邮件策略

本章包含以下部分：

邮件策略概述

邮件安全设备通过邮件策略，执行关于发送给用户和用户发送的邮件的组织策略。这些规则集指定了组织可能不希望进入或离开您的网络的可疑、敏感或恶意内容的类型。这些内容可能包括：

- 垃圾邮件
- 合法的营销邮件
- 灰色邮件
- 病毒
- 网络钓鱼和其他有针对性的邮件攻击
- 机密企业资料
- 个人身份信息

您可以创建不同的策略来满足组织内不同用户组的不同安全需求。邮件安全设备使用这些策略中定义的规则扫描每封邮件，并根据需要执行操作保护用户。例如，策略可防止向高管传送可疑垃圾邮件，而允许向IT员工传送这些可疑垃圾邮件，但主题会进行修改以发出内容警告，或面向所有用户（“系统管理员”组中的用户除外）删除危险的可执行附件。

根据每个用户执行邮件策略的方法

过程

	命令或操作	目的
步骤 1	启用您希望邮件安全设备用于传入或传出邮件的内容扫描功能。	可以启用和配置下面一个或多个功能： • 防病毒 • 文件信誉过滤和文件分析：（仅限传入邮件） • 管理垃圾邮件和灰色邮件 • 灰色邮件检测和安全取消订阅。请参阅管理垃圾邮件和灰色邮件。 • 病毒爆发过滤器 • 防数据丢失（仅限传出邮件） • 内容过滤器
步骤 2	（可选）对于面向包含特定数据的邮件采取的操作，创建内容过滤器。	请参阅内容过滤器
步骤 3	（可选）定义一个 LDAP 组查询，以指定邮件策略规则适用的具体用户。	请参阅使用组 LDAP 查询确定收件人是否为组成员。
步骤 4	（可选）定义适用于传入或传出邮件的默认邮件策略。	请参阅配置传入或传出邮件的默认邮件策略，第 7 页。
步骤 5	定义要为其设置用户特定邮件策略的用户组。	创建传入或传出邮件策略。 有关详细信息，请参阅配置邮件策略，第 7 页。
步骤 6	配置内容安全功能和设备对邮件采取的内容过滤器操作。	为邮件策略配置不同的内容安全功能。 • 内容过滤器：将内容过滤器应用到特定用户组的邮件 • 防病毒：配置面向用户的病毒扫描操作 • 文件信誉过滤和文件分析：文件信誉过滤和文件分析： • 反垃圾邮件：定义反垃圾邮件策略 • 灰色邮件检测和安全取消订阅：配置灰色邮件检测和安全取消订用的传入邮件策略 • 病毒爆发过滤器：病毒爆发过滤器功能和病毒爆发隔离区

	命令或操作	目的
		• 防数据丢失：使用传出邮件策略向发件人和收件人指定 DLP 策略。

以不同方式处理传入和传出邮件

邮件安全设备对于邮件内容安全使用两种不同的邮件策略集。

- 传入邮件策略所适用的邮件是通过与任何侦听程序中的 ACCEPT HAT 策略匹配的连接收到的邮件。
- 传出邮件策略所适用的邮件是通过与任何监听程序中的 RELAY HAT 策略匹配的连接收到的邮件。其中包括适用 SMTP 验证的任何连接。

使用不同的策略集允许您对发送给用户和用户发送的邮件，定义不同的安全规则。在 GUI 中使用**邮件策略 > 传入邮件策略**或**传出邮件策略**页面（或在 CLI 中使用 policyconfig 命令）可管理这些策略。

注释 某些功能只能应用于传入或传出邮件策略。例如，只能对传出邮件执行防数据丢失扫描。高级恶意软件防护（文件信誉扫描和文件分析）可用于传入邮件策略和传出邮件策略。

在某些安装中，通过思科设备路由的“内部”邮件可能被视为传出，即使所有收件人的地址均为内部地址亦不例外。例如，默认情况下，对于 C170 和 C190 设备，系统设置向导仅配置一个物理以太网端口及一个侦听程序，用来接收入站邮件和中继出站邮件。

匹配用户与邮件策略

设备收到邮件时，邮件安全设备将根据其为传入还是传出邮件，尝试将每个邮件收件人和发件人与传入或传出邮件策略表中的邮件策略匹配。

匹配的依据是收件人的地址、发件人的地址或两者。

- 收件人地址与信封收件人地址匹配

  在匹配收件人地址时，输入的收件人地址是邮件管道前面部分处理之后的最终地址。例如，如果启用，默认域、LDAP 路由或伪装、别名表、域映射和邮件过滤器功能可重写信封收件人地址，并可能会影响邮件是否与邮件策略匹配。

- 发件人地址匹配：
  - 信封发件人（RFC821 MAIL FROM 地址）
  - “RFC822 From:”信头中的地址
  - “RFC822 Reply-To:”信头中的地址

