管理垃圾邮件和灰色邮件

本章包含以下部分：

反垃圾邮件扫描概述

反垃圾邮件进程会根据配置的邮件策略扫描传入（和外发）邮件。

- 一个或多个扫描引擎会通过其过滤模块扫描邮件。
- 扫描引擎为每封邮件分配得分。得分越高，邮件是垃圾邮件的可能性就越大。
- 根据得分，每封邮件将分类为以下类别之一：
  - 不是垃圾邮件
  - 疑似垃圾邮件
  - 确认的垃圾邮件
- 将根据结果采取措施。

对确认的垃圾邮件、疑似垃圾邮件或标识为不需要的营销邮件所执行的操作并不互相排斥；可以以不同方式将它们部分或全部整合在不同的传入或外发策略中，从而满足用户组的不同处理需求。还可以在同一策略中对确认的垃圾邮件与疑似垃圾邮件采用不同的操作。例如，您可能希望丢弃已确认的垃圾邮件，但隔离疑似垃圾邮件。

对于每个邮件策略，可以为一些类别指定阈值，并确定要为每个类别执行的操作。可以将不同的用户分配到不同的邮件策略，并为每个策略定义不同的扫描引擎、垃圾邮件定义阈值和垃圾邮件处理操作。

Note 有关反垃圾邮件扫描如何以及何时应用的信息，请参阅邮件管道和安全服务。

相关主题

- 反垃圾邮件解决方案 , on page 2

反垃圾邮件解决方案

邮件网关提供以下反垃圾邮件解决方案：

- IronPort 反垃圾邮件过滤, on page 3。
- 配置智能多重扫描和灰色邮件检测, on page 6.

可以在邮件网关上为这两个解决方案授予许可并启用，但是在特定邮件策略中仅可使用其中一个解决方案。可以为不同的用户组指定不同的反垃圾邮件解决方案。

如何配置邮件网关以扫描垃圾邮件

Procedure

	Command or Action	Purpose
步骤 1	在邮件网关上启用反垃圾邮件扫描。	**Note** 该表中的其余步骤对两个扫描引擎选项均适用。 如果有适用于思科 IronPort 反垃圾邮件和智能多重扫描的功能密钥，则可以在邮件网关上启用这两个解决方案。 • IronPort 反垃圾邮件过滤, on page 3 • 配置智能多重扫描和灰色邮件检测, on page 6
步骤 2	配置是在本地邮件网关上隔离垃圾邮件，还是使用思科安全邮件和 Web 管理器上的外部隔离区来隔离垃圾邮件。	• 设置本地垃圾邮件隔离区 • 使用外部垃圾邮件隔离区
步骤 3	定义要为其扫描垃圾邮件的用户组。	为发件人和收件人组创建邮件策略
步骤 4	为定义的用户组配置反垃圾邮件扫描规则。	定义反垃圾邮件策略 , on page 17

	Command or Action	Purpose
步骤 5	如果希望某些邮件跳过思科反垃圾邮件扫描，请创建使用 skip-spamcheck 操作的邮件过滤器。	绕过反垃圾邮件系统操作
步骤 6	（推荐）为每个入站邮件流量策略启用 IP 信誉服务评分，即使不根据 IP 信誉得分拒绝连接也是如此。	对于每个入站邮件流量策略，请确保打开“使用 SenderBase 进行流量控制”(Use SenderBase for Flow Control)。 请参阅使用邮件流策略定义传入邮件规则。
步骤 7	如果邮件网关不直接连接到外部发件人来接收传入邮件，而是接收通过邮件交换、邮件传输代理或网络中的其他计算机中继的邮件，请确保中继的传入邮件包括原始发件人 IP 地址。	通过传入中继确定部署中的发件人 IP 地址 , on page 30
步骤 8	避免邮件网关生成的警报和其他邮件被错误第标识为垃圾邮件。	避免垃圾邮件过滤器过滤邮件网关生成的邮件, on page 24
步骤 9	（可选）启用 URL 过滤以增强保护来抵御邮件中的恶意 URL。	启用 URL 过滤
步骤 10	测试配置。	测试反垃圾邮件, on page 39
步骤 11	（可选）配置服务更新设置（包括反垃圾邮件规则）。	默认情况下，两种反垃圾邮件解决方案的扫描规则都从思科更新服务器进行检索。 • 服务更新 • 通过代理服务器进行更新 • 配置服务器设置以下载升级和更新

IronPort 反垃圾邮件过滤

相关主题

- 试用版密钥, on page 3
- 思科反垃圾邮件：概述 , on page 4
- 配置 IronPort 反垃圾邮件扫描, on page 4

试用版密钥

您的邮件网关随附思科反垃圾邮件软件的 30 天试用版密钥。在您接受系统设置向导、“安全服务”>“IronPort 反垃圾邮件”页面（在 GUI 中）或者 systemsetup 或 antispamconfig 命令（在 CLI

中）中的许可协议后，才会启用此密钥。接受该协议后，默认情况下将为默认的传入邮件策略启用思科反垃圾邮件。此外，还会向配置的管理员地址发送警报（请参阅系统设置向导，第 2 步：系统），指明反垃圾邮件许可证将在 30 天后到期。警报将分别在到期之前 30 天、15 天、5 天和 0 天时发送。有关在30天试用期过后如何启用该功能的信息，请与思科销售代表联系。可以通过“系统管理”>“功能密钥”页面或发出 featurekey 命令来查看评估的剩余时间。（有关详细信息，请参阅功能密钥。）

思科反垃圾邮件：概述

IronPort反垃圾邮件解决了各种已知威胁，包括垃圾邮件、网络钓鱼和僵尸攻击，以及难以检测的少量短时出现的邮件威胁（如“419”骗局）。此外， IronPort 反垃圾邮件可识别新的和不断发展的混合型威胁，例如通过下载 URL 或可执行文件分发恶意内容的垃圾邮件攻击。

要识别这些威胁，IronPort反垃圾邮件会检查邮件完整上下文：邮件内容、邮件的构建方法、发件人的信誉、邮件中宣传的网站的信誉等等。IronPort反垃圾邮件将邮件和网络信誉数据的强大功能整合在一起，利用全球最大邮件和网络流量监控网络 SenderBase 的所有强大功能来即时检测新出现的攻击。

IronPort 反垃圾邮件会分析以下方面的 100,000 多个邮件属性：

- 邮件信誉 - 谁向您发送此邮件？
- 邮件内容 - 此邮件中包含什么内容？
- 邮件结构 - 此邮件是如何构建的？
- 网络信誉 - 行动号召要求您访问哪里？

分析多维关系使系统可以捕获各种威胁，同时保持准确性。例如，其内容声称来自合法金融机构，但是从消费者宽带网络中的 IP 地址发送或包含“僵尸”PC 中托管的 URL 的邮件，将被视为可疑邮件。相反，来自具有良好信誉的一家制药公司的邮件不会被标记为垃圾邮件，即使该邮件包含与垃圾邮件密切相关的词语也是如此。

相关主题

- 关于 URL 的保护和控制

配置 IronPort 反垃圾邮件扫描

Procedure

步骤 1 依次选择**安全服务 (Security Services) > IronPort 反垃圾邮件 (IronPort Anti-Spam)**。

步骤 2 如果未在系统设置向导中启用 IronPort 反垃圾邮件：

a) 单击**启用 (Enable)**。

b) 滚动到许可协议页面底部，并单击**接受 (Accept)** 以接受该协议。

步骤 3 单击**编辑全局设置 (Edit Global Settings)**。

步骤 4 选中**启用 IronPort 反垃圾邮件扫描 (Enable IronPort Anti-Spam Scanning)** 对应的复选框。

选中此复选框，将以全局方式为邮件网关启用该功能。

步骤 5 要优化邮件网关的吞吐量同时仍可扫描由垃圾邮件发件人发送的不断增大的邮件，请配置思科反垃圾邮件进行的邮件扫描的阈值。

选项	说明
邮件扫描阈值 (Message Scanning Thresholds)	**a.** 为始终扫描小于以下值的邮件**输入值** - 建议的值为 1 MB 或更小。小于始终扫描大小的邮件将进行完全扫描，“及早退出”的情况除外。如果邮件大于此大小但小于从不扫描大小，则对邮件进行部分扫描 思科建议始终扫描邮件的大小不超过 3 MB。更大的值可能导致性能降低。 **b.** 为从不扫描大于以下值的邮件**输入值** - 建议的值为 2 MB 或更小。大于此大小的邮件不会通过思科反垃圾邮件进行扫描，并且 X-IronPort-Anti-Spam-Filtered: true 信头不会添加到邮件中。 思科建议从不扫描邮件的大小不超过 10 MB。更大的值可能导致性能降低。 对于大于始终扫描大小或小于从不扫描大小的邮件，则会执行有限且更快的扫描。 **Note** 如果病毒爆发过滤器最大邮件大小大于思科反垃圾邮件的始终扫描邮件，则小于病毒爆发过滤器最大大小的邮件将进行完全扫描。
扫描一封邮件的超时时间 (Timeout for Scanning Single Message)	输入扫描邮件时等待超时的秒数。 输入 1 到 120 之间的整数。默认值为 60 秒。
扫描配置文件 (Scanning Profile)	从以下任一扫描配置文件中选择，以捕获垃圾邮件： • **正常** - 启用此选项以采用阻止垃圾邮件的平衡方法。 • **主动**-启用此选项，以更好地强调阻止垃圾邮件。启用此选项后，调整反垃圾邮件策略阈值将对垃圾邮件检测产生比正常扫描配置文件更大的影响，并且造成误报的可能性更大。 **Note** 使用新的主动扫描配置文件邮件策略时，调整反垃圾邮件阈值所产生的影响比以前更大。因此，在启用主动配置文件时，先前调整的任何反垃圾邮件策略阈值都应重置为默认设置，然后重新评估，以达到垃圾邮件捕获率与误报可能的最佳平衡点。

步骤 6 提交并确认更改。

配置智能多重扫描和灰色邮件检测

本节介绍如何配置思科智能多重扫描和灰色邮件检测以及安全取消订用。

- 配置思科智能多重扫描，第 6 页
- 配置智能多重扫描和灰色邮件检测的全局设置，第 17 页
- 管理灰色邮件，第 7 页

配置思科智能多重扫描

思科智能多重扫描合并了多个反垃圾邮件扫描引擎（包括思科反垃圾邮件），以提供多层反垃圾邮件解决方案。

当通过思科智能多重扫描进行处理时：

- 邮件首先由第三方反垃圾邮件引擎进行扫描。
- 然后，思科智能多重扫描会将邮件及第三方引擎的判定传送到到负责进行最终判定的思科反垃圾邮件。
- 在思科反垃圾邮件执行其扫描后，会向 AsyncOS 返回一个合并的多重扫描得分。
- 将第三方扫描引擎的优势与思科反垃圾邮件相结合，可捕获更多垃圾邮件，同时保持思科反垃圾邮件的较低误报率。

