Figure 2: 安全服务不可用



为传入邮件配置默认反垃圾邮件策略

邮件策略表中的每个行代表一个不同的策略。每个列均表示不同的安全服务。

- 要编辑默认策略，请单击传入或传出邮件策略表底部行中与任一安全服务对应的链接。

在本例中，将传入邮件默认策略的反垃圾邮件设置更改为更积极的设置。默认值是隔离确认的垃圾邮件和疑似垃圾邮件，并禁用营销邮件扫描。此示例显示了如何更改设置，以便丢弃确认的垃圾邮件。疑似垃圾邮件将继续被隔离。将启用营销邮件扫描功能，并营销邮件传送到目标收件人。营销邮件的主题将预置文本 [MARKETING]。

Procedure

步骤 1 单击反垃圾邮件安全服务的链接。

Note 对于默认安全服务设置，页面中的第一个设置定义了是否为策略启用该服务。可以单击“禁用”(Disable) 来完全禁用该服务。

步骤 2 在“确认的垃圾邮件设置”(Positively Identified Spam Settings) 部分中，将“对邮件执行此操作”(Action to apply to this message) 更改为“删除”(Drop)。

步骤 3 在“营销邮件设置”(Marketing Email Settings) 部分中，单击**是 (Yes)** 以启用营销邮件扫描。

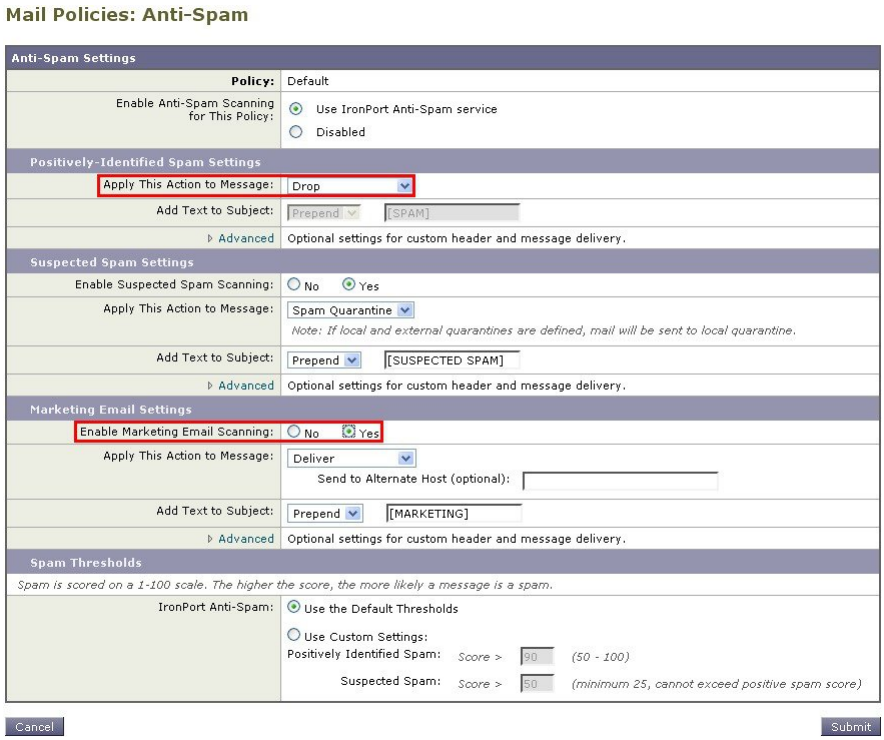
如果启用，则默认操作是传送合法的营销邮件，同时在主题前预置文本 [MARKETING]。

“添加文本到邮件”(Add text to message) 字段仅接受 US-ASCII 字符。

步骤 4 单击**提交 (Submit)**。请注意，传入邮件策略表中反垃圾邮件安全服务的摘要链接已更改，从而反映新值。

与上述步骤一样，可以为默认策略更改默认防病毒和病毒爆发过滤器设置。

Figure 3: *“反垃圾邮件设置”(Anti-Spam Settings)* 页面



为发件人和收件人组创建邮件策略

在此示例部分中，将创建两个新策略：一个用于销售组织（其成员由 LDAP 接受查询定义），另一个用于工程组织。将为两个策略分配策略管理员自定义用户角色，使属于此角色的授权的管理员负责管理这些策略。然后，为每个策略配置不同的邮件安全设置。