地址可能基于完整的邮件地址、用户、域或部分域匹配，也可能匹配 LDAP 组成员。

相关主题

- 第一个匹配为准，第 4 页
- 策略匹配示例，第 4 页

第一个匹配为准

对照相应邮件策略表中定义的每个邮件策略，从上到下依次评估各个用户（发件人或收件人）。

对于每个用户，以第一个匹配策略为准。如果某个用户与任何特定策略都不匹配，该用户将自动匹配表的默认策略。

如果根据发件人地址进行匹配，邮件的所有剩余收件人都将与该策略匹配。（这是因为，每封邮件只能有一个发件人。）

将邮件与邮件策略匹配时，信封发件人和信封收件人的优先级高于发件人信头。如果将邮件策略配置为与特定用户匹配，则邮件将根据信封发件人和信封收件人自动归类到邮件策略中。

策略匹配示例

以下示例帮助显示如何从上到下匹配策略表。

假定下表显示的邮件安全策略表中有下列传入邮件，则传入邮件将匹配不同的策略。

表 *1:* 策略匹配示例

订单	策略名称	用户	
		发件人	收件人
1	special_people	ANY	joe@example.com ann@example.com
2	from_lawyers	@lawfirm.com	ANY
3	acquired_domains	ANY	@newdomain.com @anotherexample.com
4	engineering	ANY	PublicLDAP.ldapgroup: engineers
5	sales_team	ANY	jim@john@larry@
6	默认策略	任意	任意

相关主题

- 示例 1，第 5 页
- 示例 2，第 5 页

• 示例 3 ， 第 5 页

示例 1

发件人 bill@lawfirm.com 发送到收件人 jim@example.com 的邮件：

- 在用户描述匹配发件人 (@lawfirm.com) 和收件人（任意）时匹配策略 #2。
- 在信封发件人为 bill@lawfirm.com 时匹配策略 #2。
- 在信头发件人为 bill@lawfirm.com 但信封发件人不匹配 @lawfirm.com 时匹配策略 #5。

示例 2

发件人 joe@yahoo.com 发送的一封传入邮件包含三个收件人：john@example.com、jane@newdomain.com 和 bill@example.com：

- 收件人 jane@newdomain.com 的邮件将收到策略 #3 中定义的反垃圾邮件、防病毒、病毒爆发过滤器和内容过滤器。
- 收件人 john@example.com 的邮件将收到策略 #5 中定义的设置。
- 由于收件人 bill@example.com 与工程 LDAP 查询不匹配，所以该邮件将收到默认策略定义的设置。

本示例演示的是包含多个收件人的邮件如何进行邮件拆分。有关详细信息，请参阅邮件拆分 ， 第 5 页。

示例 3

发件人 bill@lawfirm.com（bill@lawfirm.com 用于信封发件人）将邮件发送给收件人 ann@example.com 和 larry@example.com：

- 收件人 ann@example.com 将收到策略 #1 中定义的反垃圾邮件、防病毒、病毒爆发过滤器和内容过滤器。
- 收件人 larry@example.com 将收到策略 #2 中定义的反垃圾邮件、防病毒、病毒爆发过滤器和内容过滤器，因为发件人 (@lawfirm.com) 和收件人 (ANY) 匹配。

邮件拆分

智能邮件拆分机制允许对包含多个收件人的邮件，单独应用不同的基于收件人的内容安全规则。

对照相应邮件策略表（传入或传出）中的每个策略，从上到下依次评估各个收件人。

每个与邮件匹配的策略将创建一封包含这些收件人的新邮件。此过程定义为邮件拆分：

- 如果某些收件人与不同的策略匹配，则根据这些收件人匹配的策略对他们分组，该邮件将被拆分为与匹配的策略数相同的邮件数，并为收件人设置各个适当的“拆分”。
- 如果所有收件人与同一策略匹配，则不对邮件拆分。相反，一封邮件最多可针对每个邮件收件人进行拆分。

- 然后，在邮件管道中由反垃圾邮件、防病毒、高级恶意软件防护（仅限传入邮件）、DLP 扫描（仅限传出邮件）、病毒爆发过滤器和内容过滤器单独处理每个邮件拆分。

下表说明在邮件管道中拆分邮件的位置。

<table>
<tr><td rowspan="9">工作队列</td><td>邮件过滤器
(filters)</td><td rowspan="9">邮件安全管理器扫描（每个收件人）</td><td>↓ 所有收件人的邮件</td></tr>
<tr><td>反垃圾邮件
（antispamconfig、antispamupdate）</td><td rowspan="8">邮件在经过邮件过滤器处理后、反垃圾邮件处理前立即拆分。
匹配策略 1 的所有收件人的邮件
匹配策略 2 的所有收件人的邮件
所有其他收件人的邮件（匹配默认策略）
注释 DLP 扫描只针对传出邮件执行。</td></tr>
<tr><td>防病毒
（antivirusconfig、antivirusupdate）</td></tr>
<tr><td>文件信誉和分析（高级恶意软件防护）
(ampconfig)</td></tr>
<tr><td>灰色邮件管理</td></tr>
<tr><td>内容过滤器
(policyconfig -> filters)</td></tr>
<tr><td>病毒爆发过滤器
（outbreakconfig、outbreakflush、outbreakstatus、outbreakupdate）</td></tr>
<tr><td>防数据丢失
(policyconfig)</td></tr>
</table>