不能配置在思科智能多重扫描中使用的扫描引擎的顺序；思科反垃圾邮件始终最后扫描邮件，而且如果第三方引擎确定某封邮件为垃圾邮件，则思科智能多重扫描不会跳过。

使用思科智能多重扫描可能造成系统吞吐量降低。请联系您的思科支持代表获得更多信息。

注释 智能多重扫描功能密钥还可在邮件网关上启用思科反垃圾邮件，使您可以为邮件策略选择启用思科智能多重扫描或思科反垃圾邮件。

重要事项 在系统设置期间启用了思科智能多重扫描时，它会用于默认传入邮件策略，并且对全局设置使用默认值。

开始之前

激活此功能的功能密钥。请参阅功能密钥。仅当您执行了此操作后，才会看到 IronPort 智能多重扫描选项。

过程

步骤 1 选择**安全服务 (Security Services) > IMS 和灰色邮件 (IMS and Graymail)**。

步骤 2 如果未在系统设置向导中启用思科智能多重扫描：

a) 单击**启用 (Enable)**。

b) 滚动到许可协议页面底部，并单击**接受 (Accept)** 以接受该协议。

步骤 3 单击**编辑设置 (Edit Settings)**。

步骤 4 选中**启用智能多重扫描 (Enable Intelligent Multi-Scan)** 复选框，为邮件网关全局启用该功能。但是，仍然必须在邮件策略中启用按收件人的设置。

步骤 5 （可选）单击**编辑全局设置 (Edit Global Settings)** 以配置邮件扫描的阈值。有关全局设置的详细信息，请参阅配置智能多重扫描和灰色邮件检测的全局设置，第 17 页。

步骤 6 提交并确认更改。

管理灰色邮件

灰色邮件概述

灰色邮件是不适合垃圾邮件定义的邮件，例如新闻通讯、邮寄列表订用、社交媒体通知等等。这些邮件在某些时候有用，但随后价值会降低，直至最终用户不想再收到它们。

灰色邮件与垃圾邮件之间的区别是：最终用户在特定时候有意提供邮件地址（例如，最终用户订用了电子商务网站上的新闻通讯，或在某会议期间为某个组织提供了联系人详细信息），而垃圾邮件则相反，最终用户没有注册获取这些邮件。

邮件网关中的灰色邮件管理解决方案

邮件网关中的灰色邮件管理解决方案包括两个组成部分：集成的灰色邮件扫描引擎和基于云的取消订用服务。

灰色邮件管理解决方案可以让各个组织：

- 使用集成的灰色邮件引擎识别灰色邮件，并应用适当的策略控制。
- 为最终用户提供简单的机制，以便使用取消订用服务来取消订用不需要的邮件。

除了上述功能外，灰色邮件管理解决方案还可帮助组织提供：

- **面向最终用户的安全取消订用选项**。模仿取消订用选项是一种无处不在的网络钓鱼技术。因此，最终用户通常会谨慎单击未知的取消订用链接。对于这些情景，基于云的取消订用服务会提取原始取消订用 URI，检查该 URI 的信誉，然后代表最终用户执行取消订用流程。这帮助最终用户防御伪装成取消订用链接的恶意威胁。
- **最终用户的统一订用管理接口**。不同的灰色邮件发件人使用不同的布局向用户显示取消订用链接。用户必须在邮件正文中搜索取消订用链接并执行取消订用操作。不管灰色邮件发件人是谁，灰色邮件管理解决方案都会提供一个通用布局来为用户显示取消订用链接。
- **使管理员更好地了解各种灰色邮件类别**。灰色邮件引擎将每封灰色邮件分为以下三个类型（请参阅灰色邮件分类, on page 8），并且管理员可以根据这些类别设置策略控制。
- **提高了垃圾邮件效力**

相关主题

- 灰色邮件分类, on page 8

灰色邮件分类

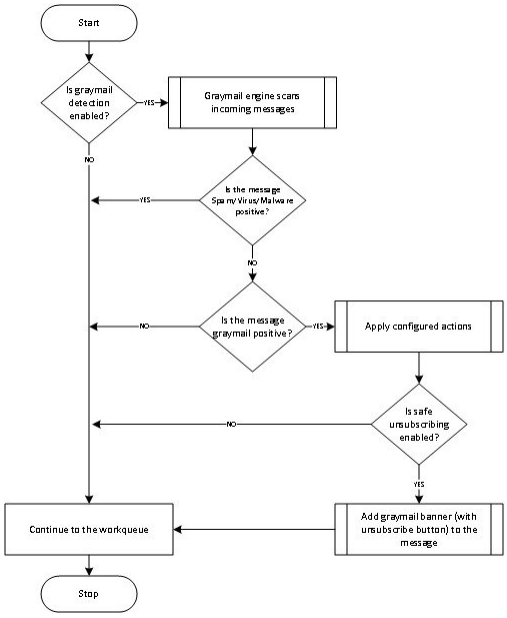
灰色邮件引擎将每封灰色邮件分类为以下类别之一：

- **市场营销邮件**。专业营销团队发送的广告邮件，例如，Amazon.com 发送的公告，其中包含有关其最近发布的产品的详细信息。
- **社交网络邮件**。来自社交网络、交友网站、论坛等等来源的通知邮件。示例包括以下来源的提醒：
  - LinkedIn，提供您可能感兴趣的职位
  - CNET 论坛，提醒您用户回复了您的帖子。
- **批量邮件**。无法识别的营销人员发送的广告邮件，例如，技术媒体公司 TechTarget 发送的新闻通讯。

灰色邮件管理解决方案工作原理

以下步骤介绍灰色邮件管理解决方案的工作流：

Figure 1: 灰色邮件管理解决方案工作流程



工作流程

Procedure

步骤 1 邮件网关接收传入邮件。

步骤 2 邮件网关检查是否已启用灰色邮件检测。如果已启用灰色邮件检测，请转至步骤 3。否则，请转至步骤 8。

步骤 3 邮件网关检查邮件的垃圾邮件、病毒或恶意软件检测是否为阳性。如果是阳性，请转至步骤 8。否则，请转至步骤 4。

步骤 4 邮件网关检查邮件是否为灰色邮件。如果邮件是灰色邮件，请转至步骤 5。否则，请转至步骤 8。

步骤 5 邮件网关会应用配置的策略操作，例如丢弃、传送、退回或隔离到垃圾邮件隔离区。

步骤 6 邮件网关会检查是否启用了安全取消订用。如果启用了安全取消订用，请转至步骤 7。否则，请转至步骤 8。

步骤 7 邮件网关会将具有取消订用按钮的横幅添加到邮件。此外，邮件网关会重写邮件正文中的现有取消订用链接。

步骤 8 邮件网关通过其邮件工作队列的后续阶段处理邮件。

What to do next

有关如何通过系统处理邮件（从接收到路由再到传送）的概述，请参阅了解邮件通道

相关主题

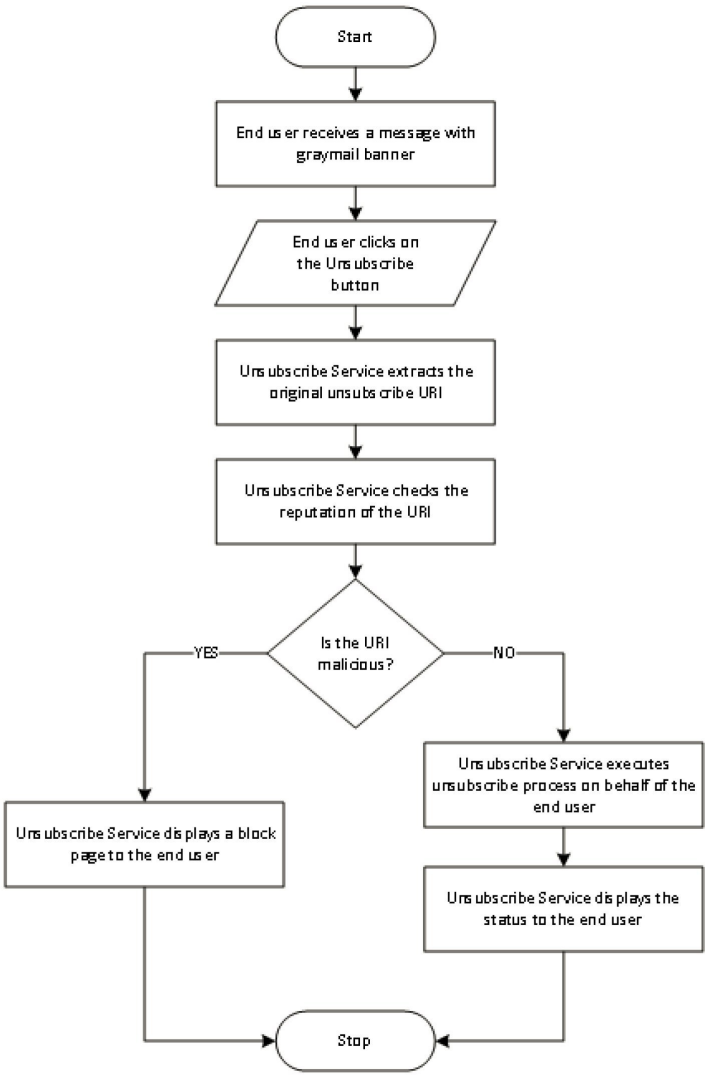
- 安全取消订用工作原理, on page 10

- 了解邮件通道

安全取消订用工作原理

以下流程图显示了安全取消订用的工作原理。

Figure 2: 安全取消订用工作流程



工作流程

Procedure

步骤 1 最终用户收到包含灰色邮件标语的邮件。

步骤 2 最终用户单击“取消订用”(Unsubscribe) 链接。

步骤 3 取消订用服务提取原始取消订用 URI。

步骤 4 取消订用服务检查 URI 的信誉。

步骤 5 根据 URI 的信誉，取消订用服务会执行以下任一操作：

- 如果 URI 是恶意的，则取消订用服务不会执行取消订用流程并为最终用户显示阻止页面。
- 如果 URI 不是恶意的，则根据 URI 类型（http 或 mailto），取消订用服务会将取消订用请求发送给灰色邮件发件人。
  - 如果请求成功，则取消订用服务会向最终用户显示“已成功取消订用”(Successfully unsubscribed) 状态。
  - 如果第一个取消订用请求失败，则取消订用服务会显示“正在进行取消订用处理”(Unsubscribe process in progress) 状态，并提供可用于跟踪取消订用状态的 URL。

    以后，最终用户可以使用此URL跟踪该状态。在第一次尝试失败后，取消订用服务会发送定期取消订用请求并且持续四小时。

    如果最终用户以后检查取消订用流程的状态，

  - 如果在四个小时的持续时间（从第一次尝试失败开始）内有一个请求成功，则取消订用服务会向最终用户显示“已成功取消订用”(Successfully unsubscribed) 状态。
  - 如果在四个小时的持续时间（从第一次尝试失败开始）内没有任何请求成功，则取消订用服务会向最终用户显示“无法取消订用”(Unable to subscribe) 状态，并提供可用于手动取消订用灰色邮件的 URL。