Procedure

步骤 1 单击**添加策略 (Add Policy)** 按钮开始创建新策略。

步骤 2 为每个策略定义唯一名称，并调整策略的顺序（如果需要）。

策略的名称必须在定义的邮件策略表（传入或传出）中是独一无二的。

切记，需对照相应表（传入或传出）中的每个策略，从上到下依次评估各个收件人。

步骤 3 单击“可编辑者（角色）”(Editable by [Roles]) 链接并为负责管理邮件策略的授权管理员选择自定义用户角色。

当单击该链接时，AsyncOS 会为具有邮件策略编辑权限的授权管理员显示自定义角色。委派管理员可以编辑策略的反垃圾邮件、防病毒和病毒爆发过滤器设置，并为该策略启用或禁用内容过滤器。

邮件策略和内容过滤器示例

只有操作员和管理员才能修改邮件策略的名称或其发件人、收件人或组。系统自动为邮件策略分配具有完全访问邮件策略权限的自定义用户角色。

有关授权管理的详细信息，请参阅分配管理任务。

步骤 4 定义策略的用户。

定义用户是发件人还是收件人。（有关详细信息，请参阅策略匹配示例。）下图显示的表单默认将收件人对应传入邮件策略，并将发件人对应传出邮件策略。

特定策略的用户可通过以下方式定义：

- 完整的邮件地址：user@example.com
- 不完整邮件地址：user@
- 域中的所有用户：@example.com
- 不完整域中的所有用户：@.example.com
- 通过匹配 LDAP 查询

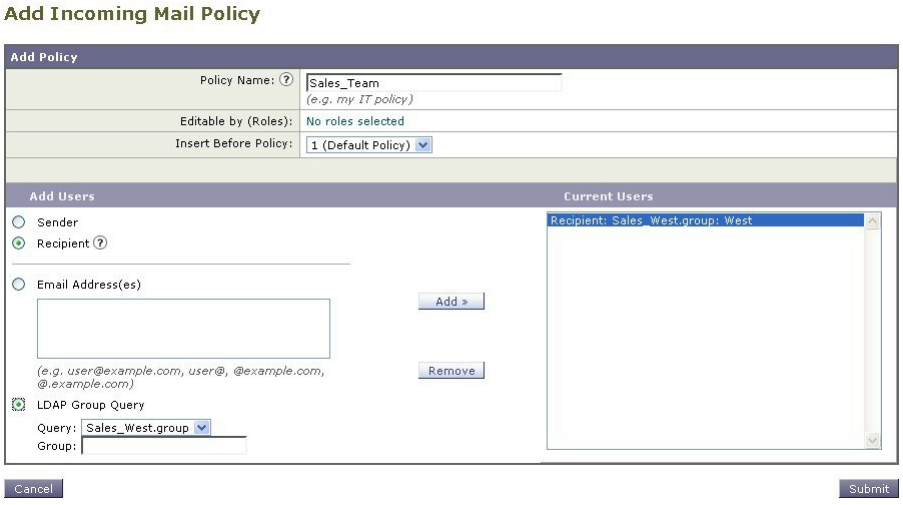
Note AsyncOS GUI 和 CLI 中的用户条目都不区分大小写。例如，如果输入收件人 Joe@ 作为用户，则发送到 joe@example.com 的邮件与之匹配。

如果在网络基础设施的 LDAP 目录中（例如，在 Microsoft Active Directory、SunONE Directory Server [以前称为“iPlanet Directory Server”] 或 OpenLDAP 目录中）存储用户信息，则可以将邮件网关配置为查询 LDAP 服务器以接受收件人地址、将邮件重路由到备用地址和/或邮件主机、伪装信头以及确定邮件是否具有来自特定组的收件人或发件人。