注释 对于每个邮件拆分创建新 MID（邮件 ID）（例如，MID 1 将变成 MID 2 和 MID 3）。有关详细信息，请参阅“日志记录”一章。此外，跟踪功能可显示引发邮件拆分的策略。

在邮件安全管理器策略中，策略匹配和邮件拆分明显会影响管理设备中可用邮件处理的方式。

相关主题

- 托管例外，第 7 页

托管例外

由于每个拆分邮件的迭代处理都会影响性能，所以思科建议基于托管例外配置内容安全规则。换句话说，评估组织的需求并尝试配置功能，使得大多数邮件由默认邮件策略处理，少数邮件由几个其他“例外”策略处理。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。

配置邮件策略

邮件策略将不同的用户组映射到特定安全设置，例如反垃圾邮件或防病毒。

相关主题

- 配置传入或传出邮件的默认邮件策略 ，第 7 页
- 为发件人和收件人组创建邮件策略，第 8 页
- 查找适用于发件人或收件人的策略，第 11 页

配置传入或传出邮件的默认邮件策略

默认邮件策略适用于任何其他邮件策略均未涵盖的邮件。如果没有配置其他策略，默认策略则适用于所有邮件。

准备工作

了解如何定义邮件策略的各项安全服务。请参阅根据每个用户执行邮件策略的方法，第 2 页。

过程

步骤 1 根据您的要求，选择下列选项之一：

- **邮件策略 > 传入邮件策略**
- **邮件策略 (Mail Policies) > 传出邮件策略 (Outgoing Mail Policies)**。

步骤 2 单击要为默认邮件策略配置的安全服务链接。

注释 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 3 配置安全服务的设置。

步骤 4 单击**提交**。

步骤 5 提交并确认更改。

为发件人和收件人组创建邮件策略

准备工作

- 了解如何定义邮件策略的各项安全服务。请参阅根据每个用户执行邮件策略的方法，第 2 页。
- 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。有关详细信息，请参阅第一个匹配为准，第 4 页。
- （可选）定义负责管理邮件策略的授权管理员。委派管理员可以编辑策略的反垃圾邮件、防病毒、高级恶意软件防护和病毒爆发过滤器设置，为策略启用或禁用内容过滤器。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。

过程

步骤 1 依次选择**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 单击**添加策略**。

步骤 3 输入邮件策略的名称。

步骤 4 （可选）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。

步骤 5 定义策略的用户。有关定义用户的说明，请参阅为邮件策略定义发件人和收件人，第 8 页。

步骤 6 单击**提交**。

步骤 7 单击要为该邮件策略配置的内容安全服务的链接。

步骤 8 从下拉列表中，选择自定义策略的设置（而不是使用默认设置）的选项。

步骤 9 自定义安全服务设置。

步骤 10 提交并确认更改。

下一步做什么

相关主题

- 为邮件策略定义发件人和收件人，第 8 页
- 将设备配置为扫描邮件以检测垃圾邮件的方法

为邮件策略定义发件人和收件人

您可以按以下方式定义策略所适用的发件人和收件人：

- 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

注释 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。

在定义邮件策略的发件人和收件人时，请牢记：

- 必须至少指定一个发件人和收件人。
- 如果满足以下条件，则可以设置与之匹配的策略：
  - 邮件来自任意发件人、一个或多个指定发件人或非指定发件人。
  - 邮件发送给任意收件人、一个或多个指定收件人、所有指定收件人和非指定收件人。

过程

步骤 1 在**用户 (Users)** 部分下，单击**添加用户 (Add User)**。

步骤 2 定义策略的发件人。选择以下选项之一：

- **任意发件人 (Any Sender)**。如果邮件来自任何发件人，则此策略匹配。
- **以下发件人 (Following Senders)**。如果邮件来自一个或多个指定的发件人，则此策略匹配。选择此选项，并在文本框中输入发件人详细信息或选择 LDAP 组查询。
- **非以下发件人 (Following Senders are Not)**。如果邮件并非来自任何指定的发件人，则此策略匹配。选择此选项，并在文本框中输入发件人详细信息或选择 LDAP 组查询。