配置灰色邮件检测和安全取消订用

灰色邮件检测和安全取消订用的要求

- 要进行灰色邮件检测，必须全局启用反垃圾邮件扫描。这可以是 IronPort 反垃圾邮件，也可以是“智能多扫描”功能或病毒爆发过滤器。请参阅管理垃圾邮件和灰色邮件, on page 1。
- 对于安全取消订用，

- 添加安全取消订用功能键。
- 最终用户计算机必须能够直接通过互联网连接到基于云的取消订用服务。

集群配置中的灰色邮件检测和安全取消订用

可以在计算机中、组或集群级别启用灰色邮件检测和安全取消订用。

启用灰色邮件检测和安全取消订用

过程

步骤 1 选择**安全服务 (Security Services) > IMS 和灰色邮件 (IMS and Graymail)**。

步骤 2 单击**编辑灰色邮件设置 (Edit Graymail Settings)**。

步骤 3 选中**启用灰色邮件检测 (Enable Graymail Detection)**。

步骤 4 选中**启用安全取消订用 (Enable Safe Unsubscribe)**。

步骤 5 （可选）选中**启用自动更新 (Enable Automatic Updates)** 以启用引擎自动更新。

邮件网关从更新服务器获取特定引擎所需的更新。

步骤 6 单击**提交 (Submit)**。

步骤 7 （可选）单击**编辑全局设置 (Edit Global Settings)** 以配置邮件扫描的阈值。有关详细信息，请参阅配置智能多重扫描和灰色邮件检测的全局设置，第 17 页。

步骤 8 提交并确认更改。

下一步做什么

要在 CLI 中配置“灰色邮件检测”和“安全取消订用”全局设置，请使用 `imsandgraymailconfig` 命令。有关详细信息，请参阅《适用于思科安全邮件网关的 *AsyncOS CLI* 参考指南》。

配置灰色邮件检测和安全取消订用的传入邮件策略

准备工作

启用灰色邮件检测和安全取消订用, on page 12

Procedure

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

步骤 2 单击要修改的邮件策略的**灰色邮件 (Graymail)** 列中的链接。

步骤 3 根据需求，选择以下选项：

- 启用灰色邮件检测
- 启用安全取消订用

- 选择是将上述操作应用于所有邮件还是仅应用于未签名的邮件。

  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。

- 要对各种灰色邮件类别（营销邮件、社交网络邮件和批量邮件）执行的操作：
  - 删除、传送、退回或隔离（到垃圾邮件隔离区）邮件

    Note 如果计划使用安全取消订用选项，则必须将操作设置为传送或隔离。

  - 将邮件发送到备用主机
  - 修改邮件的主题
  - 添加自定义信头
  - 将邮件发送到备用信封收件人

    Note 如果要将灰色邮件检测为阳性的邮件发送到备用信封收件人，则不会添加标语。

  - 存档邮件

    Note 如果计划仅监控检测到的灰色邮件，则可以按策略启用灰色邮件检测，无需为各种灰色邮件类别配置操作。在此情况下，邮件网关不会对检测到的灰色邮件执行任何操作。

步骤 4 提交并确认更改。

What to do next

Note 还可以配置为灰色邮件检测配置外发邮件策略。请记住，在此情况下，不能配置安全取消订用。

要在 CLI 中为灰色邮件检测和安全取消订用配置策略设置，请使用 **policyconfig** 命令。有关详细信息，请参阅《适用于思科安全邮件网关的 *AsyncOS CLI* 参考指南》。