如果将邮件网关配置为执行此操作，则可以使用配置的查询来为邮件策略定义用户。

有关详细信息，请参阅LDAP 查询。

Figure 4: 为策略定义用户



步骤 5 单击**添加 (Add)**按钮将用户添加到当前用户列表中。

策略可以包含发件人、收件人和 LDAP 查询的组合。

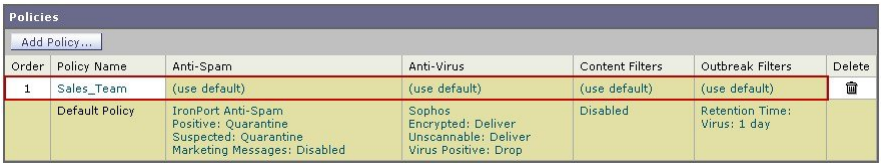
使用**删除**按钮可从当前用户的列表中删除已定义的用户。

邮件策略和内容过滤器示例

步骤 6 添加完用户后，单击**提交 (Submit)**。

请注意，所有安全服务设置都设置为在首次添加策略时使用默认值。

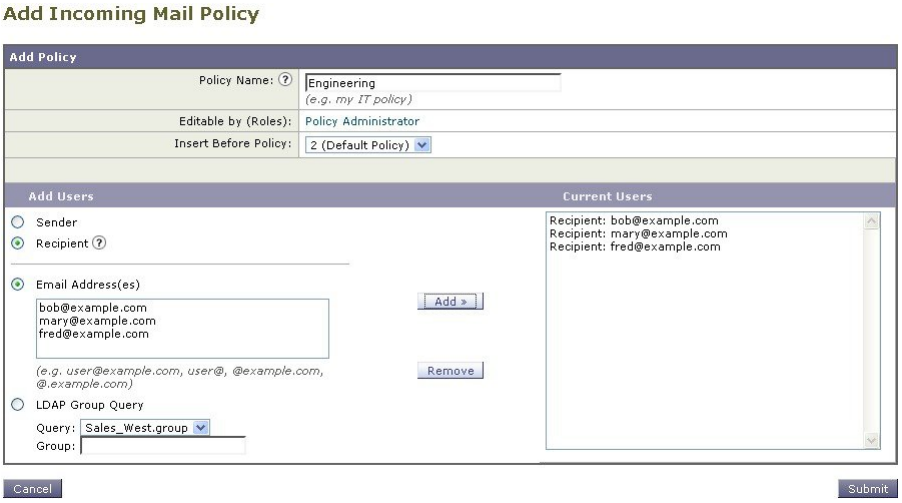
Figure 5: 新添加的策略 - 销售组



步骤 7 再次单击**添加策略 (Add Policy)** 按钮以添加另一个新策略。

在此策略中，定义了工程团队成员的各个邮件地址：

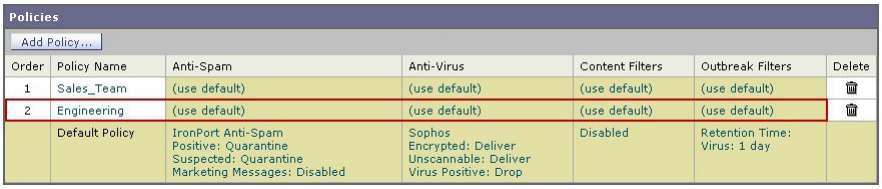
Figure 6: 为工程团队创建策略



步骤 8 为工程策略添加完用户后，单击**提交 (Submit)**。

步骤 9 确认您的更改。

Figure 7: 新添加的策略 - 工程团队



Note 此时，两个新创建的策略将应用与默认策略相同的设置。发送给任一策略用户的邮件都将匹配；但是，邮件处理设置与默认策略没有任何不同之处。因此，对于与“Sales_Group”或“Engineering”策略中的用户匹配的邮件的处理方式，与默认策略没有任何不同之处。