要了解选择上述字段时如何设置发件人条件，请参阅示例，第 10 页。

步骤 3 定义策略的收件人。选择以下选项之一：

- **任意收件人 (Any Recipient)**。如果邮件发送到任何收件人，则此策略匹配。
- **以下收件人 (Following Recipients)**。如果邮件发送到指定收件人，则此策略匹配。选择此选项，并在文本框中输入收件人详细信息或选择 LDAP 组查询。

如果邮件发送到一个或多个指定收件人或所有指定收件人，可以选择策略是否匹配。从下拉列表中选择以下选项之一：**一个或多个条件匹配时 (If one more conditions match)** 或**只有所有条件匹配时 (Only if all conditions match)**。

- **非以下收件人 (Following Recipients are Not)**。如果邮件发送到非指定收件人，则此策略匹配。选择此选项，并在文本框中输入收件人详细信息或选择 LDAP 组查询。

注释 只有从下拉列表中选择**以下收件人 (Following Recipients)** 和**只有所有条件匹配时 (Only if all conditions match)** 时，才能配置此选项。

要了解选择上述字段时如何设置收件人条件，请参阅示例，第 10 页。

步骤 4 单击**提交**。

步骤 5 查看在**用户 (Users)** 部分所选的条件。

下一步做什么

相关主题

- 为发件人和收件人组创建邮件策略， 第 8 页
- 示例， 第 10 页

示例

下表介绍选择“添加用户”(Add User) 页面的各种选项时，如何设置条件。

发件人			收件人			情况
任意发件人 (Any Sender)	**以下发件人 (Following Senders)**	**非以下发件人 (Following Senders are Not)**	**任何收件人 (Any Recipient)**	**以下收件人 (Following Recipients)**	**非以下收件人 (Following Recipients are Not)**	

已选定	-	-	-	已选定
				（默认）选择**只有所有条件匹配时 (Only if all conditions match)** 选项
				值：
				`user1@,`
				`user2@`
					-	**发件人：**任意
						收件人：
						`user1@[AND]user2@`

-	已选定
	值：
	`u1@a.com,`
	`u2@a.com`
		-	-	已选定
				（默认）选择**只有所有条件匹配时 (Only if all conditions match)** 选项
				值：
				`u1@b.com,`
				`u2@b.com`
					已选定
					值：
					`u3@b.com,`
					`u4@b.com`
						发件人：
						`u1@a.com[OR]u2@a.com`
						收件人：
						`[u1@b.com[AND]u2@b.com]`
						`[AND]`
						`[[NOT]`
						`[u3@b.com[AND]u4@b.com]]`

-	-	已选定 值： u1@a.com， u2@a.com	-	已选定 选择**一个或多个条件匹配时 (If one or more conditions match)** 选项 值： u1@b.com， u2@b.com	-	**发件人：** [NOT] [u1@a.com[OR]u2@a.com] **收件人：** u1@b.com [OR] u2@b.com

相关主题

- 为邮件策略定义发件人和收件人，第 8 页

查找适用于发件人或收件人的策略

使用“邮件策略”(Find Policies) 页面顶部的“查找策略”(Find Policies) 部分，可搜索传入或传出邮件策略中已定义的用户。

例如，键入 bob@example.com 并单击“查找策略”按钮以显示结果，表明哪些策略包含与该策略匹配的定义用户。

单击策略的名称可编辑该策略的用户。

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。

相关主题

- 托管例外，第 7 页

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。

表 *2:* 主动和保守邮件安全管理器设置

	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“[Marketing]”	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“[Suspected Spam]” 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
高级恶意软件保护（文件信誉过滤和文件分析）	未扫描的附件：丢弃 附件带恶意软件的邮件：丢弃 包含待定文件分析的邮件：隔离	未扫描的附件：传送并在邮件主题前面加上“[WARNING: ATTACHMENT UNSCANNED]”。 附件带恶意软件的邮件：丢弃 包含待定文件分析的邮件：传送并在邮件主题前面加上“[WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]”。
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

设置邮件信头的优先级

您可以设置邮件信头的优先级，以匹配设备中的传入和传出邮件。

重要事项 您可以设置设备在传入和传出消息中检查邮件信头的优先级。设备首先检查所有邮件策略的具有最高优先级的消息报头。如果没有报头与任何邮件策略匹配，设备将查找所有邮件策略的优先级列表中的下一个消息报头。如果没有邮件报头与任何邮件策略匹配，则使用默认的邮件策略设置。

过程

步骤 1 转至**邮件策略 > 邮件策略设置**。

默认情况下，“信封发件人”信头设置为优先级1。您可以单击“信封发件人”链接以更改优先级。

步骤 2 单击**添加优先级**并单击相应的信头名称（例如信头“发件人”）复选框以添加新的优先级。

步骤 3 单击**提交**和提交您的更改。