在灰色邮件扫描过程中添加的 IronPort-PHdr 信头

在以下情况下，IronPort-PHdr 信头将添加到灰色邮件引擎处理的所有邮件：

- 在邮件网关上已全局启用灰色邮件引擎。
- 为特定邮件策略启用了灰色邮件扫描。

注释 如果没有为特定邮件策略启用灰色邮件扫描，则在邮件网关上全局启用了灰色邮件引擎时，仍会将 IronPort-PHdr 信头添加到所有邮件。

IronPort-PHdr 信头包含编码的专有信息，且不可由客户解码。此信头提供有关调试灰色邮件配置问题的其他信息。

注释 如果为特定邮件策略启用了反垃圾邮件引擎或病毒爆发过滤器，则 IronPort-PHdr 信头将添加到通过特定邮件策略的所有邮件。

使用邮件过滤器绕过灰色邮件操作

如果不希望对某些邮件应用灰色邮件操作，则可以使用下列邮件过滤器绕过灰色邮件操作：

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
();
}
```

监控灰色邮件

可以使用以下报告查看有关检测到的灰色邮件的数据。

报告	包含以下灰色邮件数据	更多信息
“概述”(Overview) 页面 > “传入邮件摘要”(Incoming Mail Summary)	每种灰色邮件类别（营销 [Marketing]、社交 [Social] 和批量 [Bulk]）下的传入灰色邮件数量，以及灰色邮件总数。	“概述”(Overview) 页面

报告	包含以下灰色邮件数据	更多信息
“传入邮件”(Incoming Mail) 页面 > “按灰色邮件列出的发件人排行榜”(Top Senders by Graymail Messages)	排名靠前的灰色邮件发件人。	“传入邮件”页面
“传入邮件”(Incoming Mail) 页面 > “传入邮件详细信息”(Incoming Mail Details)	所有 IP 地址、域名或网络所有者的每种灰色邮件类别（营销 [Marketing]、社交 [Social] 和批量 [Bulk]）下的传入灰色邮件数量，以及灰色邮件总数。	
“传入邮件”(Incoming Mail) 页面 > “传入邮件详细信息”(Incoming Mail Details) > “发件人配置文件”(Sender Profile)（深入分析视图）	给定 IP 地址、域名或网络所有者的每种灰色邮件类别（营销 [Marketing]、社交 [Social] 和批量 [Bulk]）下的传入灰色邮件数量，以及灰色邮件总数。	
“内部用户”(Internal Users) 页面 > “按灰色邮件列出的用户排行榜”(Top Users by Graymail)	接收灰色邮件的排名靠前的最终用户。	“内部用户”页面
“内部用户”(Internal Users) 页面 > “用户邮件流详细信息”(User Mail Flow Details)	所有用户的每种灰色邮件类别（营销 [Marketing]、社交 [Social] 和批量 [Bulk]）下的传入灰色邮件数量，以及灰色邮件总数。	
“内部用户”(Internal Users) 页面 > “用户邮件流详细信息”(User Mail Flow Details) > “内部用户”(Internal User)（深入分析视图）	给定用户的每种灰色邮件类别（营销 [Marketing]、社交 [Social] 和批量 [Bulk]）下的传入灰色邮件数量，以及灰色邮件总数。	

如果在邮件策略的反垃圾邮件设置下启用了营销邮件扫描，在升级到 AsyncOS 9.5 或更高版本后，请牢记：

- 营销邮件的数量是在升级前后检测到的营销邮件之和。
- 灰色邮件总数不包括在升级之前检测到的营销邮件数量。
- 尝试的邮件总数还包括在升级前检测到的营销邮件数量。

更新灰色邮件规则

如果启用了服务更新，则会从思科更新服务器检索灰色邮件管理解决方案的扫描规则。但是在一些情况下（例如，已禁用自动服务更新或自动服务更新不起作用），则可能需要手动更新灰色邮件规则。

要手动更新灰色邮件规则，请执行以下任一操作：

- 在 Web 界面中，转到**安全服务 (Security Services)** > **IMS 和灰色邮件 (IMS and Graymail)** 页面，然后单击**立即更新 (Update Now)**。
- 在 CLI 中，运行 graymailupdate 命令。

要了解现有灰色邮件规则的详细信息，请参阅 Web 界面中 **IMS 和灰色邮件**页面上的**规则更新**部分，或使用 CLI 中的 graymailstatus 命令。

为最终用户自定义取消订用页面的外观

当最终用户单击取消订用链接时，取消订用服务会显示带有思科品牌的取消订用页面，指示取消订用流程的状态（请参阅安全取消订用工作原理, on page 10）。可以使用**安全服务 (Security Services)** > **阻止页面自定义 (Block Page Customization)** 来自定义取消订用页面的外观并显示贵组织的品牌（例如公司徽标、联系人信息等）。有关说明，请参阅自定义最终用户访问恶意站点时看到的通知。

最终用户安全列表

如果贵组织中的最终用户为他们自己的邮件账户配置了安全列表，则灰色邮件扫描引擎不会扫描来自安全列表中某个发件人的灰色邮件。有关安全列表的更多信息，请参阅使用安全列表和阻止列表基于发件人控制邮件发送。

查看日志

灰色邮件检测和安全取消订用信息将发布到以下日志：

- **灰色邮件引擎日志**。包含有关灰色邮件引擎、状态、配置的信息等。大多数信息处于信息或调试级别。
- **灰色邮件存档**。包含存档的邮件（经过扫描且与“存档邮件”操作关联的邮件）。日志文件为 mbox 格式。
- **邮件日志**。包含有关灰色邮件检测以及为安全取消订用添加标语的信息。大多数信息处于信息或调试级别。

对灰色邮件检测和安全取消订用进行故障排除

无法执行安全取消订用, on page 16

无法执行安全取消订用

问题

单击“取消订用”链接后，最终用户将看到以下信息：“无法取消订用...”

解决方案

如果取消订用服务无法代表最终用户执行安全取消订用，则会发生此问题。以下是取消订用服务无法执行安全取消订用的一些常见情况：

- 取消订用 URI 或 mailto 地址是错误的。
- 需要最终用户的凭证才能取消订用的网站。
- 要求最终用户通过登录邮件账户来确认取消订用请求的网站。
- 需要解析验证码而取消订用服务无法解析验证码的网站。
- 需要进行交互取消订用的网站。

最终用户可以使用在取消订用页面底部的 URL 来手动取消订用。

配置智能多重扫描和灰色邮件检测的全局设置

要优化邮件网关的吞吐量，您可以配置通过思科智能多重扫描和灰色邮件扫描邮件的阈值和超时设置。这些全局配置设置对思科智能多重扫描和灰色邮件配置通用。

1. 选择**安全服务 (Security Services)** > **IMS 和灰色邮件 (IMS and Graymail)**
2. 单击**编辑全局设置 (Edit Global Settings)**。
3. 选择用于通过思科智能多重扫描进行扫描的阈值。

   默认值为：

   - 始终扫描 512K 或更小的邮件。
   -

     注释 此设置不适用于灰色邮件检测和安全取消订用。
   - 绝不扫描 1M 或更大的邮件。
4. 输入扫描邮件时等待超时的秒数。

   当指定秒数时，输入介于 1 和 120 之间的整数。默认值为 60 秒。

   大多数用户不必更改要扫描的最大邮件大小或超时值。也就是说，可以通过降低最大邮件大小设置来优化邮件网关的吞吐量。
5. 提交更改。

定义反垃圾邮件策略

对于每个邮件策略，指定设置以确定哪些邮件被视为垃圾邮件，以及对这些邮件执行什么操作。此外，还指定哪个引擎将扫描该策略应用到的邮件。

可以为默认传入和传出邮件策略配置不同的设置。如果需要为不同的用户使用不同的反垃圾邮件策略，请使用具有不同反垃圾邮件设置的多个邮件策略。每个策略仅可启用一个反垃圾邮件解决方案；不能对同一策略同时启用两个解决方案。

准备工作

- 完成如何配置邮件网关以扫描垃圾邮件, on page 2表中此步骤之前的所有步骤。
- 熟悉以下内容：
  - 了解确认和疑似垃圾邮件阈值, on page 20
  - 配置示例：针对肯定是垃圾邮件与疑似垃圾邮件的操作 , on page 20
  - 来自合法源的不需要的营销邮件, on page 21
  - 如果启用了多个反垃圾邮件解决方案：在不同的邮件策略中启用不同的反垃圾邮件扫描引擎：配置示例 , on page 22
  - 在反垃圾邮件扫描期间添加的信头 , on page 24

- 如果将垃圾邮件存档到“反垃圾邮件存档”(Anti-Spam Archive) 日志中，另请参阅日志记录。
- 如果要将邮件发送到备用邮件主机，另请参阅修改传送主机操作。

Procedure

步骤 1 导航到**邮件策略 (Mail Policies) > 传入邮件策略 (Incoming Mail Policies)** 页面。

或

步骤 2 导航到**邮件策略 (Mail Policies) > 传出邮件策略 (Outgoing Mail Policies)** 页面。

步骤 3 单击邮件策略的**反垃圾邮件 (Anti-Spam)** 列下与任意邮件策略对应的链接。

步骤 4 在**为此策略启用反垃圾邮件扫描 (Enable Anti-Spam Scanning for This Policy)** 部分中，选择要用于策略的反垃圾邮件解决方案。

所显示的选项取决于已启用的反垃圾邮件扫描解决方案。

对于默认策略以外的邮件策略：如果使用默认策略中的设置，则该页面中的其他所有选项将被禁用。

还可以为此邮件策略一起禁用反垃圾邮件扫描。

步骤 5 配置针对已确认的垃圾邮件、疑似垃圾邮件和营销邮件的设置。

选项	说明
启用疑似垃圾邮件扫描 (Enable Suspected Spam Scanning) 启用营销邮件扫描	选择一个选项。 如果启用了反垃圾邮件扫描，则已确认的垃圾邮件扫描始终处于启用状态。
对邮件执行此操作 (Apply This Action to Message)	选择要对已确认的垃圾邮件、疑似垃圾邮件或不需要的营销邮件执行的整体操作： • 传送 • 删除 • 退回 • 隔离
（可选）发送到备用主机 (Send to Alternate Host)	可以将确认的垃圾邮件发送到备用目标邮件主机（除 SMTP 路由或 DNS 中所列的主机之外的一台邮件服务器）。 输入 IP 地址或主机名。如果输入主机名，将首先查询其邮件交换 (MX)。如果不存在，将使用 DNS 服务器上的 A 记录（与 SMTP 路由一样）。 如果要重定向邮件，例如重定向到沙盒邮件服务器进行进一步检查，请使用此选项。 有关其他重要信息，请参阅修改传送主机操作。

选项	说明
添加文本到主题 (Add Text to Subject)	可以通过预置或附加特定文本字符串来更改已识别邮件的主题中的文本，从而帮助用户更轻松地识别和排序垃圾邮件以及不需要的营销邮件。 **Note** 在此字段中未忽略空白区域。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，如果要进行预置，则添加文本 `[Spam]` 以及一些结尾空格。 “添加文本到主题”(Add Text to Subject) 字段只接受 US-ASCII 字符。
高级选项（用于自定义信头和邮件传送）	
（可选）添加自定义信头 (Add Custom Header)	可以将自定义信头添加到识别的邮件。 单击**高级 (Advanced)** 并定义信头和值。 可以将自定义信头与内容过滤器结合使用来执行操作，例如重定向疑似垃圾邮件中的URL，以便它们通过思科网络安全代理服务。有关信息，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 , on page 21。
（可选）发送到备选信封收件人 (Send to an Alternate Envelope Recipient)	可以将已识别的邮件发送到备用信封收件人地址。 单击**高级 (Advanced)** 并定义备用地址。 例如，可以将确认的垃圾邮件的邮件路由到管理员的邮箱以进行后续检查。如果是多收件人邮件，则仅将一个副本发送到备用收件人。
存档邮件 (Archive Message)	您可以将确认的垃圾邮件存档到“反垃圾邮件存档”日志。日志文件为 mbox 格式。
垃圾邮件阈值 (Spam Thresholds)	使用默认阈值，或为确认的垃圾邮件输入一个阈值并为疑似垃圾邮件输入一个值。

步骤 6 提交并确认更改。

What to do next

如果为传出邮件启用了反垃圾邮件扫描，请检查相关主机访问表的反垃圾邮件设置，尤其是对于专用侦听程序。请参阅使用邮件流策略定义邮件发件人的访问规则。

相关主题

- 如何配置邮件网关以扫描垃圾邮件, on page 2
- 了解确认和疑似垃圾邮件阈值, on page 20
- 配置示例：针对肯定是垃圾邮件与疑似垃圾邮件的操作 , on page 20
- 来自合法源的不需要的营销邮件, on page 21

- 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 , on page 21
- 在不同的邮件策略中启用不同的反垃圾邮件扫描引擎：配置示例 , on page 22

了解确认和疑似垃圾邮件阈值

当评估邮件是否为垃圾邮件时，两种反垃圾邮件扫描解决方案会应用数千条规则，以便计算邮件的总体垃圾邮件得分。然后，将得分与适用的邮件策略中指定的阈值进行比较，以确定是否将邮件视为垃圾邮件。

为实现最高的准确性，默认情况下确认的垃圾邮件的阈值非常高：得分介于 90 和 100 之间的邮件被视为确认的垃圾邮件。可疑垃圾邮件的默认阈值为 50。

- 得分低于疑似垃圾邮件阈值的邮件将被视为合法。
- 高于疑似邮件阈值但低于确认的垃圾邮件阈值的指定将被视为疑似垃圾邮件。

可以配置反垃圾邮件解决方案，以通过在每个邮件策略中自定义确认的垃圾邮件和疑似垃圾邮件的阈值来反应贵组织对于垃圾邮件的容忍程度。

可以将确认的垃圾邮件的阈值更改为介于 50 和 99 之间的值。可以将疑似垃圾邮件的阈值更改为介于 25 和为确认的垃圾邮件指定的值之间的任何值。

如果更改阈值：

- 指定较小的数（更积极的配置）会将更多邮件识别为垃圾邮件，并且可能产生更多误报情况。这会降低用户看到垃圾邮件的风险，但会提高将合法邮件标记为垃圾邮件的风险。
- 指定较高的数量（一种较保守的配置）会将较少的邮件识别为垃圾邮件，并且可能传送更多垃圾邮件。这会提高用户看到垃圾邮件的风险，但会降低将合法邮件扣留为垃圾邮件的风险。理想情况下，如果设置正确，邮件主题会将邮件确定为很可能是垃圾邮件，并传送该邮件。

可以定义一个对确认的垃圾邮件和疑似垃圾邮件执行的单独操作。例如，您可能希望丢弃“已确认的”垃圾邮件，但隔离“疑似”垃圾邮件。

相关主题

- 反垃圾邮件解决方案 , on page 2
- 配置示例：针对肯定是垃圾邮件与疑似垃圾邮件的操作 , on page 20

配置示例：针对肯定是垃圾邮件与疑似垃圾邮件的操作

垃圾邮件	操作示例 （积极）	操作示例 （保守）
肯定是垃圾邮件	丢弃	• 在邮件主题中添加“`[Positive Spam]`”并传送，或 • 隔离

垃圾邮件	操作示例 （积极）	操作示例 （保守）
疑似垃圾邮件	在邮件主题中添加“[Suspected Spam]”并传送，或	在邮件主题中添加“[Suspected Spam]”并传送，或

积极策略的示例仅标记疑似垃圾邮件，同时丢弃确认的垃圾邮件。管理员和最终用户可以检查传入邮件的主题行以了解误报情况，而且管理员可以在必要时调整疑似垃圾邮件阈值。

在保守策略示例中，已确认的垃圾邮件和疑似垃圾邮件通过更改后的主题传送。用户可以删除疑似垃圾邮件和已确认的垃圾邮件。此方法比第一种方法更加保守。

有关邮件策略中积极策略和保守策略的深入讨论，请参阅托管例外。

来自合法源的不需要的营销邮件

如果在反垃圾邮件设置下为某个邮件策略配置了营销邮件设置，则升级到适用于邮件的 AsyncOS 9.5 后，反垃圾邮件设置下的营销邮件设置将移至同一策略的灰色邮件设置下。请参阅管理垃圾邮件和灰色邮件, on page 1。

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

可以重写疑似垃圾邮件中的 URL，以便在收件人单击邮件中的链接时，将通过思科网络安全代理服务（该服务会评估单击时的网站安全性，并阻止访问已知的恶意网站）路由请求。

准备工作

启用 URL 过滤功能及其前提条件。请参阅设置 URL 过滤。

Procedure

步骤 1 将自定义信头应用到疑似垃圾邮件：

a) 依次选择**邮件策略 (Mail Policies) > 传入邮件策略 (Incoming Mail Policies)**。
b) 单击**反垃圾邮件 (Anti-Spam)** 列中与某个策略（如默认策略）对应的链接。
c) 在疑似垃圾邮件设置部分中，启用了疑似垃圾邮件扫描。
d) 单击**高级 (Advanced)** 以显示“添加自定义信头”(Add Custom Header) 选项。
e) 添加自定义标题，如 url_redirect。
f) 提交并确认更改。

步骤 2 创建内容过滤器以重定向具有自定义信头的邮件中的 URL：

a) 依次选择**邮件策略 (Mail Policies) > 传入内容过滤器 (Incoming Content Filters)**。
b) 单击**添加过滤器 (Add Filter)**。

c) 将过滤器命名为 url_redirect。
d) 单击**添加条件 (Add Condition)**。
e) 单击**其他信头 (Other Header)**。
f) 输入信头名称：url_redirect。

确保其与您创建的上述信头完全匹配。

g) 选择**存在信头 (Header exists)**。
h) 单击**确定 (OK)**。
i) 单击**添加操作 (Add Action)**。
j) 单击 **URL 类别 (URL Category)**。
k) 选择**可用类别 (Available Categories)** 中的所有类别，并将它们添加到**选定的类别 (Selected Categories)**。
l) 对于针对 URL 的操作，选择**重定向到思科安全代理 (Redirect to Cisco Security Proxy)**。
m) 单击**确定 (OK)**。

步骤 3 将内容过滤器添加到邮件策略。

a) 依次选择**邮件策略 (Mail Policies) > 传入邮件策略 (Incoming Mail Policies)**。
b) 单击**内容过滤器 (Content Filters)** 列中与先前在此过程中选择的策略对应的链接。
a) 如果尚未选择，请选择**启用内容过滤器 (Enable Content Filters)**。
b) 选中此复选框可启用 **url_filtering** 内容过滤器。
c) 提交并确认更改。

What to do next

相关主题

- 重定向 URL
- 内容过滤器

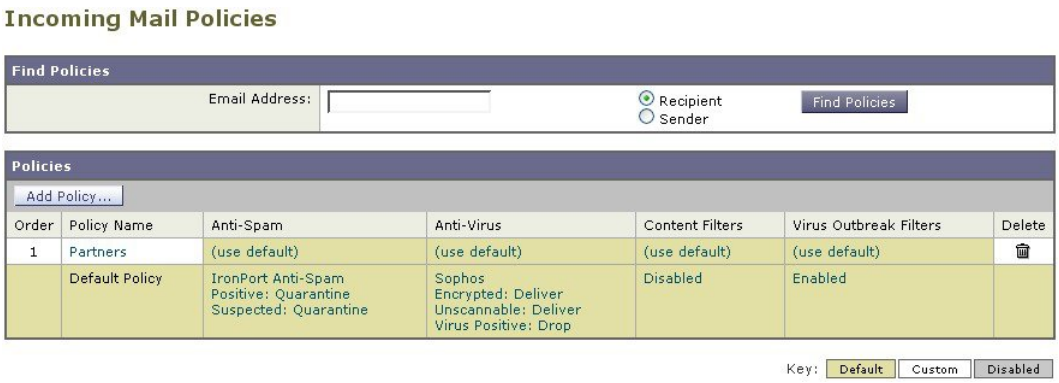
在不同的邮件策略中启用不同的反垃圾邮件扫描引擎：配置示例

当使用“系统设置向导”（或 CLI 中的 systemsetup 命令）时，系统会提供选项用于启用思科智能多重扫描或思科反垃圾邮件引擎。在系统设置期间，不能同时启用两者，但是，在系统设置完成后，可以使用“安全服务”(Security Services) 菜单启用未选择的反垃圾邮件解决方案。

设置了系统后，可以通过“**邮件策略**”>“**传入邮件策略**”页面为传入邮件策略配置反垃圾邮件扫描解决方案。（通常，会为外发邮件策略禁用反垃圾邮件扫描。）甚至可以为某个策略禁用反垃圾邮件扫描。

在本例中，默认邮件策略和“合作伙伴”(Partners) 策略使用思科反垃圾邮件扫描引擎隔已确认垃圾邮件和疑似垃圾邮件。

Figure 3: 邮件策略 - 按收件人的反垃圾邮件引擎

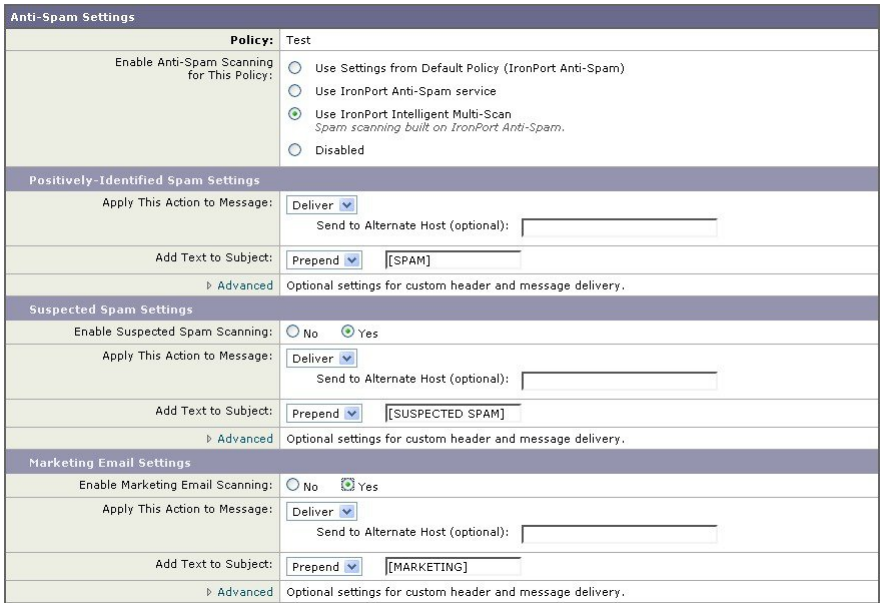


要将“合作伙伴”(Partners) 策略更改为使用思科智能多重扫描，并扫描不需要的营销邮件，请单击“反垃圾邮件”(Anti-Spam) 列中与“合作伙伴”(Partners) 行（“use default”）对应的条目。

为扫描引擎选择思科智能多重扫描，并选择“是”(Yes) 启用对不需要的营销邮件的检测。为不需要的营销邮件检测使用默认设置。

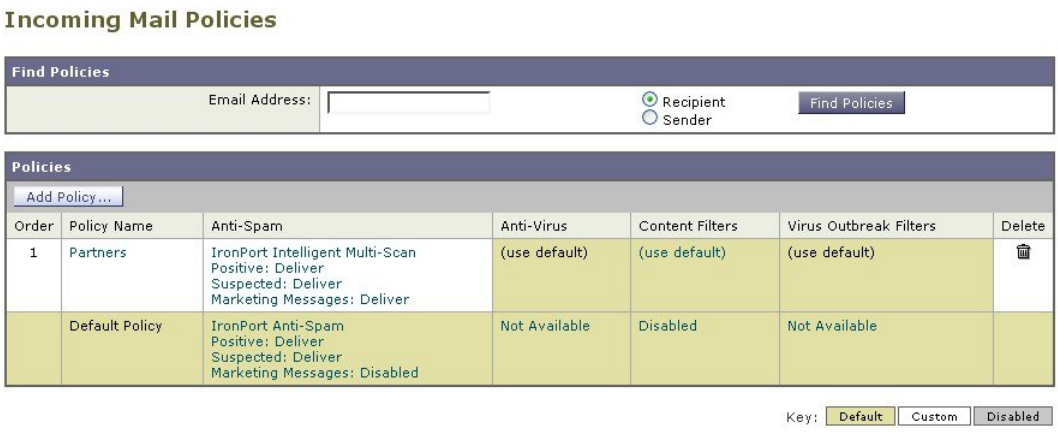
下图显示了在某个策略中启用的思科智能多重扫描和不需要的营销邮件检测。

Figure 4: 邮件策略 - 启用思科智能多重扫描



确认并提交更改后，邮件策略将如下所示：

Figure 5: 邮件策略 - 在策略中启用智能多重扫描



避免垃圾邮件过滤器过滤邮件网关生成的邮件

由于邮件网关自动发送的邮件（例如邮件警报和计划报告）可能包含使其错误地被标识为垃圾邮件的 URL 或其他信息，因此应执行以下步骤来确保其顺利传送：

在绕开反垃圾邮件扫描的传入邮件策略中包含这些邮件的发件人。请参阅为发件人和收件人组创建邮件策略和绕过反垃圾邮件系统操作。

在反垃圾邮件扫描期间添加的信头

- 如果为邮件策略启用了任何一个反垃圾邮件扫描引擎，则通过该策略处理的每封邮件都会添加下列信头：

  X-IronPort-Anti-Spam-Filtered: true

  X-IronPort-Anti-Spam-Result

  第二个信头包含允许思科支持识别用于扫描邮件的规则和引擎版本的信息。结果信息是已编码的专有信息，并且客户无法解码。

- 思科智能多重扫描还从第三方反垃圾邮件扫描引擎添加信头。
- 可以为指定的邮件策略定义要添加到所有邮件（已确认的垃圾邮件、疑似垃圾邮件或已识别为不需要的营销邮件）的其他自定义信头。请参阅定义反垃圾邮件策略 , on page 17。

相关主题

- 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 , on page 21

向思科报告分类错误的邮件

似乎分类错误的邮件可以报告给思科进行分析。报告的邮件用于提高产品的准确性和有效性。

您可以报告属于以下类别的分类错误的邮件：

- 错过的垃圾邮件
- 标记为垃圾邮件但不是垃圾邮件的邮件
- 错过的营销邮件
- 标记为营销邮件但不是营销邮件的邮件
- 错过的网络钓鱼邮件

相关主题

- 如何向思科报告分类不正确的邮件, on page 25
- 跟踪邮件提交的方法, on page 29

如何向思科报告分类不正确的邮件

准备工作

在开始向思科报告分类错误的邮件之前，必须执行以下步骤。仅执行此步骤一次。

过程

步骤 1 通过以下任何方式之一均可在思科 Talos 邮件状态门户上注册为管理员：

注释　思科 Talos 邮件状态门户是一个基于 Web 的工具，它允许邮件管理员查看和跟踪门户上的邮件提交。

- 当您是组织中访问该门户的第一个管理员时，进行注册的步骤：
  1. 使用思科凭证登录思科 Talos 邮件状态门户 (https://talosintelligence.com/email_status_portal)。
  2. 单击**管理帐户 (Manage Account)**。
  3. 单击**添加域 (Add Domain)**。
  4. 在**域 (Domain)** 字段中输入组织的域名，以便向门户注册您的域。

     注释　确保输入了有效的域名，例如，`example.com` 是以下电子邮件地址中的域名：`user@example.com`。如果组织中有多个域，请确保添加所有域。
  5. 如果您是在步骤“d”中输入的域的所有者，请选中**我拥有此域 (I own this domain)** 复选框。

     注释　如果未选中“我拥有此域”(I own this domain) 复选框，则您只会拥有域查看访问权限。有关详细信息，请参阅“思科 Talos 邮件状态门户帮助”页面，网址为：https://talosintelligence.com/tickets/email_submissions/help
  6. 单击**提交 (Submit)**。

     单击“提交”(Submit) 后，系统会自动将一封包含 6 位数字符验证码的邮件发送到 `postmaster@domain.com`（其中 domain.com 是您在步骤“d”中输入的域），以便确认域的所有权。

如果您的组织未使用 postmaster@domain.com 或您的管理员无权访问 postmaster 邮箱，请创建一个邮件过滤器（在所有邮件网关上），从而将从 SubmissionPortal@cisco.com 发送到 postmaster@domain.com 的邮件重定向到其他邮件地址。以下为邮件过滤器示例：