默认、自定义和已禁用

表底部的图例显示了特定策略单元格的颜色编码如何与为默认行定义的策略相关：

- 黄色表明策略使用与默认策略相同的设置。
- 无色（白色）表明策略使用与默认策略不同的设置。
- 灰色表明已为策略禁用了安全服务。

为不同的发件人组和收件人组创建邮件策略

在此示例部分中，将编辑在上一部分中创建的两个策略。

- 对于销售团队，将反垃圾邮件设置更改为比默认策略更积极的设置。（请参阅为传入邮件配置默认反垃圾邮件策略, on page 3。）丢弃已确认的垃圾邮件的默认策略将保留。但是，在本例中，将更改营销邮件的设置，以便不将它们发送到垃圾邮件隔离区。

  这一积极的策略可最大限度减少发送到销售团队收件箱的不需要邮件。

  有关反垃圾邮件设置的详细信息，请参阅管理垃圾邮件和灰色邮件。

- 对于工程团队，自定义“病毒爆发过滤器”(Outbreak Filters) 功能设置，使其能够修改可疑邮件中除 example.com 链接之外的 URL。病毒爆发过滤器扫描会绕开扩展名为“dwg”的附件文件。

  有关配置病毒爆发过滤器的详细信息，请参阅病毒爆发过滤器。

  为销售团队策略编辑反垃圾邮件策略步骤：

Procedure

步骤 1 单击销售策略行中与反垃圾邮件安全服务（反垃圾邮件）列对应的链接。

由于已添加该策略，因此链接名为：(use default)。

步骤 2 在反垃圾邮件安全服务页面上，将“为此策略启用反垃圾邮件扫描”(Enable Anti-Spam Scanning for This Policy) 的值从“使用默认设置”(Use Default Settings) 更改为“使用反垃圾邮件”(Use Anti-Spam service)。

此处选择“使用反垃圾邮件服务”(Use Anti-Spam service) 可以覆盖在默认策略中定义的设置。

步骤 3 在“确认的垃圾邮件设置”(Positively-Identified Spam Settings) 部分中，将“对邮件执行此操作”(Action to apply to this message) 更改为“删除”(Drop)。

步骤 4 在“疑似垃圾邮件设置”(Suspected Spam Settings) 部分中，单击**是 (Yes)** 启用疑似垃圾邮件扫描。

步骤 5 在“疑似垃圾邮件设置”(Suspected Spam Settings) 部分中，将“对邮件执行此操作”(Action to apply to this message) 更改为“垃圾邮件隔离区”(Spam Quarantine)。

Note 选择“垃圾邮件隔离区”(Spam Quarantine) 会根据在“垃圾邮件隔离区”一章中定义的设置转发邮件。

步骤 6 在“添加文本到主题”(Spam Quarantine) 字段中，单击**无 (None)**。

传送到垃圾邮件隔离区的邮件没有其他主题标记。

步骤 7 在“营销邮件设置”(Marketing Email Settings) 部分中，单击**是 (Yes)** 以启用对来自合法源的营销邮件的扫描。

步骤 8 在“对邮件执行此操作”(Action to apply to this message) 部分中，选择“垃圾邮件隔离区”(Spam Quarantine)。

步骤 9 提交并确认更改。

请注意，使用的颜色表明策略使用与默认策略不同的设置。

此时，被识别为疑似垃圾邮件并且其收件人与为销售团队策略定义的 LDAP 查询匹配的邮件都将传送到垃圾邮件隔离区。

为不同的发件人组和收件人组创建邮件策略

为工程团队策略编辑爆发过滤器设置的步骤：

Procedure

步骤 1 单击工程策略行中与爆发过滤器功能安全服务（“爆发过滤器”(Outbreak Filters) 列）列对应的链接。

由于已添加该策略，因此链接名为：（使用默认名称）。

步骤 2 在病毒爆发过滤器功能安全服务页面上，将策略的扫描设置更改为“启用病毒爆发过滤 (自定义设置)”(Enable Outbreak Filtering (Customize settings))。