```
redirect_postmaster: if (rcpt-to == "postmaster@domain.com") AND (mail-from ==
"^SubmissionPortal@cisco.com$") { alt-rcpt-to ("admin@domain.com"); }
```

7. 在**域所有权验证代码 (Domain Ownership Verification Code)** 对话框中输入 6 位数字符验证代码，以便确认域的所有权。
8. 单击**提交验证代码 (Submit Verification Code)**。

   单击“提交验证代码”(Submit Verification Code) 按钮后，您就会自动获得管理员访问权限。系统会自动生成一个注册 ID，在门户的“管理帐户”部分中可以查看该 ID。您可以将注册 ID 用于组织中的所有邮件网关。

   注释 注册 ID 是标识从属于特定组织的思科邮件安全网关进行的提交的唯一标识符。

- 当您组织中的某个管理员已在该门户上注册时，进行注册的步骤：

1. 使用思科凭证登录思科 Talos 邮件状态门户 (https://talosintelligence.com/email_status_portal)。
2. 单击**管理帐户 (Manage Account)**。
3. 单击**添加域 (Add Domain)**。
4. 在**域 (Domain)** 字段中输入组织的域名，以便向门户注册您的域。

   注释 确保输入了有效的域名，例如，example.com 是以下电子邮件地址中的域名：user@example.com。如果组织中有多个域，请确保添加所有域。

5. 单击**提交 (Submit)**。

单击“提交”(Submit) 后，将向已在门户上注册的管理员发送邮件通知。该管理员必须登录到门户，然后单击“管理帐户”(Manage Accounts) 的“权限请求”(Permission Requests) 部分中的**批准 (Approve)**，以批准您的注册请求。

在注册请求获批之后，系统会自动生成一个注册 ID，在门户的“管理帐户”部分中可以查看该 ID。您可以将注册 ID 用于组织中的所有邮件网关。

注释 注册 ID 是标识从属于特定组织的思科邮件安全网关进行的提交的唯一标识符。

步骤 2 为组织中的所有邮件网关添加从思科 Talos 邮件状态门户生成的注册 ID。

1. 使用 Web 界面登录到您的邮件网关。
2. 转到**系统管理 (System Administration)** > **思科 Talos 邮件状态门户注册 (Cisco Talos Email Status Portal Registration)**。
3. 如果您的邮件网关是集群的一部分，请将该模式设置为集群级别。
4. 单击**设置注册 ID**。
5. 在**注册 ID (Registration ID)** 字段中输入从思科 Talos 邮件状态门户获取的注册 ID。

6. 提交并确认更改。
7. 如果您的邮件网关不是集群的一部分，则必须对组织中的所有邮件网关重复第 1 步到第 6 步。

也可以使用 CLI 中的 `portalregistrationconfig` 命令来设置注册 ID。

如何向思科报告分类不正确的邮件

有关详情，请参阅：

- 如何在https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214133-how-to-submit-email-messages-to-cisco.html#anc5中将邮件提交至思科文档。
- “思科 Talos 邮件状态门户帮助”页面位于 https://talosintelligence.com/tickets/email_submissions/help。

Procedure

步骤 1 执行 如何向思科报告分类不正确的邮件, on page 25 的**准备工作**部分提到的步骤。

步骤 2 使用以下方法之一向思科报告分类不正确的邮件：

- 使用思科邮件安全插件, on page 27
- 将分类错误的邮件作为附件进行转发, on page 28

向思科报告分类错误的邮件后，您将根据在门户的“管理帐户”(Manage Account) 部分的“邮件通知和报告”(Email Notification and Reports) 按钮下选择的选项收到邮件通知。

Note 默认情况下，“邮件通知和报告”(Email Notification and Reports) 按钮下的“我的提交通知”(My Submission Notifications) 和“我的提交报告”(My Submission Reports) 选项设置为关闭。有关详细信息，请参阅“思科 Talos 邮件状态门户帮助”页面，网址为：https://talosintelligence.com/tickets/email_submissions/help

What to do next

跟踪邮件提交的方法, on page 29

使用思科邮件安全插件

思科邮件安全插件是一种工具，允许用户（邮件管理员和最终用户）使用 Microsoft Outlook 向思科报告分类错误的邮件。当您将此插件部署为 Microsoft Outlook 的一部分时，将向 Microsoft Outlook 的 Web 界面添加一个报告菜单。您可以使用该插件菜单报告分类错误的邮件。

更多信息

- 您可以从以下页面下载思科邮件安全插件：https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=284900944&flowid=41782&softwareid=283090986。
- 有关详细信息，请参阅《思科邮件安全插件管理员指南》http://www.cisco.com/c/en/us/support/security/email-encryption/products-user-guide-list.html。

将分类错误的邮件作为附件进行转发

根据邮件的类别，可以将每个分类不正确的邮件作为 RFC 822 附件转发到下表中所示的地址：

邮件提交	定义	提交方法	用户提交注意事项
垃圾邮件/网络钓鱼	未经请求和不需要。垃圾邮件/网络钓鱼从来都是不合法的，也可能是恶意的（网络钓鱼、病毒、恶意软件、诈骗等）	spam@access。 ironport.com phish@access。 ironport.com virus@access。 ironport.com Outlook 插件“垃圾邮件”(Spam)、“网络钓鱼”(Phish) 或“病毒”(Virus) 按钮	已传送到用户的收件箱，但用户将邮件视为垃圾邮件或网络钓鱼。 被检测为垃圾邮件，但用户认为邮件是合法的。
Legitimate	合法（正常）邮件，而非垃圾邮件。也称为“Ham”。	ham@access。 ironport.com Outlook 插件“非垃圾邮件”(Not Spam) 按钮	未被检测为营销/灰色邮件的营销/灰色邮件。
市场营销/灰色邮件	营销是属于商业批量邮件的合法（非垃圾邮件）邮件。通常基于订用，有时是不需要的。 用户可能会有意或无意地向发件人请求邮件。例如，在会议上刷徽章或进行在线购买等。基于合法订用的营销邮件将具有有效的取消订用机制。 灰色邮件是一个更广泛的类别，包括营销以及其他合法的批量邮件。	ads@access。 ironport.com Outlook 插件“营销”(Marketing) 按钮	被检测为垃圾邮件，但用户认为邮件是合法的

邮件提交	定义	提交方法	用户提交注意事项
非营销/灰色邮件	非批量且不基于订用的合法邮件（非垃圾邮件）。通常是个人对个人和/或事务性邮件。	not_ads@access。ironport.com	检测为营销/灰色邮件，但用户认为该邮件是事务性邮件，或者不是营销/灰色邮件。

如果使用下列邮件程序之一转发邮件，可以获得最佳效果：

- Apple 邮件
- Microsoft Outlook for Mac
- Microsoft Outlook Web App
- Mozilla Thunderbird

注意 如果您使用的是适用于 Microsoft Windows 的 Microsoft Outlook 2010、2013 或 2016，则必须使用思科邮件安全插件或 Microsoft Outlook Web App 来报告分类不正确的邮件。这是因为 Outlook for Windows 可能无法转发所需的信头保持不变的邮件。此外，仅当您可以将原始邮件作为附件转发时，才使用移动平台。

跟踪邮件提交的方法

收到含提交详细信息的邮件通知后，可以在思科 Talos 邮件状态门户网站上查看和跟踪邮件提交。

过程

步骤 1 使用思科凭证登录思科 Talos 邮件状态门户 (https://talosintelligence.com/email_status_portal)。

步骤 2 单击 思科 Talos 邮件状态门户上的**提交 (Submissions)**。

步骤 3 单击**过滤器选项 (Filter Options)** 并选择适当的过滤器选项。

步骤 4 （可选）单击日历按钮以选择特定日期。

下一步做什么

有关详细信息，请参阅思科 Talos 邮件状态门户帮助页面，网址为 https://talosintelligence.com/tickets/email_submissions/help。

通过传入中继确定部署中的发件人 IP 地址

如果一个或多个邮件交换/传输代理（MX 或 MTA）、过滤服务器等位于网络边缘，且在邮件网关与发送传入邮件的外部计算机之间，则邮件网关无法确定发送计算机的 IP 地址。相反，邮件看似来自本地 MX/MTA。但是，IronPort 反垃圾邮件和思科智能多扫描（使用 IP 信誉服务）取决于外部发件人的准确 IP 地址。

解决方案是将邮件网关配置为使用传入中继。指定连接到邮件网关的所有内部 MX/MTA 的名称和 IP 地址，以及用于存储来源 IP 地址的信头。

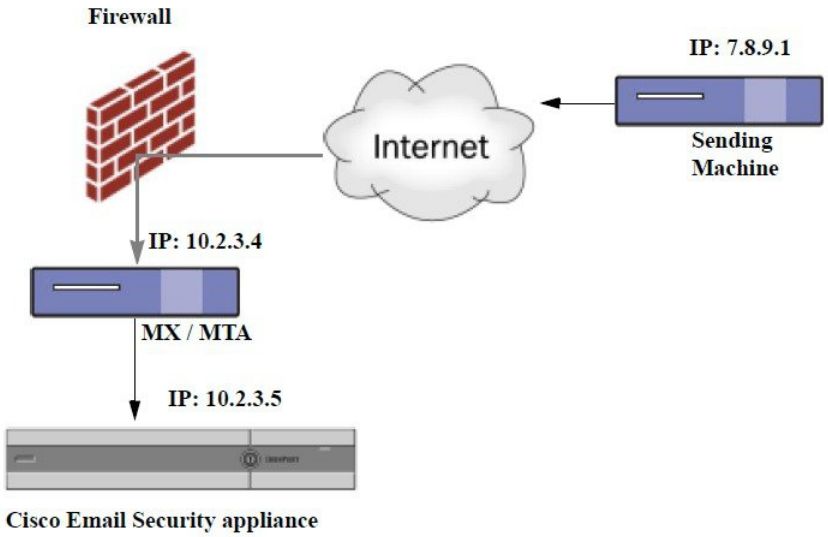
相关主题

- 具有传入中继的环境示例 , on page 30
- 配置邮件网关以使用传入中继, on page 31
- 传入中继如何影响功能 , on page 36
- 配置日志以指定要使用的信头 , on page 38

具有传入中继的环境示例

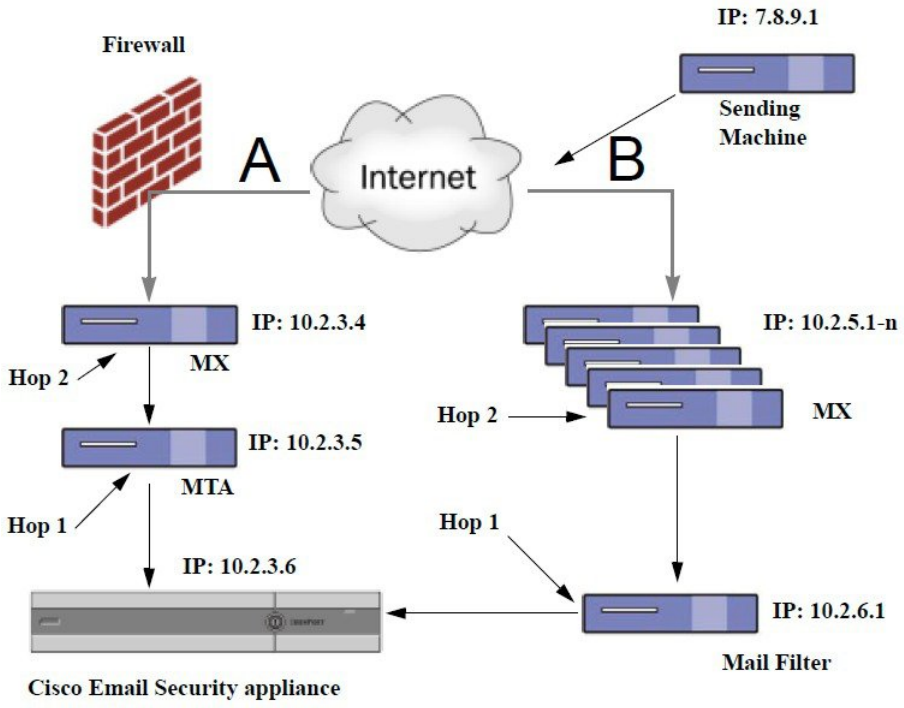
下图显示了一个非常基本的传入中继示例。从 IP 地址 7.8.9.1 发来的邮件看似是从 IP 地址 10.2.3.4 发来，因为本地 MX/MTA 正在向邮件网关中继邮件。

Figure 6: 通过 ***MX/MTA*** 中继的邮件 - 简单



下图显示了另外两个稍微复杂一些的示例，展示了如何在网络内中继邮件以及邮件在传递到邮件网关之前如何通过网络内的多台服务器处理邮件。在示例 A 中，来自 7.8.9.1 的邮件穿过防火墙并在传送到邮件网关之前通过 MX 和 MTA 来处理。在示例 B 中，来自 7.8.9.1 的邮件发送到负载均衡器或其他类型的流量整形设备，然后在传送到邮件网关之前发送到任意一个 MX。

Figure 7: 通过 *MX/MTA* 中继的邮件 - 高级



配置邮件网关以使用传入中继

相关主题

- 启用传入中继功能 , on page 31
- 添加传入中继 , on page 32
- 中继邮件的邮件信头 , on page 33

启用传入中继功能

Note 仅当本地 MX/MTA 将邮件中继到邮件网关时，才能启用传入中继功能。

Procedure

步骤 1 依次选择网络 **(Network)** > 传入中继 **(Incoming Relays)**。

步骤 2 单击启用 **(Enable)**。

步骤 3 确认您的更改。

添加传入中继

添加传入中继以识别：

- 网络中将传入邮件中继到邮件网关的每台计算机，以及
- 将标记原始外部发件人的 IP 地址的信头。

准备工作

有关完成这些前提条件所需的信息，请参阅中继邮件的邮件信头 , on page 33。

- 确定是否使用自定义或接收的信头来识别原始外部发件人的 IP 地址。
- 如果将使用自定义信头：
  - 确定将标记中继的邮件的原始 IP 地址的确切信头。
  - 对于连接到原始外部发件人的每个 MX、MTA 或其他计算机，设置该计算机，以便将信头名称和原始外部发件人的 IP 地址添加到传入邮件。

Procedure

步骤 1 依次选择**网络 (Network) > 传入中继 (Incoming Relays)**。

步骤 2 单击**添加中继 (Add Relay)**。

步骤 3 输入中继的名称。

步骤 4 输入连接到邮件网关的 MTA、MX 或其他计算机的 IP 地址，以中继传入邮件。

可以使用 IPv4 或 IPv6 地址、标准 CIDR 格式或者一个 IP 地址范围。例如，如果网络边缘有多个 MTA 在接收邮件，您可能需要输入一个 IP 地址范围以包括您的所有 MTA，例如 10.2.3.1/8 或 10.2.3.1-10。

对于 IPv6 地址，AsyncOS 支持以下格式：

- `2620:101:2004:4202::0-2620:101:2004:4202::ff`
- `2620:101:2004:4202::`
- `2620:101:2004:4202::23`
- `2620:101:2004:4202::/64`

步骤 5 指定将识别原始外部发件人的 IP 地址的信头。

在输入信头时，不需要输入拖尾冒号。

a) 选择信头类型：

选择自定义信头（推荐）或已接收的信头。

b) 对于自定义信头：

输入配置中继计算机以添加到中继邮件的信头名称。

例如：

`SenderIP`

或

`X-CustomHeader`

c) 对于已接收的信头：

输入将在其后显示 IP 地址的字符或字符串。为“跳数”输入一个数字以检查 IP 地址。

步骤 6 提交并确认更改。

What to do next

请考虑执行以下操作：

- 将中继计算机添加到具有对 DHAP 允许无限邮件的邮件流量策略的发件人组。有关说明，请参阅传入中继和目录搜集攻击防御, on page 37。
- 为便于跟踪和故障排除，请配置邮件网关日志以显示要使用的信头。请参阅配置日志以指定要使用的信头 , on page 38。

相关主题

- 如何配置邮件网关以扫描垃圾邮件, on page 2

中继邮件的邮件信头

将邮件网关配置为使用以下类型的信头之一来识别中继邮件的原始发件人：

- 自定义信头 , on page 33
- 已接收信头, on page 34

自定义信头

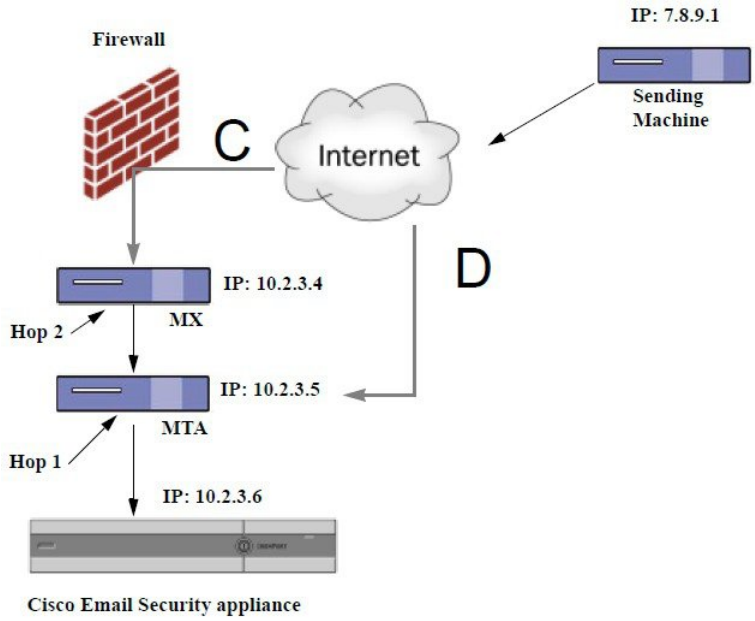
建议的识别原始发件人的方法是使用自定义信头。连接到原始发件人的计算机需要添加此自定义信头。信头的值应是外部发送计算机的 IP 地址。例如：

`SenderIP: 7.8.9.1`

`X-CustomHeader: 7.8.9.1`

如果本地MX/MTA可以从可变跳数接收邮件，则插入自定义信头是启用传入中继功能的唯一方式。例如，在下图中，路径 C 和 D 都会指向 IP 地址 10.2.3.5；但是，路径 C 有两跳，而路径 D 有一跳。由于在此情况下，跳数可能会不同，因此必须使用自定义信头来正确配置传入中继。

Figure 8: MX/MTA 中继的邮件 - 可变跳数



相关主题

- 添加传入中继 , on page 32

已接收信头

如果将 MX/MTA 配置为包含发送 IP 地址的自定义信头这一方案行不通，则可以配置传入中继功能以尝试通过检查邮件中的 Received: 信头来确定发送 IP 地址。仅当 IP 地址对应的网络“跳”数始终恒定时，使用“已接收:”(Received:) 信头才起作用。换句话说，在第一跳中的计算机（图 - 通过 *MX/MTA* 中继的邮件 - 高级中的 10.2.3.5）距离网络边缘应始终具有相同的跳数。如果传入邮件采用不同的路径（导致跳数不同，如图 - 通过 *MX/MTA* 中继的邮件 - 可变跳数中所述）到达连接到 邮件网关的计算机，则必须使用自定义信头（请参阅自定义信头 , on page 33）。

指定解析字符或字符串以及要回去查看的网络跳数（或 Received: 信头）。一跳基本上是指从一台计算机传送到另一台计算机（由邮件网关接收不计为一跳。有关更多信息，请参阅配置日志以指定要使用的信头 , on page 38）。AsyncOS 会在与指定的跳数对应的“已接收:”(Received:) 信头中首次出现解析字符或字符串之后的第一个 IP 地址。例如，如果指定两跳，则会解析从邮件网关向后数第二个 Received: 信头。如果没有找到解析字符和有效的 IP 地址，邮件网关会使用连接计算机的实际 IP 地址。

对于以下邮件信头示例，如果指定左方括号 ([) 和两跳，则外部计算机的 IP 地址为 7.8.9.1。但是，如果指定一个右圆括号 ()) 作为解析字符，就找不到有效的 IP 地址。在这种情况下，传入中继功能将禁用，并且会使用连接计算机的 IP 地址 (10.2.3.5)。

在图 - 通过 *MX/MTA* 中继的邮件 - 高级的示例中，传入中继为：

- 路径 A - 10.2.3.5（使用已接收信头时为 2 跳）
- 路径 B - 10.2.6.1（使用已接收信头时为 2 跳）

下表显示了邮件传送到邮件网关期间经历多个跃点时的邮件信头示例，如图 - 通过 *MX/MTA* 中继邮件 - 高级中所示。本例展示了外来信头（被邮件网关忽略），它们在邮件到达收件人的收件箱后出现。要指定的跳数是 2。

Table 1: 一系列“接收时间：”信头（路径 ***A*** 示例 ***1***）

1	Microsoft Mail Internet Headers Version 2.0 Received: from smemail.rand.org ([10.2.2.7]) by smmail5.customerdoamin.org with Microsoft SMTPSVC(5.0.2195.6713); Received: from ironport.customerdomain.org ([10.2.3.6]) by smemail.customerdoamin.org with Microsoft SMTPSVC(5.0.2195.6713);
2	Received: from mta.customerdomain.org ([10.2.3.5]) by ironport.customerdomain.org with ESMTP; 21 Sep 2005 13:46:07 -0700
3	Received: from mx.customerdomain.org (mx.customerdomain.org) [10.2.3.4]) by mta.customerdomain.org (8.12.11/8.12.11) with ESMTP id j8LKkWu1008155 for <joefoo@customerdomain.org>
4	Received: from sending-machine.spamham.com (sending-machine.spamham.com [7.8.9.1]) by mx.customerdomain.org (Postfix) with ESMTP id 4F3DA15AC22 for <joefoo@customerdomain.org>
5	Received: from linux1.thespammer.com (HELO linux1.thespammer.com) ([10.1.1.89]) by sending-machine.spamham.com with ESMTP; Received: from exchange1.thespammer.com ([10.1.1.111]) by linux1.thespammer.com with Microsoft SMTPSVC(6.0.3790.1830); Subject: Would like a bigger paycheck? Date: Wed, 21 Sep 2005 13:46:07 -0700 From: "A. Sender" <asend@otherdomain.com> To: <joefoo@customerdomain.org>

有关上表的说明：

- 邮件网关会忽略这些信头。
- 邮件网关收到邮件（不计为一跳）。
- 第一跳（和传入中继）。
- 第二跳。这是发送邮件的 MTA。IP 地址为 7.8.9.1。
- 邮件网关会忽略这些 Microsoft Exchange 信头。

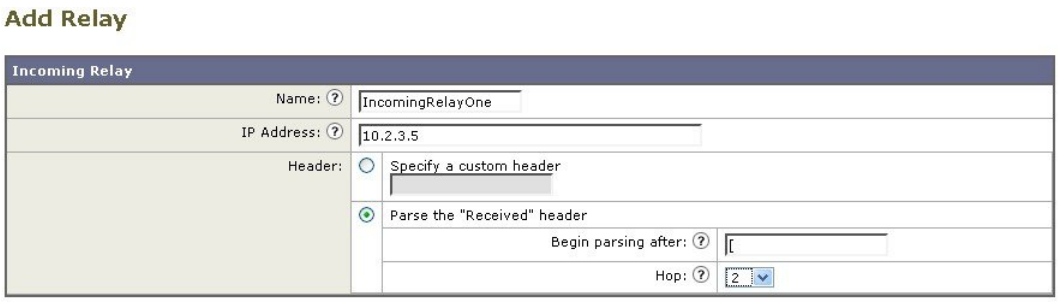
下表显示了同一邮件的信头，没有外来信头

Table 2: 一系列“接收时间：”信头（路径 ***A*** 示例 ***2***）

1	`Received: from mta.customerdomain.org ([10.2.3.5]) by ironport.customerdomain.org with ESMTP; 21 Sep 2005 13:46:07 -0700`
2	`Received: from mx.customerdomain.org (mx.customerdomain.org) [10.2.3.4]) by mta.customerdomain.org (8.12.11/8.12.11) with ESMTP id j8LKkWu1008155 for <joefoo@customerdomain.org>;`
3	`Received: from sending-machine.spamham.com (sending-machine.spamham.com [7.8.9.1]) by mx.customerdomain.org (Postfix) with ESMTP id 4F3DA15AC22 for <joefoo@customerdomain.org>;`

下图根据 GUI 中“添加中继”页面的配置显示了路径 A 的传入中继（上）：

Figure 9: 配置的具有已接收信头的传入中继



相关主题

- 添加传入中继 , on page 32

传入中继如何影响功能

传入中继和过滤器

传入中继功能通过正确的 IP 信誉得分提供各种 IP 信誉服务相关的过滤器规则 (reputation, no-reputation)。

传入中继、HAT、IP 信誉得分和发件人组

HAT 策略组当前不使用传入中继中的信息。但是，由于传入中继功能会提供信誉得分，因此可以通过邮件过滤器和 $reputation 变量模拟 HAT 策略组功能。

传入中继和目录搜集攻击防御

如果某台远程主机尝试通过向作为您网络中的传入中继的 MX 或 MTA 发送邮件来发起目录搜集攻击，则该中继分配给邮件流策略启用了目录搜集攻击防御 (DHAP) 的发件人组时，邮件网关会断开与传入中继的连接。这可防止来自中继的所有邮件（包括合法邮件）进入邮件网关。邮件网关没有机会将远程主机识别为攻击者，作为传入中继的 MX 或 MTA 将继续接收来自攻击主机的邮件。要解决此问题并继续接收来自传入中继的邮件，请通过对 DHAP 邮件没有限制的邮件流策略将该中继添加到发件人组。

传入中继和跟踪

跟踪会在跟踪结果中显示传入中继的 IP 信誉得分而不是源 IP 地址的信誉得分。

传入中继和邮件安全监控（报告）

当使用传入中继时：

- 邮件安全监控报告包含有关外部 IP 和 MX/MTA 的数据。例如，如果外部计算机（IP 为 7.8.9.1）通过内部 MX/MTA（IP 为 10.2.3.4）发送 5 封邮件，则邮件流量摘要将显示来自 IP 7.8.9.1 的 5 封邮件，以及来自内部中继 MX/MTA（IP 为 10.2.3.5）的另外 5 封邮件。
- IP 信誉得分不会在邮件安全监控报告中正确报告。此外，可能无法正确解析发件人组。

传入中继和邮件跟踪

当使用传入中继时，“邮件跟踪详细信息”(Message Tracking Details) 页面会针对邮件显示中继的 IP 地址和中继的 IP 信誉得分，而不是原始外部发件人的 IP 地址和信誉得分。

传入中继和日志记录

在以下日志示例中，发件人的 IP 信誉得分最初在第 1 行报告。稍后，在处理传入中继后，正确的 IP 信誉得分在第 5 行中报告。

1	Fri Apr 28 17:07:29 2006 Info: ICID 210158 ACCEPT SG UNKNOWNLIST match nx.domain IPR rfc1918
2	Fri Apr 28 17:07:29 2006 Info: Start MID 201434 ICID 210158
3	Fri Apr 28 17:07:29 2006 Info: MID 201434 ICID 210158 From: <joe@sender.com>
4	Fri Apr 28 17:07:29 2006 Info: MID 201434 ICID 210158 RID 0 To: <mary@example.com>
5	Fri Apr 28 17:07:29 2006 Info: MID 201434 IncomingRelay(senderdotcom): Header Received found, IP 192.192.108.1 being used, IPR **6.8**

6	Fri Apr 28 17:07:29 2006 Info: MID 201434 Message-ID '<7.0.1.0.2.20060428170643.0451be40@sender.com>'
7	Fri Apr 28 17:07:29 2006 Info: MID 201434 Subject 'That report...'
8	Fri Apr 28 17:07:29 2006 Info: MID 201434 ready 2367 bytes from <joe@sender.com>
9	Fri Apr 28 17:07:29 2006 Info: MID 201434 matched all recipients for per-recipient policy DEFAULT in the inbound table
10	Fri Apr 28 17:07:34 2006 Info: ICID 210158 close
11	Fri Apr 28 17:07:35 2006 Info: MID 201434 using engine: CASE spam negative
12	Fri Apr 28 17:07:35 2006 Info: MID 201434 antivirus negative
13	Fri Apr 28 17:07:35 2006 Info: MID 201434 queued for delivery

传入中继和邮件日志

以下示例显示了包含传入中继信息的典型日志条目：