此处选择“（自定义设置）”([Customize settings]) 可覆盖默认策略中定义的设置。

此外，这样做还可以启用页面其余部分的内容，从而允许选择不同的设置。

步骤 3 在页面的“绕过附件扫描”(Bypass Attachment Scanning) 部分中，在文件扩展名字段中键入 **dwg**。

文件扩展名“dwg”不在邮件网关进行附件扫描时可以通过其指纹识别的已知文件列表中。

Note 无需在三个字母组成的文件扩展名签名键入句点 (.)。

步骤 4 单击**添加扩展名 (Add Extension)** 将 .dwg 文件添加到将绕过病毒爆发过滤器功能扫描的文件扩展名列表。

步骤 5 单击**启用邮件修改 (Enable Message Modification)**。

启用邮件修改使邮件网关可以扫描有针对性的威胁（例如网络钓鱼和诈骗）以及指向可疑或恶意网站的 URL。如果用户尝试访问该网站，则设备会覆盖邮件中的链接，从而通过思科安全代理对用户进行重定向。

Note 必需在邮件策略中启用反垃圾邮件扫描，以便病毒爆发过滤器可以扫描有针对性的非病毒威胁。

步骤 6 选择用于**对未签名的邮件启用 (Enable for Unsigned Messages)**。

这允许邮件网关重写已签名邮件中的 URL。必须启用 URL 重定向功能，以便配置其他邮件修改设置以及确定为非病毒威胁的邮件在放行之前停留在隔离区中的时间长度。此示例使用的默认保留时间为 4 小时。

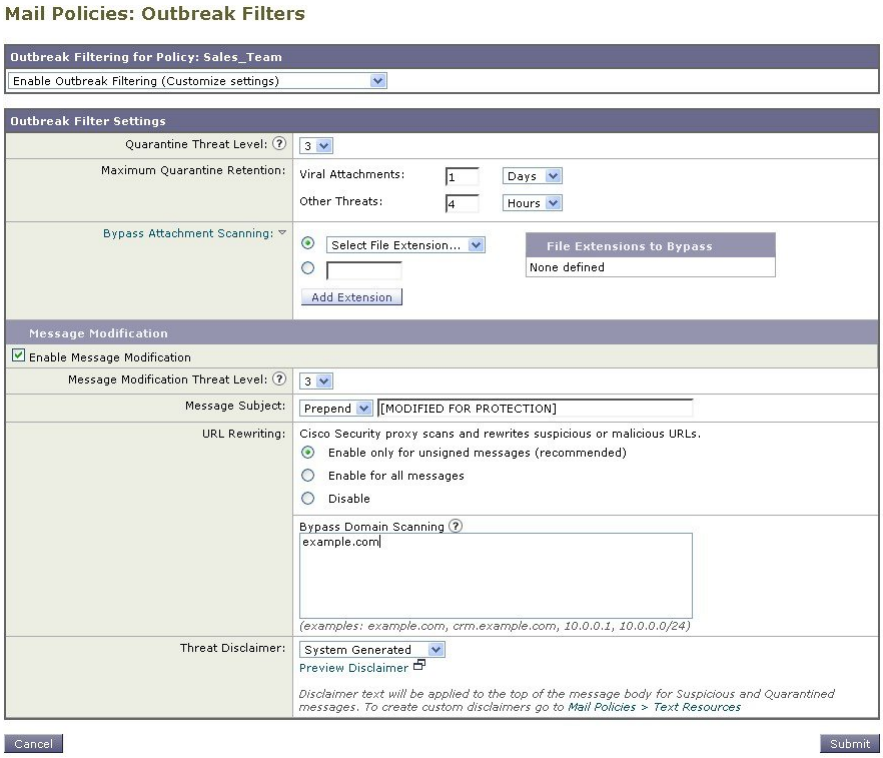
步骤 7 在**绕过域扫描 (Bypass Domain Scanning)** 字段中输入 example.com。