```
Wed Aug 17 11:20:41 2005 Info: MID 58298 IncomingRelay(myrelay): Header Received found, IP
 192.168.230.120 being used
```

配置日志以指定要使用的信头

邮件网关只检查在收到邮件时存在的信头。因此，在本地添加的其他信头（例如 Microsoft Exchange 信头等）或邮件网关接收邮件时添加的信头不会进行处理。一种有助于确定使用什么信头的方法是配置 AsyncOS 日志记录以包括所使用的信头。

要配置信头的日志记录设置，请参阅配置日志记录的全局设置。

监控规则更新

接受许可协议后，可以查看最近的思科反垃圾邮件和思科智能多重扫描规则更新。

Procedure

步骤 1 依次选择**安全服务 (Security Services) > IronPort 反垃圾邮件 (IronPort Anti-Spam)**。

或

步骤 2 选择**安全服务 (Security Services) > IMS 和灰色邮件 (IMS and Graymail)**。

步骤 3 查看**规则更新 (Rule Updates)** 部分和：

收件人	更多信息
查看每个组件的最近更新	如果尚未进行更新或者还未配置服务器，则会显示“从未更新”(Never Updated)。
查看更新是否可用	-
如果更新可用，则更新规则	单击**立即更新 (Update Now)**。

What to do next

相关主题

- 服务更新
- 通过代理服务器进行更新
- 配置服务器设置以下载升级和更新

测试反垃圾邮件

收件人	相应操作	更多信息
测试配置。	使用 `X-advertisement: spam` 信头测试配置。 为了便于测试，思科反垃圾邮件将 X 信头格式为 `X-Advertisement: spam` 的任何邮件视为垃圾邮件。	通过该信头发送的测试邮件将由思科反垃圾邮件进行标记，并且您可以确认是否执行了为该邮件策略（定义反垃圾邮件策略, on page 17）配置的操作。 将此信头与以下其中一项配合使用： • 使用 SMTP 命令发送具有此信头的测试邮件。请参阅向邮件网关发送邮件以测试思科反垃圾邮件, on page 40。 • 使用 trace 命令并包含此信头。请参阅使用测试邮件调试邮件流：追踪。
评估反垃圾邮件引擎效力。	使用直接来自互联网的实时邮件流评估产品。	有关应避免的无效评估方法的列表，请参阅不是测试反垃圾邮件效力的方式, on page 41。

相关主题

- 向邮件网关发送邮件以测试思科反垃圾邮件, on page 40
- 不是测试反垃圾邮件效力的方式, on page 41

向邮件网关发送邮件以测试思科反垃圾邮件

准备工作

查看测试反垃圾邮件配置：使用 SMTP 的示例, on page 40中的示例。

Procedure

步骤 1 为某个邮件策略启用思科反垃圾邮件。

步骤 2 将包含下列信头的测试邮件发送给该邮件策略中的用户：X-Advertisement: spam

将 SMTP 命令与 Telnet 配合使用，将此邮件发送到您有权访问的地址。

步骤 3 检查测试账户的邮箱并确认是否根据为该邮件策略配置的操作正确传送了测试邮件。

例如：

- 主题行是否已修改？
- 是否添加了其他自定义信头？
- 邮件是否已传送到备用地址？
- 邮件是否已被丢弃？

相关主题

- 测试反垃圾邮件配置：使用 SMTP 的示例, on page 40

测试反垃圾邮件配置：使用 SMTP 的示例

在本例中，邮件策略必须配置为接收发往测试地址的邮件，并且 HAT 必须接受测试连接。