邮件网关不会修改指向 example.com 的链接。

步骤 8 为**威胁免责声明 (Threat Disclaimer)** 选择“系统生成”(System Generated)。

邮件网关可以在邮件正文上方插入免责声明，从而为用户提供有关邮件内容的警告。以下示例使用系统生成的威胁免责声明。

Figure 8: **爆发过滤器设置**



步骤 9 提交并确认更改。

请注意，使用的颜色表明策略使用与默认策略不同的设置。

此时，包含文件扩展名为 dwg 的附件的任何邮件（其收件人与为工程团队策略定义的收件人匹配）将绕过病毒爆发过滤器扫描并继续处理。包含指向 example.com 域的链接的邮件不会修改其链接以通过思科安全代理重定向，并且不会被视为可疑。

在邮件策略中查找发件人或收件人

使用“查找策略”(Find Policies) 按钮搜索已在“传入邮件策略”(Incoming Mail Policies) 或“传出邮件策略”(Outgoing Mail Policies) 页面的策略中定义的用户。

例如，键入 joe@example.com 并单击“查找策略”按钮将会显示结果指明哪些策略包含与该策略匹配的定义用户。

单击策略的名称会跳至“编辑策略”(Edit Policy) 页面以编辑该策略的用户。

请注意，搜索任何用户时将始终显示默认策略，因为根据定义，如果发件人或收件人与配置的任何其他策略都不匹配，则始终匹配默认策略。

托管例外

使用上面两个示例中列出的步骤，可以基于托管例外开始创建和配置策略。换句话说，评估组织的需求后，可以将策略配置为大多数邮件交由默认策略来处理。然后，可以创建适用于特定用户或用户组的其他“例外”策略，用来根据需要管理不同的策略。通过这种方式，可尽可能地减少邮件拆分，并降低因处理工作队列中的各个拆分邮件而影响系统性能的可能性。

可以根据组织或用户对垃圾邮件、病毒和策略实施的容忍度定义策略。下表概述几个示例策略。“积极”策略旨在尽可能减少到达最终用户邮箱的垃圾邮件和病毒数量。“保守”策略的目标是避免误报并防止用户丢失邮件，无论采用哪种策略。

Table 1: 积极和保守的邮件策略设置

	积极设置	保守设置
反垃圾邮件	确定为垃圾邮件：丢弃 可疑垃圾邮件：隔离 营销邮件：传送并在邮件主题前面加上“[营销]”	确定为垃圾邮件：隔离 可疑垃圾邮件：传送并在邮件主题前面加上“[可疑垃圾邮件]” 营销邮件：已禁用
防病毒	修复的邮件：传送 加密邮件：丢弃 不可扫描的邮件：丢弃 受病毒感染的邮件：丢弃	修复的邮件：传送 加密邮件：隔离 不可扫描的邮件：隔离 受病毒感染的邮件：丢弃
病毒过滤器	已启用，不允许绕过特定文件扩展名或域 对所有邮件启用邮件修改	已启用，允许绕过特定文件扩展名或域 对未签名的邮件启用邮件修改

基于内容过滤邮件

在此示例部分中，将创建要在传入邮件策略表中使用的三个新内容过滤器。所有这些内容过滤器都可由属于策略管理自定义用户角色的授权管理员进行编辑。您将创建以下内容：

1. “scan_for_confidential”

   此过滤器将扫描邮件中的“confidential”字符串。如果找到该字符串，则将邮件副本发送到邮件别名 hr@example.com，并将该邮件发送到“策略”隔离区域。

2. “no_mp3s”

   此过滤器将删除 MP3 附件，并通知收件人已删除 MP3 文件。

3. “ex_employee”

   此内容过滤器将扫描发送到特定信封收件人地址（如前员工）的邮件。如果邮件匹配，则会向邮件的发件人发送特定通知邮件，然后退回发件人的邮件。

在创建内容过滤器后，配置每个策略（包括默认策略）以在不同的组合中启用特定内容过滤器。

隔离主题中包含“Confidential”的邮件

第一个内容过滤器示例包含一个条件和两个操作。

Procedure

步骤 1 单击“邮件策略”(Mail Policies) 选项卡。

步骤 2 单击“传入内容过滤器”(Incoming Content Filters)。

步骤 3 单击**添加过滤器 (Add Filter)** 按钮。

步骤 4 在“名称”字段中，键入 scan_for_confidential 作为新过滤器的名称。

过滤器名称可以包含 ASCII 字符、数字、下划线或连字符。内容过滤器名称的第一个字符必须是字母或下划线。

步骤 5 单击**可编辑者（角色）(Editable By [Roles])** 链接，选择“策略管理员”(Policy Administrator)，然后单击**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 6 在“说明”(Description) 字段中，键入说明。例如：scan all incoming mail for the string ‘confidential’。

步骤 7 单击“添加条件”(Add Condition)。

步骤 8 选择“邮件正文”(Message Body)。

步骤 9 在“包含文本:”(Contains text:) 字段中，键入 confidential，然后单击**确定 (OK)**。

“添加内容过滤器”(Add Content Filter) 页面会显示添加的条件。

步骤 10 单击“添加操作”(Add Action)。

步骤 11 选择“副本发送到（密件抄送：）”(Select Send Copy To [Bcc:])。

步骤 12 在“邮件地址”字段中，键入 hr@example.com。

步骤 13 在“主题”字段中，键入 [message matched confidential filter]。

步骤 14 单击**确定 (OK)**。

“添加内容过滤器”(Add Content Filter) 页面会显示添加的操作。

步骤 15 单击“添加操作”(Add Action)。

步骤 16 选择“隔离区”(Quarantine)。

步骤 17 在下拉菜单中，选择“策略”(Policy) 隔离区域。

步骤 18 单击**确定 (OK)**。

“添加内容过滤器”(Add Content Filter) 页面会显示添加的第二项操作。

步骤 19 提交并确认更改。

此时，没有为任何传入邮件策略启用内容过滤器；在本例中，仅向主列表添加了一个新的内容过滤器。由于它尚未应用到任何策略，因此邮件网关处理的任何邮件都不会受此过滤器的影响。

删除邮件中的 MP3 附件

第二个内容过滤器示例不包含条件，但包含一项操作。

Procedure

步骤 1 单击**添加过滤器 (Add Filter)** 按钮。

步骤 2 在“名称”字段中，键入 no_mp3s 作为新过滤器的名称。

步骤 3 单击**可编辑者（角色）(Editable By [Roles])** 链接，选择“策略管理员”(Policy Administrator)，然后单击**确定 (OK)**。

步骤 4 在“说明”(Description) 字段中，键入说明。例如：strip all MP3 attachments。

步骤 5 单击“添加操作”(Add Action)。

步骤 6 选择“按文件信息删除附件”(Strip Attachment by File Info)。

步骤 7 选择“文件类型为”。

步骤 8 在下拉字段中，选择 -- mp3。

步骤 9 如果需要，输入替换邮件。

步骤 10 单击**确定 (OK)**。

步骤 11 提交并确认更改。

Note 在创建内容过滤器时，不需要指定条件。如果未定义条件，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。）

退回发送到前员工的邮件

第三个内容过滤器示例使用一个条件和两项操作。

Procedure

步骤 1 单击**添加过滤器 (Add Filter)** 按钮。

步骤 2 在“名称：”(Name:) 字段中，键入 **ex_employee** 作为新过滤器的名称。

步骤 3 单击**可编辑者（角色）(Editable By [Roles])** 链接，选择“策略管理员”(Policy Administrator)，然后单击**确定 (OK)**。

步骤 4 在“说明:”(Description:) 字段中，键入说明。例如：**bounce messages intended for Doug**。

步骤 5 单击**添加条件 (Add Condition)**。

步骤 6 选择**信封收件人**。

步骤 7 对于信封收件人，选择**开头为**并选择类型 **doug@**。

步骤 8 单击**确定 (OK)**。

“内容过滤器”页面将刷新，以显示添加的条件。请注意，可以创建包含前员工邮件地址 LDAP 目录。将前员工添加到该目录后，此内容过滤器将动态更新。

步骤 9 单击“添加操作”(Add Action)。

步骤 10 选择“通知”(Notify)。

步骤 11 选中发件人对应的复选框，然后在**主题**字段中键入 message bounced for ex-employee of **example.com**。