```
# telnet IP_address_of_IronPort_Appliance_with_IronPort_Anti-Spam port

220 hostname ESMTP

helo example.com

250 hostname

mail from: <test@example.com>

250 sender <test@example.com> ok

rcpt to: <test@address>

250 recipient <test@address>
ok

data

354 go ahead
```

```
Subject: Spam Message Test

X-Advertisement: spam

spam test

.

250 Message MID accepted

221 hostname

quit
```

不是测试反垃圾邮件效力的方式

由于 IronPort 反垃圾邮件和思科智能多重扫描规则会快速添加以防止活动的垃圾邮件攻击，并且攻击一旦过去便快速到期，因此不能使用下列任一方法测试效力：

- 使用重发或转发邮件或剪切并粘贴的垃圾邮件进行评估。

  缺少适当信头、连接 IP、签名等内容的邮件会产生不正确的得分。

- 仅测试“不容易识别的垃圾邮件”。

  使用 IP 信誉服务、阻止列表、邮件过滤器等功能删除“容易识别的垃圾邮件”会降低总体捕获率百分比。

- 重新发送另一个反垃圾邮件供应商捕获的垃圾邮件。

- 测试较早的邮件。

  扫描引擎会根据当前威胁快速添加和删除规则。使用旧邮件进行测试将产生不准确的测试结果。

不是测试反垃圾邮件效力的方式