步骤 12 在“使用模板”(Use template) 部分中，选择一个通知模板。

Note 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用户界面中。例如，如果先前未通过**邮件策略 (Mail Policies) > 词典 (Dictionaries)** 页（或 CLI 中的 **dictionaryconfig** 命令）配置内容词典、通知模板和邮件免责声明，则它们不会显示为选项。有关创建词典的详细信息，请参阅内容词典。

步骤 13 单击**确定 (OK)**。

“添加内容过滤器”(Add Content Filters) 页面会显示添加的操作。

步骤 14 单击“添加操作”(Add Action)。

步骤 15 选择“退回 (最终操作)”(Bounce [Final Action])并单击“确定”(OK)。

仅可为内容过滤器指定一个最终操作。如果尝试添加多个最终操作，则 GUI 会显示错误。

添加此操作可能会导致向前员工发送邮件的发件人收到两封邮件：一个针对通知模板，另一个针对退回通知模板。

步骤 16 提交并确认更改。

将各个内容过滤器应用到不同的收件人组

在以上示例中，使用“传入内容过滤器”(Incoming Content Filters) 页面创建了三个内容过滤器。“传入内容过滤器”(Incoming Content Filters) 和“传出内容过滤器”(Outgoing Content Filters) 页面会保留可以应用于某个策略的所有可能内容过滤器的“主列表”。

Figure 9: 传入内容过滤器：创建了三个过滤器

在此示例部分中，将应用要在传入邮件策略表中使用的三个新内容过滤器。

- 默认策略将接收这三个内容过滤器。
- 工程团队不会收到 no_mp3s 过滤器。
- 销售团队将收到这些内容过滤器作为默认传入邮件策略。

默认情况下为所有收件人启用内容过滤器

单击该链接可为各个策略启用和选择内容过滤器。

Procedure

步骤 1 单击“传入邮件策略”(Incoming Mail Policies) 可返回传入邮件策略表。

该页面将刷新以显示默认策略和在为发件人和收件人组创建邮件策略, on page 4中添加的两个策略。请注意，默认情况下会为所有策略禁用内容过滤。

步骤 2 单击默认策略行中与内容过滤器安全服务（“内容过滤器”(Content Filters) 列）对应的链接。

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（在内容过滤器概述中使用“传入内容过滤器”(Incoming Content Filters) 页面创建）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从已禁用（灰色）变为已启用状态。

步骤 4 针对每个内容过滤器选中**启用 (Enable)** 复选框。

步骤 5 单击**提交 (Submit)**。

“传入邮件策略”(Incoming Mail Policies) 页面中的表会显示已为默认策略启用的过滤器的名称。

对工程团队中的收件人允许 MP3 附件

为“工程”策略禁用“no_mp3s”内容过滤器的步骤：

Procedure

步骤 1 单击工程团队策略行中与内容过滤器安全服务（“内容过滤器”[Content Filters] 列）对应的链接。

步骤 2 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])。

由于该策略使用默认值，因此将“使用默认设置”(Use Default Settings) 值更改为“是”(Yes) 时，每个过滤器的复选框将从已禁用（灰色）变为已启用状态。

步骤 3 取消选中“no_mp3s”过滤器对应的复选框。

步骤 4 单击**提交 (Submit)**。

“传入邮件策略”(Incoming Mail Policies) 页面中的表会显示已为工程策略启用的过滤器的名称。

步骤 5 确认您的更改。

What to do next

此时，与工程策略的用户列表匹配的传入邮件将不会被删除 MP3 附件；但是，其他所有传入邮件都将被删除 MP3 附件。

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。（不指定操作等同于使用 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。有关委派管理员和内容过滤器的详细信息，请参阅分配管理任务。
- 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：
  “*Warning*”

- 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。
- 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：

邮件策略和内容过滤器示例

  - 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”页面或 scanconfig 命令相同的设置，因此“整个邮件”条件不会扫描邮件的信头；选择“整个邮件”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 命令将邮件网关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”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。

Figure 10: 内容过滤器中的多个字符集

- 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。

邮件策略和内容过滤器示例